Міністерство освіти і науки України
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

А.Я. Гладун, О.О. Пучков, І.Ю. Субач, К.О. Хала

Англо-український
СЛОВНИК ТЕРМІНІВ
з інформаційних технологій та кібербезпеки

Розглянуто Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
для використання у навчальному процесі з підготовки
фахівців вищої освіти
зі спеціальностей «Комп'ютерні науки» та «Кібербезпека»

Київ
ІСЗЗІ КПІ ім. Ігоря Сікорського
2018

УДК 004.056
ББК 20я2+73я2
Г 52

Розглянуто Вченою радою
ІСЗЗІ КПІ ім. Ігоря Сікорського
(*Протокол №4 від 13.12.2018*)

Рецензенти:
О.Г. *Оксіюк*, д.т.н., проф.
В.А. *Савченко*, д.т.н., с.н.с.
С.А. *Жицька*

Г 52 Гладун А.Я. Англо-український словник термінів з інформаційних технологій та кібербезпеки / А.Я. Гладун, О.О. Пучков, І.Ю. Субач, К.О. Хала. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. – 380 с.

У структурованому вигляді подано близько 4000 загальних та спеціальних термінів і понять, зміст яких відповідає сфері кібербезпеки. Докладно розглянуті сучасні основи кібербезпеки особистості. Значну увагу приділено загрозам інформаційній безпеці, інформаційній боротьбі, безпеці інформаційних технологій, криптології, технічним методам та засобам захисту інформації, організаційно-технічному захисту інформації в комп'ютерних системах та мережах, державній та комерційній таємниці тощо.

Для курсантів, інженерів, науковців та спеціалістів у сфері кібербезпеки. Словник може бути корисним широкому колу читачів: від системних адміністраторів і проектувальників систем безпеки інформації до керівників підрозділів, що займаються питаннями забезпечення кібербезпеки держави.

УДК 004.056
ББК 20я2+73я2

ПЕРЕДМОВА

Сьогодні комп'ютери та комп'ютерні мережі проникли в усі сфери діяльності людини і стали доступними великій кількості користувачів із різним ступенем підготовки, а швидкий розвиток цифрових технологій і створення нових апаратних засобів і програмних продуктів кожен день породжують нові терміни. Крім того, значення деяких термінів міняються з часом. В перекладах англомовних матеріалів, інформаційних ресурсів мережі Інтернет, спеціалізованих підручниках, статтях, настановах та інструкціях по використанню та експлуатації подібні англійські терміни часто замінюються українськими «кальками», що утруднює розумінню змісту і наводить плутанину у визначені терміну. Словники – настільні книги професійного перекладача і кожного просунутого спеціаліста, який слідкує за новинками науки і техніки (а відомості про них зазвичай публікуються на англійській мові), тому автори намагались пропоноване друковане видання зробити максимально інформативним і зручним для будь-якого читача, хоть на жаль неможливо охопити цілком усю предметну область кібербезпеки.

Як відомо, важливою складовою будь-якої соціально значущої діяльності є понятійно-термінологічний апарат, який забезпечує належний рівень галузевої та загальної комунікації суб'єктів цієї діяльності (інтероперабельність понять) . Сьогодні широкого розповсюдження набули різноманітні терміни, що належать до особливо динамічної специфічної сфери діяльності людини, пов'язаною з інфомаційною безпекою.

Інформаційна безпека[1] — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

[1] ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи керування інформаційною безпекою. Вимоги (чинний з 01.01.2017)

Комп'ютерна безпека — це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерною технікою та комп'ютерними мережами з точки зору конфіденційності, цілісності і доступності

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «**Кібербезпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Створення безпечних комп'ютерних систем і застосунків є метою діяльності багатьох організацій та установ, системних адміністраторів мережі і системних програмістів, а також предметом теоретичного дослідження як у галузі телекомунікаційних мереж та комп'ютерних наук, так і економіки.

У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів.

Кібербезпека як нова міждисциплінарна галузь знань вимагає особливого підходу до тлумачення породжуваних нею термінів. Це завдання є досить складним тому, що розвиток сфери інформаційно-комп'ютерних технологій у порівнянні з іншими галузями світової економіки відбувається найбільш високими темпами.

Наприклад, широке розповсюдження комп'ютерів та мобільних обчислювальних пристроїв і впровадження їх практично в усі сфери людської діяльності привело до виникнення за рубежем загального терміну «комп'ютинг» (computing). На думку фахівців найбільших інформаційних організацій світу, включаючи ACM, AIS, AITP і IEEE, комп'ютинг охоплює такі галузі знань: а) обчислювальну техніку (computer engineering), б) теорію обчислювальних систем (computer science), в) інформаційні системи (information systems), г) інформаційні

технології (information technology), д) проектування й розробку програмного забезпечення (software engineering). У цілому, під комп'ютингом розуміють будь-яку цілеспрямовану діяльність, що ґрунтується на використанні комп'ютера або сферу застосування зусиль, спрямованих на його створення. Таким чином, комп'ютинг включає: а) проектування й реалізацію програмних і апаратних складових комп'ютерних систем для широкого спектра застосувань; б) обробку, структурування й керування різними видами інформації; в) виконання наукових досліджень із використанням комп'ютерів; г) створення інтелектуальних комп'ютерних систем; д) розробку й використання комунікаційних засобів і технологій для передачі інформації; е) пошук і ранжирування релевантної інформації відповідно до формованих запитів тощо.

У зв'язку з цим, на думку авторів, викликає інтерес робота, пов'язана з підбором термінів, що враховує не тільки поточну ситуацію в розвитку сучасної комп'ютерно-комунікативної індустрії, але й об'єднання деяких взаємозалежних термінів у логічно пов'язані групи. До них, на наш погляд, у першу чергу, варто віднести обчислювальні пристрої різних класів, мови програмування, види програмування, типи прикладних програм, типи програмних компонентів тощо.

За минулі роки автори маючи справу із стандартизацією у сфері інформаційної безпеки та розробки термінологічних словників у інформаційних технологіях дослідили як закордонні так і вітчизняні видання, які найбільш повно відбивають основні процеси структурування термінології в складному світі кібербезпеки та інформаційних технологій, що активно сьогодні розвиваються. Кожне з досліджених видань дуже часто, відбиває різні концепції, використовує власну систематику й часто розглядає терміни й поняття під різними кутами зору. Тому автори намагалися у своїй роботі використовувати як сучасні тенденції розвитку термінології в інформаційних технологіях, словники та довідники так рекомендації органів стандартизації України, зокрема Технічного комітету зі стандартизації науково-технічної термінології (ТК 19) під егідою Міністерства освіти і науки України, який функціонує у стінах НУ «Львівська політехніка».

Сфера кібербезпеки, завдяки своїй суспільній значущості сьогодні стала одним з пріоритетних об'єктів державної діяльності, як на

внутрішньодержавному, так і на міжнародному рівнях, а також об’єктом актуальних наукових досліджень.

У сучасну епоху зростає роль національної безпеки, першочергову увагу приділяють формування комплексних підходів до інформаційної безпеки та до її складової компонентти кібербезпеки. Це спричинює необхідність ефективної комунікації фахівців із забезпечення інформаційної безпеки. Значну роль у цьому відграє наявність міжнародного досвіду, міжнародних стандартів та настановчих матеріалів, що потребує чіткого однозначного розуміння англомовної термінології і її гармонізація з українською термінологією на усіх рівнях інформаційної безпеки. Це вказує на безперечну актуальність та важливість якісного понятійно-термінологікового апарату у цій сфері.

Інформаційну безпеку держави характеризують ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери керування, військової справи, суспільної свідомості тощо) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Зважаючи на різноплановість та неоднозначність інформаційних процесів з кібербезпеки окремі терміни мають декілька значень, які відображено у словнику. Крім того, наводиться їх усталені або нормативно визначені абревіатури.

Словник розроблено для широкого кола читачів, зокрема для студентів, що навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Керування інформаційною безпекою» тощо, а також для аспірантів, науковців та практиків, які досліджують проблематику, пов'язану із організаційно-правовим забезпеченням інформаційної безпеки в Україні.

Природно, що всі існуючі терміни, а тим більше ті, що мають міждисциплінарний характер, зібрати й витлумачити вкрай складно. Тому автори прагнули системно підійти не тільки до відбору власне статей словника, але й до подання їхнього змісту й суті.

Як нам уявляється, однією з основних проблем в освоєнні інформатики, на відміну від інших фундаментальних наук, є все зростаюча потреба у введенні нових термінів понятійної бази, яка постійно розширюється.

Словник містить понад 4 000 (найбільш популярних і значимих на думку авторів) термінів і абревіатур з найширшої області кібербезпеки та визначень, що органічно вплітаються в її тканину, з математики, електроніки, лінгвістики, біоінформатики й багатьох інших суміжних галузей.

Слова в даному виданні розміщені за абеткою, як правило, в однині. До українських термінів надаються англійські еквіваленти, а до англійських – українські (розташовувані в круглих дужках). Синоніми й абревіатури термінів, що наводяться, даються у квадратних дужках після їхнього згадування.

У словнику використано терміни, що стали широковживаними в українськомовних публікаціях, написання яких стало звичним в українській транслітерації: Інтернет, веб, веб-сторінка, веб-сервер тощо.

Автори висловлюють свою вдячність усім, хто надішле коментарі, зауваження й пропозиції щодо вдосконалювання книги на електронні адреси: *glanat@yahoo.com* або *igor_subach@ukr.net* або *cecerongreat@ukr.net* .

Використані джерела: При роботі над словником автори, природно, не могли не користуватися багаточисельними джерелами, а також сучасними компютерними засобами і технологіями, особливо Інтернет-технологіями і пошуковими системами (зокрема, семантичним пошуком), які суттєво пришвидшували технічну частину роботи – пошук термінів (з їх тлумаченням, синонімами, прикладами застосування) і Інтернеті, існуючих словниках як паперових так і електронних. Ми також звірялися з Інтернет-енциклопедіями WikipediA і Вікіпедія (варто відмітити, що більше 65% наведених у цьому словнику термінів у цих джерелах відсутні). Багато нових термінів і прикладів їх застосування було взято безпосередньо із сучасної англійської науково-технічної літератури. А також став у нагоді великий досвід роботи у сфері стандартизації при розробці стандартів та гармонізації (перекладу англомовних стандартів на українську) у технічному комітеті із стандартизації України ТК-20 «Інформаційні технології». За час роботи авторами підготовлено 164 ДСТУ, гармонізованих з

стандартами ISO/IEC, ITU-T, ETSI, ANSI, IEEE та інших міжнародних організацій по стандартизації.

Подяки.

Створення словника є неможливим без допомоги і консультацій колег-спеціалістів. Автори вдячні усім, хто посприяв у різний час виконанню цієї роботи. Ми вдячні за допомогу.

Побудова словника та словникові статті

Усі англійські терміни у словнику розташовані в алфавітному порядку й виділені напівжирним шрифтом.

Словарні статті побудовані наступним чином. Спочатку наведено термін англійською мовою. Якщо це абревіатура, то безпосередньо за нею надано розшифровку англійською мовою. Надалі наводиться переклад терміна українською мовою. Круглі скобки (всередині як англійського терміна, так і українського перекладу) містять факультативні слова, синоніми, або їх частини, або такі, що маються на увазі. Круглі скобки містять уточнюючі або роз'яснювальні слова. Синонімічні або близькі за змістом українські еквіваленти відділені комою. Терміни, які не дуже близькі за змістом, - крапкою з комою. Еквіваленти одного англійського поняття, які дуже відрізняються за змістом, відділені цифрами.

Після перекладу терміна наведено його тлумачення. У разі присутності у словнику англійського терміна, на який є посилання у тлумаченні. Його виділено курсивом.

У словнику вживається сорочення *див.*, що указує на синонім або близький за значенням термін.

Англійський алфавіт

Великі літери												
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Маленькі літери												
a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z

Перелік уживаних абревіатур

АСОІ – автоматизована система оброблення інформації
АТС – автоматична телефонна станція
БД – база даних
ВВС – взаємозвязок відкритих систем
ДПЛА – дистанційно пілотований літальний апарат
ЕОМ – електронно-обчислювальна машина
ЕПР – ефективна поверхня розсіювання
ЕС – експертна система
ІОМ – інформаційно-обчислювальна мережа
ЛА – літальний апарат
ЛМ – локальна мережа
МОІ – мережа обміну інформацією
МОС – Міжнародна організація із стандартизації
НСД – несанкціонований доступ
ОС – операційна система
ПЕОМ – персональна електронно-обчислювальна машина
ПК – персональний комп’ютер
РБД – розподілені бази даних
СКБД – система керування базою даних
СКРБД – система керування розподіленими базами даних
СУІБ – система керування інформаційною безпекою
ТЗ – технічне завдання

.NET – читають як «дот нет» (Microsoft.NET) # закінчення, яким супроводжуються практично усі назви сучасного покоління продуктів від Microsoft. Відображає точку зору Microsoft на побудову інфраструктури сучасного комунікаційного світу, у якому комп'ютерні мережі з'єднують людей і техніку. Людина, яка працює з комп'ютером або використовує смартфон, звичайним чином стає частиною локальної або глобальної мережі. У програмних продуктах .Net за цим ім'ям стоїть цілком конкретний зміст, який припускає, зокрема, наявність відкритих стандартів комунікації, перехід від створення монолітних застосувань до створення програмних компонентів (веб-сервісів), які призначені для розподіленого повторного використання в різних середовищах і застосуваннях. Можливість повторного використання вже створених компонентів і легкість розширення їх функціональності – все це неодмінні атрибути нових технологій. Важливу роль у цих технологіях відіграє мова XML, що стала стандартом обміну повідомленнями в будь-якій мережі.

3G – third generation mobile telephone system – система цифрового мобільного зв'язку третього покоління.

A

AAA – authentication, authorization and accounting – автентифікація, авторизація й облік.

abbreviated address calling – виклик за скороченою адресою # виклик, який дає змогу користувачеві під час ініціювання ним виклику застосовувати адресу, що має менше символів, ніж повна адреса.

abduction – абдукція # логікове виведення від конкретних фактів до правдоподібних пояснень цих фактів.

abductive inference – абдуктивне виведення # логікове виведення від конкретних фактів до правдоподібних пояснень цих фактів.

abort sequence – послідовність примусового переривання # визначений бітовий шаблон, який можна зустріти в будь-якому місці бітового потоку, та застосовувати для передчасного припинення пересилання кадру.

abort statement – оператор примусового переривання # простий оператор, що порушує нормальний хід виконання одного чи кількох завдань для запобігання подальшої взаємодії з таким завданням.

aborted connection – перерване з'єднання # розрив з'єднання, що не слідує за встановленими процедурами # перерване з'єднання може дозволити іншим особам отримати несанкціонований доступ.

absolute address – абсолютна адреса # безпосередня адреса, яка визначає місце розташування без посилання на базову адресу # абсолютна адреса

сама по собі може бути базовою адресою.

absolute code – абсолютний код # код, в якому всі адреси є абсолютними адресами.

absolute command – абсолютна команда.

absolute coordinate – абсолютні координати # будь-яка з координат, що визначає положення адресовної точки щодо початку заданої системи координат.

absolute error – абсолютна похибка # алгебричний результат віднімання істинного, зазначеного чи теоретично правильного значення від значення, обчисленого, спостережуваного, вимірюваного чи доступного.

absolute instruction – абсолютна інструкція # команда відображення, в якій застосовують абсолютні координати.

absolute term – абсолютний термін # термін, що виражає тільки одне поняття.

absolute vector – абсолютний вектор # вектор, початкова і кінцева точки якого зазначено в абсолютних координатах.

abstract data type – абстрактний тип даних # клас структур даних, описаний переліком операцій або функцій, які доступні в структурах даних та формальними властивостями цих операцій, з інтерфейсами, відокремленими від внутрішньої реалізації.

abstract syntax – абстрактний синтаксис # специфікація даних прикладного рівня або інформація керування протоколу прикладного рівня з застосуванням правил нотації, які не залежать від способу кодування, застосованого для їх подання.

abstract syntax notation – нотація абстрактного синтаксису # система умовних позначень для опису синтаксису протоколів.

abuser – зловмисник # 1. особа або організація, що займаються добуванням інформації в інтересах розвідки державної і комерційної, кримінальних елементів, непорядних співробітників або просто психічно хворих людей # 2. стосовно обчислювальних мереж – особа або організація, що зацікавлена в одержанні несанкціонованого доступу до програм або даних, які здійснюють спробу такого доступу або здійснили її.

ACM – association for computing machinery – ассоціація з обчислювальної техніки.

accept statement – оператор приймання # складений оператор в серверній задачі, який змушує цю серверну задачу очікувати іншу задачу чи виконати основну програму оператора вхідного виклику для синхронізації задач.

access – доступ # можливість застосовувати будь-якого ресурсу інформаційної системи. Здатність і засоби спілкування обміну даними з іншими системами або іншим чином взаємодіяти з ними, використання системних ресурсів для обробки інформації, отримання знань про

інформацію, яку містить система, або для управління компонентами системи та функціями.

access administrator – адміністратор доступу # одна з посадових осіб в складі адміністрації банку даних, що відповідає за організацію доступу користувачів до баз даних.

access authority – орган доступу – суб'єкт, відповідальний за моніторинг та надання пільг доступу для інших уповноважених організацій.

access category– категорія доступу # *1.* атрибут об’єкта доступу, що визначає рівень повноважень, який повинен мати суб’єкт доступу для одержання права доступу до даних об’єкта (наприклад, категорія секретності і службові повноваження) # *2.* комбінація ієрархічних і неієрархічнихатрибутів доступу, що відображає рівень критичності (наприклад, конфіденційності) інформації або повноважень користувача щодо доступу до такої інформації.

access check – контроль доступу # контроль за доступом # високонадійний процес, що забезпечує визначення і обмеження доступу користувачів, програм або процесів (узагалі суб’єктів) до ресурсів та об’єктів системи обчислювальної згідно з моделлю захисту. Може бути реалізований шляхом організації звернення до таблиці, яку зберігають в пам’яті і в якій перелічені права суб’єктів доступу. В ході виконання процесу може здійснюватися реєстрація всіх спроб доступу несанкціонованого в журналі контрольному.

access check to equipment – контроль доступу до апаратури # сукупність заходів по недопущенню порушника до внутрішнього монтажу, ліній зв’язку, технологічних органів керування. Здійснюють за допомогою засобів контролю розкривання апаратури не тільки в інтересах захисту інформації від НСД, але і для дотримання технологічної дисципліни з метою забезпечення нормального функціонування апаратури (системи).

access control – керування доступом [до інформації] # 1. сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням правил розмежування доступу # 2. сукупність взаємопов’язаних заходів, спрямованих на ідентифікацію осіб і звернень до інформації, перевірку повноважень осіб і звернень, реєстрацію звернень до інформації, що підлягає захисту, реагування на звернення до інформації (дозвіл доступу або відмова доступу до інформації).

access control category – категорія керування доступом # мовні елементи, призначені для визначення правил, що запобігають виконанню несанкціонованих операцій.

access control certificate – сертифікат керування доступом.

access control data – дані керування доступом # набір даних, пов’язаних з

визначенням або модифікацією привілеїв керування доступом

access control field – поле керування доступом # бітовий шаблон, що дає змогу відрізнити кадр від маркера, а також визначає мережні станції пересилання даних, які можуть застосовувати маркер, а також визначає, коли кадр має бути скасованим, і дає змогу мережним станціям запросити наступний маркер.

access control information – керування доступом до інформації.

access control key – ключ керування доступом # ключ, який процес пред'являє системі керування базами даних і який вона порівнює з відповідним замком з метою запобігання несанкціонованому доступу до даних.

access control list – **1.** перелік засобів керування доступом # **2.** список контролю доступом # список логічних об'єктів, разом з переліком їхніх прав на доступ, які мають дозвіл на доступ до ресурсу.

access control list – перелік доступу # перелік користувачів і (або) процесів з зазначенням їхніх прав доступу до об'єкта комп'ютерної системи, з яким пов'язаний цей перелік.

access control mechanism – механізм керування доступом # механізм, що може використовуватися для введення політики безпеки.

access fraud – шахрайський доступ # несанкціоноване використання послуг стільникового зв'язку шляхом навмисного або ненавмисного втручання, маніпулювання або перепрограмування серійних або ідентифікаційних номерів стільникових апаратів.

access gateway – шлюз доступу # шлюз, який підтримує інтерфейси «користувач – мережа».

access identifier – ідентифікатор доступу # унікальна ознака суб'єкта або об'єкта доступу.

access layer – рівень доступу # ієрархічна частина категорії доступу пасивного об'єкта.

access level – категорія доступу # див. access category.

access level – рівень гарантій # 1. міра впевненості в тому, що система комп'ютерна коректно реалізує політику безпеки # 2. у «загальних критеріях» – сім стандартизованих наборів вимог гарантій безпеки, що регламентують застосування різноманітних методів і технологій розробки, тестування, контролю й верифікації продукту інформаційних технологій (функціональне тестування; структурне тестування; методичне тестування й перевірка; методична розробка, тестування й аналіз; напівформальні методи розробки й тестування; напівформальні методи верифікації розробки й тестування; формальні методи верифікації розробки і і тестування), кожний з яких визначає ступінь відповідності IT-продукту кожній вимозі гарантій (гарантії зростають від першого рівня до сьомого). Назви рівнів відображають можливості засобів контролю й

верифікації, що застосовуються в ході розробки й аналізу ІТ-продукту.

access level – рівень доступу # рівень повноважень, що вимагають від об’єкта для отримання доступу до захищеного ресурсу # наприклад повноваження для доступу до даних або інформації на певному рівні безпеки.

access list – перелік повноважень для доступу # перелік об’єктів з їх правами доступу, яким дозволено одержати доступ до ресурсу.

access management service – сервіс адміністративного керування доступом # сервіс, що дає змогу користувацькому агентові та агентові передсилання повідомлень встановити доступ один до одного та адміністративно керувати відповідною інформацією.

access matrix – матриця доступу # *n*-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів системи комп’ютерної одного типу (об’єктів-користувачів, об’єктів-процесів чи об’єктів пасивних), і містить як елементи права доступу за кожним із типів об’єктів.

access mechanism – механізм доступу.

access mediation information – атрибут доступу # будь-яка зв’язана з об’єктом системи комп’ютерної інформація, яку використовують для керування доступом.

access mediation rules – правило розмежування доступу # частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів.

access method – метод доступу # метод отримання даних, застосовуючи сховище для читання чи запису даних або застосовування каналу введення-виведення для пересилання даних # наприклад випадковий метод доступу, індексований метод доступу, послідовний метод доступу.

access network – мережа доступу # сукупність засобів (кабелі, обладнання передачі тощо), які створюють необхідні для надання телекомунікаційних сервісів транспортні можливості між інтерфейсом вузла надання сервісів і відповідними інтерфейсами користувач-мережа.

access node – вузол доступу # кінцевий вузол мережі, який забезпечує користувачам доступ до її сервісів.

access object – об’єкт доступу # пасивна сутність (запис, файл, блок пам’яті і т. ін.), що містить або одержує інформацію. Доступ до об’єкту доступу здійснюють суб’єкти доступу за допомогою набору операцій, які надають об’єкту доступу.

access path – шлях доступу # ланцюжок адрес, який приводить до місця розташування потрібних даних # одночасно може бути більше ніж один шлях доступу до одного екземпляру даних.

access path independence – незалежність шляху доступу # відокремлення опису даних від шляху доступу до нього у такий

спосіб, що зміни шляху доступу не потребують внесення змін до опису даних у програмі.

access period – період доступу # проміжок часу, протягом якого переважають певні права доступу.

access permission – дозвіл на доступ # всі права доступу для заданого суб'єкта щодо будь-якого об'єкта.

access portability – **1.** переносність доступу # **2.** мобільність доступу # здатність мережі при зміні місцезнаходження абонента за його запитом оперативно надавати йому еквівалентні можливості доступу на новому мережному об'єкті [станції].

access right – право доступу # 1. сукупність правил доступу до інформації, яку захищають, встановлених правовими документами або власником інформації # 2. право, надане користувачеві на санкціоноване використання певної інформації (зокрема, програм та даних), яку зберігають в системі # 3. дозвіл або заборона здійснення певного типу доступу.

access rule – правило доступу # сукупність правил, які регламентують порядок і умови доступу до інформації, яку захищають, і до її носіїв.

access subject – суб'єкт доступу # активна сутність (процес, користувач, пристрій і т. ін.), що викликає утворення інформаційного потоку між об'єктами доступу або зміну стану обчислювальної системи. Дії суб'єкта доступу регламентують правилами розмежування доступу.

access time – час доступу # інтервал часу між моментом ініціювання запиту даних, і моментом завершення доставлення даних # час доступу дорівнює сумі часу затримки та часу пересилання.

access to data – доступ до даних # надання даних системі оброблення даних чи одержання їх від неї шляхом виконання операцій пошуку, читання та (або) записування даних.

access to information – доступ до інформації # *1.* ознайомлення з інформацією, її оброблення, а саме, копіювання, модифікація або знищення інформації # *2.* наближення органів розвідки (агентів, технічних засобів) до джерел (або носіїв) інформації для забезпечення з ними контакту розвідувального # в обчислювальних мережах – можливість одержання, оброблення та (або) порушення цілісності інформації # *4.* вид взаємодії двох об'єктів комп'ютерної системи, внаслідок якого створюють потік інформації від одного об'єкта до іншого і (або) проходить зміна стану об'єкта.

access to secret [top-secret] clearance – доступ до відомостей, що складають державну таємницю # санкціоноване повноважною посадовою особою ознайомлення конкретної особи з відомостями, що складають таємницю державну.

access type – тип доступу # 1. суттєвість доступу до об'єкта, що

характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис) # 2. тип операції, що визначають правами доступу # наприклад читання, запис, виконання, додавання, змінення, видалення, створення.

access unit – модуль доступу # функційний модуль, який пов'язує систему пересилання повідомлень з іншою системою обмінювання даними, за допомогою якого його користувачі одержують опосередкований доступ до системи опрацювання повідомлень.

accidental threat – непередбачувана загроза # ненавмисна загроза # загроза, яку спричиняють випадкові впливи на інформацію в процесі її введення, зберігання, оброблення, виведення і передавання. В результаті таких впливів на апаратному рівні відбуваються фізичні зміни сигналів в цифрових кодах, що несуть інформацію, а на програмному рівні може відбутися зміна алгоритму оброблення інформації на непередбачений, характер якої може бути різноманітним: у кращому випадку – зупинка обчислювального процесу, а в гіршому – його модифікація. Якщо засоби функціонального контролю змін не виявили, то наслідки модифікації алгоритму або даних можуть пройти непоміченими або привести до руйнування інформації, а при переплутуванні адреси пристрою – до витоку інформації. Причинами випадкових впливів при експлуатації інформаційних (обчислювальних) систем можуть бути: відмова і збої апаратури; завади на лініях зв’язку від впливів зовнішнього середовища; помилки людини як ланки системи; схемні і схемотехнічні помилки розробників; структурні, алгоритмічні і програмні помилки; аварійні ситуації та інші впливи.

accountability – **1.** відстежуваність # обліковість # властивість, яка гарантує, що дії об'єкта можуть бути однозначно відстежуваними стосовно цього об’єкта # **2.** спостережність # властивість системи (системи комп’ютерної), що дозволяє фіксувати діяльність користувачів і процесів, використання об’єктів пасивних, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання відповідальності за певні дії.

accreditation – акредитація # в галузі безпеки інформації – процедура надання формальної заяви або власне формальна заява як така, за якою офіційно уповноважений орган сертифікації повідомляє, що система оброблення даних, мережа, система автоматизована може застосовуватися для оброблення інформації критичної при використанні даної політики безпеки з даними службами та механізмами

інформаційної безпеки. Взагалі термін а. відноситься до процедури або самого факту визнання правочинності особи чи органу виконувати конкретні роботи.

accumulation – накопичення # поступове збирання, накоплення в будь-якій кількості.

accumulator – накопичувач # 1. пристрій запам'ятовуючий зовнішній # 2. у СКБД – основна частина бази даних, призначена для розташування і зберігання даних.

accuracy – точність # чинник якості за відсутності помилок # якісна оцінка за відсутності помилок; висока оцінка, що відповідає невеликій помилці # кількісна міра похибки, переважно виражена як функція відносної похибки; висока значущість цієї міри, відповідає невеликій похибці.

acknowledgment – підтвердження # ствердна відповідь приймача відправнику, яка вказує, що передані дані було отримано.

ACL – access control list – перелік керування доступом.

acoustic intelligence – акустична розвідка # вид розвідки технічної, призначений для одержання інформації з носіїв у вигляді хвиль акустичних. В залежності від середовища розповсюдження хвиль акустичної розвідки поділяють на власне акустичну (повітряно-акустичну), гідроакустичну (середовище розповсюдження – вода) і сейсмічну (середовище розповсюдження – земна поверхня).

acoustic signal masking – маскування акустичного сигналу # спосіб приховування акустичного сигналу енергетичного, заснований на створенні і розповсюдженні маскувальних звукових хвиль у напрямках можливого підслухування. Гучність звуку, яку сприймає людина, залежить не тільки від його власної інтенсивності, але і від інших звуків, що діють одночасно на барабанну перетинку вуха. Відповідно до психофізіологічних особливостей сприйняття звуку людиною інтенсивність маскувальних звуків асиметрична. Асиметричність проявляється в тому, що маскувальний звук здійснює відносно невеликий вплив на тони звуку, які маскують, нижчий його власної частоти, але сильно ускладнює сприйняття більш високих звуків. Тому для маскування акустичного сигналу ефективні низькочастотні акустичні шумові сигнали, що створюються шумовими акустичними генераторами.

acoustical material – акустичні матеріали # матеріали, призначені для пониження шуму і створення оптимальних умов чутності в приміщеннях; поділяються на звукопоглинальні і звукоізоляційні.

acquisition –# *1.* вибирання чогось з різних місць, від різних осіб і т. ін. # *2.* поступове приєднання, складання чогось одного до одного, частину до частини # *3.* складання чогось докупи, в одне місце.

action – дія # елемент дій оцінювача # ці дії або сформульовані в явному вигляді як дії оцінювача, або неявно випливають з дій розробника (де припускаються дії оцінювача) в рамках компонентів довіри.

active attack – активна атака # атака на віддалену мережу обміну інформацією, яку здійснюють з метою нанесення прямих збитків мережі шляхом порушення конфіденційності, цілісності і доступності інформації, а також здійснення впливів психологічних на користувачів мережі. Очевидною особливістю активної атаки порівняно з пасивною атакою є принципова можливість її виявлення.

active disk unit – активний накопичувач # нагромаджувач на дискові магнітному, доступний в даний момент системі і користувачу.

active hiding – активне приховування інформації # приховування інформації створенням таких фізичних полів та речовин, які ускладнюють здобування інформації або спричиняють невизначеність її змісту.

active information accumulation – активне накопичення інформації # нагромадження інформації, при якому здійснюють певне оброблення інформації, що поступає, спрямоване на збагачення знань одержувача інформації.

active matrix display – дисплей на активній матриці # пристрій відображення, який надає кожному пікселю на екрані свій власний транзистор для точнішого керування ним # це забезпечує кращу контрастність і меншу розмитість відображень.

active matrix display device – пристрій дисплея з активною матрицею.

active threat – активна загроза # будь-яка загроза навмисної несанкціонованої зміни стану системи опрацювання даних # наприклад загрози, що призводять до модифікації повідомлень, вставки помилкових повідомлень, маскування логічних об'єктів або відмови в обслуговуванні сервісу.

active window – активне вікно # будь-яке з множини вікон, з яким в заданий час проводять маніпуляції.

active wiretapping – активне перехоплення під час під’єднання до лінії зв'язку # прослуховування лінії зв'язку з метою змінити або вставити дані.

activities – діяльність # див. activity, work.

activity – діяльність # *1.* специфічна людська форма активного відношення до навколишнього світу, зміст якої складає його доцільна зміна і перетворення # *2.* робота, заняття в якій-небудь галузі # *3.* робота будь-яких закладів, органів влади. Типи, види і форми д. різноманітні: д. законодавча, парламентська, політична, адміністративна, організаторська, виховна освітня, наукова, інформаційна, військова, міжнародна, дипломатична і т. ін.

actor – актор # сутність, яка заповнює тематичну роль в сценарії # наприклад агент, супровідний агент, бенефіціар, пацієнт.

actual argument – фактичний аргумент # параметр, такий як вираз, ідентифікатор або інша мовна конструкція, яку застосовують у виклику або універсальному екземплярі для асоціювання об'єкта даних з відповідною декларацією # відповідною декларацією називають формальний параметр.

actual parameter – фактичний параметр.

actual recipient – фактичний отримувач # потенційний отримувач, якому фактично роблять доставку чи направляють підтвердження # статус потенційного отримувача буде змінено на фактичного отримувача у разі завершення доставляння або підтвердження.

actual transfer rate– [фактична] швидкість пересилання даних # середня кількість бітів, символів або блоків, що передають за одиницю часу між двома точками.

actuator – актуатор # механізм, відповідальний за переміщення приводу доступу або механічного гребня.

AD – administrative domain – домен адміністративного керування.

ad hoc – у перекладі з латині означає «спеціальний, для даної, конкретної мети» # режим з'єднання декількох пристроїв за технологією Wi-Fi (комп'ютер-комп'ютер або комп'ютер-кишеньковий ПК). Режим ad hoc призначений для об'єднання в бездротову мережу декількох пристроїв (стандартно – до 8). Максимальна відстань між пристроями не повинна перевищувати 450 метрів. Станції зможуть зв'язуватися одна з одною як тільки завершують конфігурацію всієї мережі. Інша перевага цього режиму полягає в можливості розташовування комп'ютерів на значній відстані один від одного, що дає змогу одержувати збільшену зону дії мережі в цілому.

ad hoc project – спеціальний проект # разовий проект # конкретне рішення # див. ad hoc, ad hoc queries.

ad hoc queries – нерегламентовані, незаплановані запити [до БД] # див. ad hoc, ad hoc project.

adaptive chosen plaintext attack – криптоаналітична атака з адаптивно-вибраним відкритим текстом # частковий випадок ітеративної атаки криптоаналітичної з вибраним відкритим текстом, при якій крипто аналітик обирає відкритий текст на наступному кроці залежно від отриманого результату на поточному кроці.

add-in – вбудовування # процес уставляння, приладжування якогось предмета, деталі і т.ін. усередину чого-небудь.

address – адреса # *1.* значення, яке визначає місце розташування # наприклад номер регістра, адреса певної частини пристрою зберігання, адреса пристрою, мережна адреса # *2.* ім'я, однозначне у рамках

середовища ВВС, що застосовують для визначення множини точок доступу до сервісу, який розташований на границі між n-рівнем і (n+1)-рівнем в одній відкритій системі.

address administration – адміністрування адрес # призначення ЛМ адрес локально або на універсальній основі.

address format – формат адреси # число та розташування елементів адресі # наприклад сторінка і зміщення в системі віртуальної адресації; канал, пристрій, сектор і записи в пам'ять на дисковому запам’ятовувальному пристрої.

address modification – модифікація адреси # будь-яка арифметична, логікова або синтаксична операція, яку виконують з адресою.

address offset – адреса зміщення # число, яке має бути додано до відносної адреси, щоб визначити адресу місця зберігання, до якого отримують доступ.

address resolution protocol – протокол перетворення адреси # протокол мережі Інтернет, використовуваний для перетворення IP-адрес в MAC-адреси керування доступом до середовища, що дозволяє опорним комп’ютерам і маршрутизаторам визначати адреси рівня ланки даних за допомогою процесу запиту (ARP Request) і відповіді (ARP Response).

address space – адресний простір # набір адрес, які може бути використано в конкретній програмі або функційному блоці # адресний простір може охоплювати віртуальні адреси.

address translator – транслятор адрес # функційний модуль, який перетворює віртуальні адреси на фізичні.

addressing domain – адресний домен # централізовано адміністрована частина ієрархічного адресного простору мережі Інтернет, яка має ідентифікуючу її унікальну назву і яку обслуговує група серверів доменних імен.

adequacy – достовірність, вірогідність # *1.* форма існування істини, обґрунтованої яким-небудь способом (наприклад, експериментом, логічним доказом) для об’єкта, який пізнають (вивчають) # *2.* властивість інформації бути правильно сприйнятою; ймовірність відсутності помилок.

adjacent domains – суміжні домени # два домени, з'єднані між собою за допомогою обладнання, розташованого на суміжних вузлах.

adjacent nodes – суміжні вузли # два вузли, з'єднані гілкою.

ADMD – домен адміністративного керування

administration domain name – ім’я адміністративного домену # атрибут, який визначає домен адміністративного керування щодо країни.

administration management domain – домен адміністративного керування # домен керування, адміністрований оператором телекомунікацій, який визнано уповноваженим органом

телекомунікацій даної країни # оператор телекомунікацій надає послуги населенню в цілому.

administrative domain – домен адміністративного керування # сукупність мережного обладнання, яке підлягає керуванню одним вузлом адміністративного керування.

administrative security – адміністративна безпека.

administrator – адміністратор # *1.* адміністративно-посадова особа, керівник, розпорядник, організатор # *2.* користувач, роль якого охоплює функції керування системою комп'ютерною і (або) комплексом засобів захисту.

ADSL – asymmetric digital subscriber line – асиметрична цифрова абонентська лінія.

ADT – **abstract data type –** абстрактний тип даних.

advantage – перевага # зверхність над ким-чим-небудь у якому-небудь відношенні.

adversary – противник # див. opponent, enemy.

aerial – антена # див. antenna.

aerial line – повітряна лінія зв'язку # лінія зв'язку проводова, основним елементом якої є два провідники з однаковими електричними властивостями. В залежності від типу несучих конструкцій повітряних ліній зв'язку поділяють на стовпові, несучими конструкціями яких є дерев'яні або залізобетонні опори, і стоякові, несучими конструкціями яких є металеві стійки, встановлені, наприклад, на дахах будинків. Для ізоляції проводів повітряних ліній один від одного і відносно землі їх закріплюють на ізоляторах.

AES – advanced encryption standard – покращений стандарт шифрування.

affine transformation – афінне перетворення # перетворення, що приводить до системи лінійних рівнянь, яка має однозначно означене рішення. Прикладом афінного перетворення є $y = (ax + s) mod n$.

after-image – залишковий образ [пепретворенній образ] # копія блока або запису після зміни.

after-look journal – журнал змін # журнал, в який заносяться нові значення змінених записів. Використання цього журналу дозволяє повторити зміни.

ag(e)ing – старіння # процес зміни характеристик або параметрів будь-чого внаслідок дії часу.

agency – **1.** агентство # *1.* організація, що виконує певні доручення державних і інших установ або приватних осіб # *2.* установа, що збирає та подає інформацію в пресу, на радіо, телебачення # *3.* представництво, відділення центральної установи # **2.** керування # див. management, control # **3.** орган # установи, організації, що виконують певні функції.

agency of technical protection of information – орган технічного захисту інформації # спеціалізований підрозділ, призначений для забезпечення захисту інформації технічного в організації. Може входити до складу служби безпеки

організації. Основні завдання органу: обслідування виділених будівель (приміщень) з метою встановлення потенційно можливих каналів витоку конфіденційної інформації через технічні засоби, конструкції будівель і обладнання; виявлення і оцінка ступеня небезпеки технічних каналів витоку інформації; розроблення заходів ліквідації (запобігання витоку) потенційних каналів витоку інформації; організація контролю (в тому числі і інструментального) за ефективністю прийняти захисних заходів, аналіз результатів контролю і розроблення пропозицій з підвищення надійності і ефективності заходів захисту; підготовка заявок на придбання технічних засобів захисту, участь у встановленні засобів захисту, їхній експлуатації і контролі стану. Крім того, на орган технічного захисту інформації доцільно покласти також технічні питання охорони носіїв інформації.

agent group – агентурна група # група агентів і нелегалів, яких об’єднує одне завдання, один об’єкт розвідки і які знаходяться на зв’язку однієї людини, куратора або резидента. В кожній агентурній групі може існувати декілька осередків, відокремлених один від іншого. Таке подрібнення необхідне для того, щоб провал одного агента або одного осередку не привів до провалу всієї агентури.

agents – *1.* агентство # див. agency # *2.* агентура # див. intelligence network.

aggregate – агрегат # структурована колекція компонентів, де компоненти можуть мати однакову або різну структуру даних, і де структура даних самої колекції також може бути складовою частиною відповідного зіставного типу.

aggregate device – агрегатний пристрій # пристрій, що містить множину логічних або фізичних пристроїв.

aggregate value – агреговані значення # значення даних, пов'язане з агрегатом.

aggregation – агрегування # отримання конфіденційної інформації за допомогою збирання та кореляції інформації меншої уразливості.

aggression – агресія # *1.* мотивована деструктивна поведінка, що суперечить нормам та правилам співіснування людей у суспільстві, наносить шкоду об’єктам нападу # *2.* міжнародно-правове поняття, що характеризує незаконне застосування збройної сили однієї держави (групи держав) проти іншої держави (групи держав) для її захоплення, поневолення або примусу до прийняття своїх умов шляхом порушення її суверенітету, територіальної цілісності, політичної та економічної незалежності # Інформаційно-психологікова агресія – дії, спрямовані на нанесення противнику конкретного, відчутного впливу в окремих галузях його діяльності. Ознаками інформаційно-психологічної агресії можуть бути: обмежене та локальне за своїми масштабами застосування сили;

виключення із засобів інформаційно-психологічного впливу найбільш небезпечних видів інформаційної зброї, які не дозволяють контролювати розміри нанесених збитків; обмеження розмірів простору, об'єктів інформаційної інфраструктури і соціальних груп, що можуть бути уражені інформаційно-психологічним впливом (агресія торкає не весь інформаційно-психологічний простір держави-жертви, а тільки частину), обмеження за цілями (переслідує локальні, часткові цілі) і часу (як правило, завершують агресію після повного досягнення агресором усіх поставлених цілей і рідко приймає затяжний характер), а також по залученим силам та засобам.

aging intelligence information – старіння розвідувальної інформації # часткова або повна втрата інформативності розвідувальних даних для тих, кому вони призначені, з плином часу.

aging of information – старіння інформації # процес втрачення з часом практичної цінності інформації, зумовлений зміною об'єкта інформації. Як характеристики процесу старіння, звичайно, використовують або напівперіод життя наукових документів, або період їхнього життя. Напівперіодом життя наукової літератури вважають час, за який половина всієї опублікованої у теперішній момент літератури в певній галузі перестане використовуватися. Період життя наукової літератури – час, за який перестане використовуватися вся опублікована у теперішній момент література.

agreement – погодження # 1. взаємна згода, домовленість # 2. договір, що встановлює які-небудь умови, взаємовідносини, права й обов'язки сторін.

Aiken code – код Айкена # спосіб двійкового кодування десяткових цифр, при якому код цифр 0-4 співпадає з двійковим кодом чисел 0-4, а код цифр 5-9 – з двійковим кодом чисел 11-15 відповідно.

aiming – наведення # встановлення зв'язку, контакту.

air interface – повітряний інтерфейс # бездротовий радіоінтерфейс між абонентським пристроєм мобільного зв'язку й базовою станцією.

airborne vehicle – літальний апарат # ЛА # технічний пристрій для польотів в атмосфері Землі або в космічному просторі. Розрізняють такі ЛА: легші за повітря (повітроплавні), важчі за повітря (авіаційні, космічні, авіаційно-космічні та ракети). ЛА поділяють також на пілотовані та безпілотні, на одно- та багаторазового використання, за призначенням – на науково-дослідні,народногосподарські та військові. До повітроплавних ЛА відносяться аеростати і дирижаблі. Авіаційні ЛА поділяються на крилаті (літаки, планери) та гвинтокрилі (гелікоптери, автожири,

гвинтокрили); ракети на балістичні та крилаті. До КЛА відносяться навколоземні орбітальні космічні апарати – ШСЗ та міжпланетні автоматичні станції. Авіаційно-космічні апарати поєднують ознаки авіаційних і космічних апаратів (повітряно-космічний корабель, повітряно-космічний літак).

aircraft – літальний апарат # див. airborne vehicle.

airship – літальний апарат # див. airborne vehicle.

alarm signaling – тривожна сигналізація # сигналізація, призначена для психологічного впливу на порушника, який скріпо проникає в зони, що охороняються, з метою примусити його відмовитися від наміру. Засобами сигналізації служать, найчастіше разом, звукові і світлові сповіщувачі. В системі охорони об’єктів вони повинні мати відповідну потужність випромінювання звуку і світла, яка не тільки інформує зловмисника про те, що він виявлений, але і викликає у нього почуття страху. Найбільш сильний психологічний вплив в тихий нічний час здійснює звук сирени на межі больового відчуття (біля 120 дБ) і яскраве миготливе світло.

alert – сигнал тривоги # негайне сповіщення про те, що інформаційна система і мережа можуть піддаватися атаці або перебувають в небезпеці внаслідок аварії, збою або людської помилки

algorithm – алгоритм # *1.* система точно визначених правил дії (програма) з зазначенням, як і в якій послідовності ці правила застосувати до первинних даних певної задачі, щоб одержати її розв’язок. Назва походить від імені середньовічного узбецького математика Мухамеда-ібн-Суса (арабізоване аль-Хорезмі) # *2.* точний припис, який визначає процес обчислювальний, що йде від варійованих початкових даних до шуканого результату. Одним із способів задавання алгоритма є логікова схема (блок-схема). Програма являє собою опис а. на мові програмування # *3.* точно визначене правило дій (програма), для якого задана вказівка як і в якій послідовності це правило потрібно застосовувати до вхідних даних задачі для того, щоб отримати її рішення. Це поняття не є точним математичним визначенням, а лише визначає суть слова а. Існують декілька точних математичних формалізації поняття алгоритм, серед яких загальнорекурсивні та частково-рекурсивні функції, машини Тьюрінга, нормальні алгоритми Маркова, алгоритм Колмогорова і т.ін. Відомо, що всі формальні визначення алгоритм еквівалентні між собою. При визначенні а. вважаються зафіксованими вхідний *A* та вихідний *B*. Алгоритм отримує на вхід слово w з множини всіх слів вхідного алфавіту *A** і як результат виконання послідовності елементарних операцій (або кроків

роботи), подає на вихід слово *f(w)* з множини всіх слів вихідного алфавіту *B**. Алгоритм розв'язує масову задачу, якщо при отриманні на вході будь-якої індивідуальної задачі *w є A** він за скінченну кількість кроків подає на вихід її розв'язок. Довжиною вхідного слова |*w*| є кількість букв у слові *w*. Алгоритм розв'язує задачу за час *£*, якщо на кожному вході w він робить не більше, ніж t кроків. Звичайно, *t* залежить від |*w*|.

algorithm theory – теорія алгоритмів # розділ математики, який вивчає загальні властивості алгоритмів. Виділяють дві гілки теорії: логічну теорію, яка охоплює питаннями конструктивного обґрунтування математики і вивченням феномена алгоритмічної невирішеності проблем, і аналітичну теорію алгоритмів, зв'язану з вивченням самих алгоритмів, аналізом їхньої структури, методами еквівалентних перетворень, способами побудови і оцінкою ефективності.

algorithmic access – алгоритмічний доступ # доступ, що базують на обчисленні адреси за деяким алгоритмом.

algorithmic check – алгоритмічний контроль # контроль програмний, суть якого в тому, що задача, вирішена за будь-яким алгоритмом, перевіряють повторно по грубішому алгоритму з достатнім ступенем точності. Продуктивність ЕОМ при к. а. вище, проте він має такі ж недоліки як і контроль програмно-логічний та, крім того, обмежене застосування, так як не завжди можна знайти для основного алгоритму скорочений.

alias – псевдонім # (електронна пошта) альтернатива для імені відправника/отримувача чи адреси відправника/отримувача. Псевдонім можа застосовувати в каталозі # (мови програмування) альтернативний ідентифікатор для мовних конструкцій.

allowed radio frequency band – дозволена смуга радіочастот /разрешенная п. радиочастот/ — смуга частот, в межах якої радіостанції дозволене випромінювання. Ширина дозволеної смуги радіочастот дорівнює смузі радіочастот необхідній плюс подвоєне абсолютне допустиме значення відхилення частоти, а для космічних станцій – плюс подвоєний максимальний допплерівський зсув частоти відносно будь-якої точки земної поверхні.

alphabet – алфавіт # абетка # набір символів, в якому заздалегідь був узгоджений порядок його елементів # наприклад набір з 128 ASCII-символів.

alphabetic character set – набір абеткових символів # набір символів, що містить літери та, можливо, спеціальні символи, але не містить цифр.

alphabetic code – абетковий код # абеткова схема кодування.

alphabetic code element set – абетковий кодовий набір [елементів] # кодовий

набір, елементи якого побудовано з набору абеткових символів.

alphabetic code set – абетковий кодовий набір [елементів].

alphabetic coding – літерне кодування # кодування даних, при якому кодові комбінації складаються тільки з букв деякого алфавіту.

alphabetic string – абетковий рядок # рядок, складений тільки із символів, що належать до одного набору абеткових символів.

alphabetic word – абеткове слово # слово, яке складено із символів з одного набору абеткових символів.

alphanumeric – літерно-цифровий # дані, які складають з літер, цифр і зазвичай інших символів, таких як знаки пунктуації, а також процесів і функційних блоків, які застосовують ці дані.

alphanumeric character – літерно-цифровий символ # символ набору літерно-цифрових символів.

alphanumeric character set – набір літерно-цифрових символів # набір символів, який містить літери та цифри і можливо спеціальні символи.

alphanumeric code – абетково-цифровий код # літерно-цифровий код # код, набір знаків якого складають з букв, цифр та інших знаків.

alphanumeric code – літерно-цифровий код # код, чиє застосування призводить до набору літерно-цифрового коду.

alphanumeric code element set – набір [елементів] літерно-цифрового коду # кодовий набір, елементи якого побудовані з набору літерно-цифрових символів.

alphanumeric code set – набір [елементів] літерно-цифрового коду.

alpha-numeric coding – літерно-цифрове кодування # кодування даних, при якому кодові комбінації складаються з букв, цифр та інших знаків деякого алфавіту.

alphanumeric data – літерно-цифрові дані # дані, представлені літерами та цифрами, можливо, разом із спеціальними символами і символ пробілу.

alphanumeric word – літерно-цифрове слово # слово, яке складено із символів того самого набору літерно-цифрових символів.

alternate recipient – альтернативний отримувач # потенційний отримувач, якому повідомлення чи зразок буде надістано тільки в тому разі, коли його не має змоги переслати конкретному пріорітетному отримувачу # альтернативного отримувача призначає або відправник, або потенційні отримувачі.

alternate track – альтернативна доріжка.

alternative track – доріжка заміни # запасну доріжку застосовують замість нормальної доріжки в тому випадку, якщо остання пошкоджена або несправна.

american national standards institute – американський національний інститут стандартів # американський представник міжнародної організації стандартів (ISO). Приватна,

недержавна організація, заснована в 1918 р. і відповідальна в США за розробку й публікацію стандартів, пов'язаних з кодуванням, передачею сигналів (ANSI/IEEE 802 і FDDI) і т.п. ANSI об'єднує виробників устаткування, телекомунікаційних операторів та інші організації.

anagement domain name – ім'я домену адміністративного керування # ідентифікатор домену адміністративного керування.

anagram – анаграма # *1.* синонім шифру перестановки # *2.* переставляння окремих літер або складів у слові, внаслідок чого утворюються нові слова з іншим значенням.

analog signal – аналоговий сигнал # сигнал, в якому характеристична величина подання даних може набути в будь-який момент будь-яке значення в межах неперервного інтервалу # наприклад, аналоговий сигнал може неперервно слідувати за значеннями іншої фізичної величини, що представляє дані.

analog variable – аналогова змінна # неперервно змінюваний сигнал, що представляє або математичну змінну або фізичну величину.

analysis – аналіз # *1.* метод дослідження, що полягає в м нелепому або практичному розчленуванні цілого на складові частини # протилежне до синтезу # *2.* уточнення логічної форми (побудови, структури) міркування засобами формальної логіки.

analyst – аналітик # *1.* фахівець, який здійснює аналіз # *2.* особа, яка систематизує розрізнені у часі події, роз'ясненням, тлумаченням, співставленням однозначних або розрізнених фактів # *3.* фахівець в інформатиці й конкретній прикладній галузі, обов'язками якого є аналіз проблем, постановка завдань і розробка пропозицій для їхнього виконання.

analytical – аналітичний # такий, що отримують в результаті розчленування об'єкта й аналізу одержаних унаслідок цього частин.

analytical attack – аналітична атака.

analytical model – аналітична модель # алгоритм або обчислення, які комбінують один чи більше базових показників і/або похідних показників разом з відповідним критерієм прийняття рішення

analytical model – аналітична модель # алгоритм або обчислення, які комбінують один чи більше базових показників і/або похідних показників разом з відповідним критерієм прийняття рішення

analytical model – аналітична модель # алгоритм або розрахунок, що охоплює одну або більше основних і/або похідних заходів, з відповідним критеріями прийняття рішень.

analyzer – аналізатор # *1.* в оптиці – прилад (поляризаційна призма, поляроїд і т. ін.) для виявлення і дослідження поляризації світла # *2.* аналізатор гармонік – прилад для дослідження складових (гармонік) спектра частот; застосовують у

високочастотній техніці # *3.* в акустиці – аналізатор звуку прилад для аналізу звуку за частотними та часовими характеристиками # *4.* фізіологічні аналізатори – анатомофізіологічні системи у людини і тварин, що здійснюють сприйняття і аналіз подразників, що поступають з зовнішнього і внутрішнього середовища; до аналізаторів відносяться всі органи чуттів (зоровий, слуховий, нюховий і т. ін.); кожний аналізатор містить рецептор, провідникову частину і вищий центр – групи нейронів у корі головного мозку.

android – андроїд – від грец. «людина» # мобільна ОС, що працює на ядрі Linux. Спочатку була розроблена компанією Android Inc. (Palo Alto, California, USA), пізніше придбаною Google. Вона дозволяє розроблювачам створювати на мові Java застосування, з метою керування мобільними пристроями за допомогою розроблених Google бібліотек. Для неї є можливість писати застосування на C і інших мовах програмування за допомогою Android Native Development Kit.

angle reflector – кутовий відбивач # радіовідбивач, що містить жорстко зв’язані між собою перпендикулярні площини. Найважливішою властивістю кутового відбивача є те, що значна частка енергії хвилі, що падає на нього в межах достатньо великого кута (біля 80 градусів), відбивають назад в бік опромінюючої радіолокаційної станції. Тому кутові відбивачі навіть невеликих розмірів мають значну ефективну поверхню розсіювання. Кутовий відбивач з трьох граней з розмірами 0,5 м при довжині хвилі радіолокаційної станції 3 см створює ефективну поверхню розсіювання 290 $м^2$ (ефективна поверхня розсіювання літака- бомбардувальника В-52 – біля 100 $м^2$).

ANSI – american national standards institute – американський національний інститут стандартів.

anonymous – анонімний # об'єкт даних, який не має чітко вказаного типу даних.

anonymous remailer – анонімний поштовий сервер # анонімний відправник # функційний модуль, який дає змогу відправникам повідомлень приховувати свої ідентифікаційні дані від кінцевих отримувачів.

answering – автоматична відповідь # процес відповіді на виклик станції пересилання даних для завершення встановлення з'єднання між станціями пересилання даних.

antagonism – протиборство # див. confrontation, opposition.

antenna – антена #пристрій для випромінювання (передавальна а.) або приймання (приймальна а.) радіохвиль. Передавальна а. перетворює енергію змінного струму високої частоти, що поступає від передавача, в енергію електромагнітних хвиль, які розповсюджуються від антени в просторі. Приймальна антена

вловлює енергію електромагнітних хвиль і перетворює її в енергію змінного струму високої частоти (в електричні сигнали, амплітуда, частота і фаза яких відповідає аналогічним характеристикам електромагнітних хвиль). Основними характеристиками антени є діаграма спрямованості антени, коефіцієнт корисної дії антени, коефіцієнт спрямованої дії антени, коефіцієнт підсилення, частотна характеристика, опір випромінювання антени і т.ін. У відповідності з принципом взаємності (оборотності) кожна антена може працювати і як передавальна, і як приймальна, при цьому її основні характеристики не змінюються. Разом із тим передавальні і приймальні антени можуть відрізнятися одна від іншої конструкцією, електричною стійкістю і деякими іншими параметрами. Антену класифікують за наступними основними ознаками: за призначенням – передавальні, приймальні і приймально-передавальні, а також у залежності від галузі застосування – зв'язкові, телевізійні, радіолокаційні, радіоастрономічні, радіопеленгаційні і т. ін.; за діапазоном хвиль, що передаються або приймаються, на кілометрові, метрові, декаметрові, сантиметрові і міліметрові; за конструкцією та принципом дії – на проводові антени (вібраторні, штирові), антени акустичного типу (хвилепровідні, рупорні), антени оптичного типу (дзеркальні, лінзові), рамкові антени, спіральні антени, антени поверхневих хвиль (щілинні антени, діелектричні антени, антенні решітки); за розподілом випромінюваної енергії у просторі – на неспрямовані і спрямовані антени (із різноманітною формою діаграми спрямованості); за способом керування положенням діаграми спрямованості – на антени з механічним, електромеханічним і електричним скануванням променя; за місцем установлення – на антени наземній, підземні, танкові, корабельні, літакові (вертолітні), космічних апаратів та і т. ін.; за способом установки – на антени стаціонарні, тимчасові (аварійні), зовнішні, внутрішні, нестабілізовані, стабілізовані.

antenna direction diagram – діаграма спрямованості антена # графічне зображення рівня сигналу антени (випромінюваного або того, що приймають) в залежності від кута обернення антени в горизонтальній і вертикальній площинах. Діаграми спрямованості антена зображують в прямокутних і полярних координатах. Діаграми спрямованості можуть мати різноманітний покраяний характер, який визначають механічною конструкцією і електричними параметрами. Пелюстку діаграмм спрямованості антени з максимумом потужності випромінюваного або того, що приймають електромагнітним полем, називають головною або основною пелюсткою,

а решта – боковими і задніми. Співвідношення між величинами потужності основної пелюстки у порівнянні з рештою пелюсток характеризує спрямовані властивості антени. Ширину головної пелюстки вимірюють кутом між прямими, проведеними з початку полярних координат до значень діаграм спрямованості антена, які відповідають половині максимальної потужності випромінювання або 0,707 напруги електричного сигналу приймальної антени. Чим вужча ширина діаграми спрямованості антена, тим вищий її коефіцієнт спрямованої дії.

anticountermeasures – контрпротидія #запобігання дії, що перешкоджає іншій дії.

antivirus – антивірус # в обчислювальній техніці – програма, що виявляє або виявляє та знищує віруси комп'ютерні.

anti-virus program – антивірусна програма.

APDU – application protocol data unit – протокольний блок даних прикладного рівня.

API – application programming interface – інтерфейс прикладного програмування.

apparatus – апарат # прилад, пристрій.

application – **1.** застосунок # **2.** застосовна програма # програма, яка виконує свої функції безпосередньо для користувача # **3.** застосування # обробка даних та операцій, пов'язані з особливими вимогами до інформаційних систем

application capabilities type – тип можливостей додатків # тип можливостей хмари, в якому споживач служби хмарних обчислень може використовувати додатки постачальника служби хмарних обчислень.

application process – **1.** застосовний процес # оброблення інформації в реальній відкритій системі в конкретних застосунках # **2.** прикладний процес # процес, специфікований відповідно до вимог певної інформаційної системи.

application programming interface – інтерфейс прикладного програмування # інтерфейс, за допомогою якого реалізуються процеси створення, встановлення, тестування та модифікації застосовних програм

application server – сервер застосувань # сервер, який надає інформацію, запитувану віддаленою чи місцевою застосовною програмою [клієнтом].

application system – прикладна система # набір прикладних процесів, що використовують послуги, які забезпечує інтерфейс між людиною та комп'ютером, полегшення комунікації та система керування даними, що виконує обробку, необхідну для задоволення вимог до інформаційної системи.

application task – прикладна задача # задача, яка ставиться у певній галузі практичної діяльності людини у інформаційному середовищі (полі).

application-process-invocation – виклик прикладного процесу # конкретне

часткове або повне використання можливостей цього прикладного процесу для підтримання конкретного сеансу оброблення інформації.

application-process-type – тип прикладного процесу # опис класу прикладних процесів як набору можливостей, які застосовуються при обробленні інформації.

applied cryptanalysis – прикладний криптоаналіз # метод криптоаналізу шляхом викрадення всієї інформації про криптосистему (в тому числі і ключів).

approach – підхід # принцип # сукупність прийомів, способів впливу на кого-що-небудь, вивчення будь- чого, ведення справи # див. principle, concept.

arbiter – арбітр # посередник, що його обирають сторони за взаємною згодою або в передбаченому законом порядку з метою розв'язання спору.

arbitrary [technical] channel of information leakage – **1.** самочинний [технічний] канал витоку інформації # **2.** ненавмисний канал витоку інформації # технічний канал витоку інформації, в якому носії інформації та/або середовище їх поширення формуються самочинно.

architecture – архітектура # *1.* базова організація системи, реалізована в її компонентах, їхніх відношеннях між собою і з середовищем, а також принципи, що визначають її проектування і розвиток # *2.* концепція взаємозв'язку елементів складної структури. Охоплює компоненти логічної, фізичної і програмної структур.

architecture of information security in telecommunication networks – архітектура захисту інформації в мережах телекомунікацій # концепція захисту інформації в мережах телекомунікацій, що використовують міжнародні стандарти, яка розроблена і супроводжена Міжнародною організацією зі стандартизації (ISO) у відповідності до ідеології моделі взаємодії відкритих систем.

architecture open system – архітектура відкритих систем # концепція обчислювальної мережі, яка розроблена і супроводжена Міжнародною організацією зі стандартизації (ISO); семирівнева модель з'єднання відкритих систем, яка відіграє важливу роль як методологічна, концептуальна й термінологікова основа побудови обчислювальних мереж.

archive document – архівний документ # документ, який зберігають або підлягає збереженню внаслідок його значимості для суспільства, а також такий, що має цінність для його власника.

archive file – архівний файл # файл, відкладений для подальшого дослідження або перевірки з метою безпеки чи будь-якої іншої мети.

archived file – заархівований файл # файл, для якого є архівний файл.

argument – **1.** аргумент # *1.* підстава, доказ, які наводяться для обґрунтування, підтвердження чого-

небудь. При використанні впливу змісту інформації застосовують три основні категорії аргумента для переконування: правдиві факти; аргументи, що дають “психологічне задоволення”, оскільки вони апелюють до позитивного очікування; аргументи, що апелюють до негативних очікувань. За способом подання аргумент розрізняють так звані повідомлення односторонні й повідомлення двосторонні # *2.* аргумент функції — незалежна змінна величина # **2.** незалежна змінна # фактичний параметр # будь-яке значення незалежної змінної # наприклад ключ пошуку; номер, який визначає розташування елемента в таблиці.

argumentation – аргументація # *1.* наведення аргументів # *2.* сукупність аргументів на користь чого-небудь. Підбір, побудова і подання а. є однією з важливих характеристик змісту інформації.

arm – зброя # пристрої і засоби, призначені для ураження противника в боротьбі збройній. Складають засоби ураження і засоби їх доставки до цілі; більш складна зброя містить також прилади і пристрої керування і наведення.

ARP – address resolution protocol – протокол перетворення адреси.

artificial intelligence – штучний інтелект # наука, що виникла на базі міжгалузевих досліджень в галузі техніки обчислювальної, математичної логіки, програмування, психології, лінгвістики, нейрофізіології та інших галузей знань. Об’єктом вивчення штучного інтелекту є метапроцедури, що використовуються людиною при вирішенні задач, що традиційно називаються інтелектуальними або творчими. Мета досліджень в галузі штучного інтелекту – створення арсеналу метапроцедур, достатнього для того, щоб ЕОМ (або інші технічні системи) могли знаходити по постановках задач їхнє рішення. Основними методами, що використовують в штучному інтелекті, є різного роду програмні моделі і засоби, експеримент на ЕОМ і теоретичні моделі. Основні досліджувані проблеми: подання знань; моделювання міркувань, діалогові процедури на природній мові; планування доцільної діяльності; навчання інтелектуальних систем в процесі їхньої діяльності.

artificial optical masks – штучні оптичні маски # металеві або дерев’яні каркаси, що накриваються суцільним або сіткоподібним (транспарантним) покриттям. В залежності від форми маски і способу її розташування біля об’єкта маскування розрізняють наступні типи оптичних масок: маски-навіси; маски вертикальні; перекриття маски; маски похилі; маски радіопрозорі; маски деформуючі. Штучні оптичні маски виготовляються у вигляді збірних маскувальних комплектів багаторазового використання, що не впливають на навколишнє

середовище та можуть використовуватися разом з іншими способами захисту.

artificially [technical] channel of information leakage – **1.** штучний [технічний] канал витоку інформації # **2.** навмисний канал витоку інформації.

ASCE – association control service element – асоціативний елемент сервісу керування.

ASE – application service element – елемент прикладного сервісу.

ASN – abstract syntax notation – нотація абстрактного синтаксису.

ASN.1 – abstract syntax notation one – абстрактний синтаксис нотація один.

ASR – speech recognition – розпізнавання мовлення

ASR – speech recognition – розпізнавання мовлення.

assertion – твердження # заява об'єкта без супроводжуючих її юридичних доказів # вимоги і твердження щодо значень термінів, як правило, погоджені так, щоб запеспечити їх подобу, але зі злегка різними значеннями. Для цілей цього Міжнародного стандарту «твердження» вважають більш сильним терміном, ніж «претензії».

assignment – оцінка # завдання # *1.* визначений, запланований для виконання обсяг роботи # *2.* одиниця роботи, яку визначають користувачі і виконують обчислювальною машиною; одиниця системи операційної, що являє собою послідовність управляючих операторів, які визначають виконувані програми і використовувані ними дані # *3.* доручення # *4.* мета, ціль # див. evaluation, estimation, estimate.

associate – асоціювання # сполучення, з'єднання, від associo з'єдную) – сполучення, з'єднання чого-небудь в єдине ціле.

associate with another program – асоціація з іншою програмою # інтеграція коду програми з потенційно небезпечними наслідками або її частини в код іншої програми таким чином, щоб при деяких умовах керування передавалося на код програми з потенційно небезпечними наслідками.

association – асоціація # спільна взаємозалежність між викликами логічних об'єктів. Вона може здійснюватись шляхом обміну протокольною інформацією керування.

association for computing machinery – ассоціація з обчислювальної техніки # міжнародна науково-освітня асоціація з обчислювальної техніки , що була заснована в 1947 р. Є головною організацією для комітету SIGGRAPH і чотирьох десятків інших груп, що працюють за напрямками інтересів (наприклад, SIGGRAPH – комп'ютерна графіка; SIGPLAN – мови програмування; SIGOPS – операційні системи; SIGDA – автоматизація проектування і т.д.). Охоплює питання підвищення технічної компетентності фахівців у галузі комп'ютерних технологій, організовує й проводить конференції,

видає журнали й бюлетені за комп'ютерними технологіями, розробляє та просуває різноманітні стандарти у галузі IT. Публікує «рекомендації до викладання інформатики» в університетах (Computing Curricula).

association security state – стан захисту асоціації # стан захисту, що стосується об'єднання чи групи.

assurance – гарантія # див. guarantee.

assurance class – клас вимог гарантій беспеки # верхній рівень формальної структури вимог гарантій безпеки. Містить наступні елементи: назву класу; опис класу; розділи вимог гарантій беспеки. Вимоги розподілені на 7 класів вимог гарантій беспеки: керування проектом; дистрибуція; розробка; документація; процесу розробки; тестування; оцінка захисту.

assurance family – розділи вимог гарантій беспеки.

asymmetric communications – асиметричний обмін даними # засоби двостороннього обміну даними з об'ємом трафіку, що розрізняють, у різних напрямках # наприклад, телебачення за замовленням або супутниковий Інтернет (DirectPC або HTB-Internet).

asymmetric cryptography – криптографія із відкритим ключем # асиметрична криптографія # криптографія, в якій для шифрування та дешифрування застосовують відкритий ключ і відповідний приватний ключ # якщо для шифрування застосовують відкритий ключ, для розшифрування застосовують відповідний приватний ключ, і навпаки.

asymmetric cryptosystem – асиметрична криптосистема # криптосистема, у якоїключі зашифровування і розшифровування розрізняються таким чином, що за допомогою обчислень практично неможливо вивести один ключ з іншого.

asymmetric key cryptosystem – асиметрична криптосистема # криптосистема з відкритим ключем #

asynchronous – асинхронний # два або більше процесів, що не залежать від виникнення конкретних подій, таких як загальні сигнали синхронізації.

asynchronous data transmission – асинхронне передавання даних # метод передавання даних, за яким кожний символ передають з попереднім стартовим бітом (start bit) і наступним стоповим бітом (stop bit). Це дозволяє передавати символи через нерегулярні інтервали часу між ними. Має ряд переваг у випадках, коли передавання має нерегулярний характер.

asynchronous transfer mode – асинхронний режим перенесення інформації # орієнтований на з'єднання режим пакетного передавання, в якому інформація будь-якого типу передають в комірках, а потоки комірок від різних користувачів асинхронно мультиплексуються в спільному цифровому тракті.

asynchronous transmission – асинхронне пересилання # пересилання даних, за якого початок кожного символа або блока символів є довільним, але тільки після початку, час появи кожного елемента сигналу має таке саме відношення до значущих моментів фіксованої основи часу.

ATM – asynchronous transfer mode – асинхронний режим передавання.

ATM cell – **1.** комірка асинхронного режиму перенесення інформації # **2.** комірка АТМ # пакет фіксованої довжини (5 октетів заголовка і 48 – даних користувача), використовуваний в технології асинхронного режиму перенесення інформації.

attack – атака # спроби порушити безпеку комп'ютера, спроба знищити, розкрити, змінити, зробити недоступним, вкрасти або отримати несанкціонований доступ або несанкціоновано використовувати актив # наприклад зловмисна логіка, перехоплення інформації в лініях пересилання.

attack object – об’єкт атаки # сторона, яку атакують. В мережах обміну інформацією (МОІ) вона може бути представлена окремим комп’ютером (з інформацією, що зберігають й обробляють в ньому), сегментом МОІ або МОІ в цілому.

attack subject – суб’єкт атаки # сторона, що реалізовує атаку.

attack to network of exchange of information – атака на мережу обміну інформацією # реалізація загрози мережі обміну інформацією, що полягає в пошуку й використанні цієї чи іншої уразливості мережі.

attack upon request of the object – атака за умови запиту об’єкта # атака на віддалену мережу обміну інформацією, яку здійснюють суб’єктом атаки при умові одержання від потенційного об’єкта атаки запиту певного типу.

attack without feedback – атака без зворотного зв’язку # односпрямована атака # атака на віддалену мережу обміну інформацією , яку здійснюють внаслідок передачі на об’єкт атаки одиночних запитів, відповіді на які суб’єктові атаки не потрібні.

attacker – порушник # будь-яка особа, що навмисно використовує вразливості технічних і нетехнічних засобів керування безпекою з метою захоплення або компрометації інформаційних систем і мереж, або зниження приступності ресурсів інформаційної системи і мережних ресурсів для законних користувачів

attestation – атестація # *1.* авторитетне підтвердження відповідності продукту своєму призначенню # *2.* діяльність, спрямована на підтвердження відповідності об’єкта інформаційної діяльності вимогам державних стандартів, інших нормативних документів із захисту інформації, затвердженими державними органами із сертифікації в межах їхньої компетенції. А. дає право власнику об’єкта інформаційної діяльності обробляти

інформацію з рівнем секретності, що відповідає рівню безпеки інформації.

attribute – атрибут # *1.* елемент даних, який описує користувача або перелік розсилання і використаний для визначення цього користувача або переліку щодо фізичної або організаційної структури системи опрацювання повідомлень # *2.* поіменована властивість або характеристика сутності, відмінність якої, кількісно або якісно, від іншої може бути встановлено безпосередньо людиною або автоматизованими засобами # наприклад імена, адреси.

attribute class – клас атрибута # сукупність всіх можливих значень атрибута, які відповідають тій самій властивості екземплярів сутностей певного класу сутностей # наприкла назву стовпчика «таблиці співвідношення» можна розглядати як ім’я класу атрибута # клас атрибута має бути підмножиною відповідного домену атрибута.

attribute identifier – атрибутний ідентифікатор # ідентифікатор атрибута # засіб ідентифікації людей, допущених у контрольовану зону або до носіїв інформації, у вигляді певного атрибута: перепустка, жетон, будь-який інший документ на право допуску, картка ідентифікаційна. Основний недолік ідентифікатора атрибута – можливість попадання до сторонніх осіб, які можуть скористатися ними для протиправних дій.

AU – access unit – модуль доступу.

audio document – аудіальний документ # документ, що містить запис фонетичної інформації і призначений для звукового відтворення інформації. Наприклад, диск оптичний, магнітна стрічка із записаною інформацією і т. ін.

audio source – джерело звуку # будь-які явища, що викликають локальну зміну тиску або механічної напруги. Широко розповсюджені джерела звуку у вигляді твердих тіл, що коливаються (наприклад, дифузори гучномовців і мембрани телефонів, струни і деки музичних інструментів); в діапазоні ультразвукових хвиль це пластинки і стрижні з матеріалів п’єзоелектричних або матеріалів магнітострикційних. Цілий клас джерела звуку складають перетворювачі акустоелектричні.

audio-interception – аудіоперехоплення # метод добування інформації, що розповсюджують або відтворюють за допомогою акустичних хвиль. В залежності від місця встановлення акустоперетворюючих пристроїв, можна виділити два основні різновиди а.: аудіоперехоплення без заходу на об’єкт і аудіоперехоплення із заходом на об’єкт.

audio-interception with an approach to the object – аудіоперехоплення із заходом на об’єкт # аудіоперехоплення, здійснюване за допомогою пристроїв підслухування, встановлених в апаратуру засобів оброблення інформації, в різноманітні технічні пристрої, на

проводові комунікаційні лінії (радіо, телефон, телевізійний кабель, охоронно-пожежної сигналізації і т. ін.), а також в різноманітні конструкції інженерно-технічних споруд і побутових предметів, що знаходяться на об'єкті, з метою перехоплення розмов працюючого персоналу і звукових сигналів технічних пристроїв.

audio-interception without access to the object – аудіоперехоплення без заходу на об'єкт # аудіоперехоплення, яке здійснюють за допомогою акустичних та вібраційних датчиків знімання інформації, що встановлюються на інженерно-технічні конструкції, які знаходяться за межами об'єкта (приміщення), з якого необхідно приймати мовні сигнали. Часто для а. використовують мікрофони спрямовані, мікрофони лазерні тощо, призначені для дистанційного знімання мовної інформації через наскрізні отвори (двері, вікна, кватирки, сміттє- і повітропроводи і т. ін.) і віконне (автомобільне) скло.

audio-visual document – аудіовізуальний документ # документ, що містить одночасно запис звуку та видимого зображення і призначений для аудіовізуального повідомлення. Наприклад, кінострічка.

audit – **1.** аудит # аналіз процедур # систематичний, незалежний та задокументований процес для отримання доказів аудиту та об'єктивного його зіставлення для визначення ступеня виконання критеріїв аудиту # аудит може бути внутрішнім аудитом (перша сторона) або зовнішнім аудитом (друга чи третя сторона), а також він може бути комбінованим аудитом (поєднання двох чи більше дисциплін) # див. security audit.

audit journal – контрольний журнал # журнал, в якому реєструються події, що мають відношення до забезпечення безпеки обчислювальної системи, зокрема, звернення до захищених даних. Перегляд цього журналу дозволяє виявити спроби доступу несанкціонованого і ідентифікувати осіб, які роблять такі спроби.

audit logging – ведення аудиту # фіксування даних про події, пов'язані з інформаційною безпекою, з метою перевірки, аналізу і постійного моніторингу.

audit sample – аудиторська вибірка # в обчислювальній техніці – множина зроблених у хронологічному порядкові реєстраційних записів про події, пов'язані із зміною стану системи обчислювальної.

audit scope – 1. сфера застосування аудиту # 2. область аудиту # обсяг та межі аудиту.

audit tools – засоби аудиту # автоматизовані інструментальні засоби, що допомагають аналізувати зміст журналів аудиту.

audit trail – **1.** контрольна позначка # **2.** дані трасування # дані, зібрані для потенційного використання під час перевірки безпеки # див. security

audit trail # **3.** контрольний журнал # запис діяльності, яку здійснюють в інформаційній системі за певний період часу.

authentic – автентичний # дійсний, вірний, такий, що ґрунтують на першоджерелі.

authentication – автентифікація # *1.* перевірка щодо належності суб'єктові доступу пред'явленого ним ідентифікатора; процес установлення достовірності ідентифікаційної інформації # *2.* процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єктові; установлення або підтвердження автентичності.

authentication code – код автентифікації # контрольне поле, що додають до блока даних для автентифікації повідомлень. Прикладом коду автентифікації є код автентифікації повідомлень (MAC).

authentication exchange – обмін автентифікацією # *1.* двохсторонні переговори між двома системами щодо виконання процесу аутентифікації # прикладом методів обміну аутентифікації є розширюваний протокол автентифікації (EAP) і проста автентифікація та рівень безпеки (SASL) # *2.* механізм призначений для забезпечення ідентичності об'єкта через інформаційний обмін.

authentication factor – фактори автентифікації # частина інформації та/або процесу, що застосовують для перевірки автентичності або перевірки ідентичності об'єкта # фактори автентифікації поділяються на чотири категорії: ті, які об'єкт має (наприклад, підпис пристрою, паспорт, апаратний пристрій, що містить повноваження (credential), особистий ключ); ті, які об'єкт знає (наприклад, пароль, PIN-код); ті, які є частиною об'єкта (наприклад, біометричні характеристики); або ті, які об'єкт, як правило, робить (наприклад, зразок поведінки).

authentication information – інформація для автентифікації # інформація, яку застосовують для встановлення обґрунтованості заявленої ідентичності суб'єкта.

authentication procedure in telecommunication systems – процедура автентифікації в телекомунікаційних системах # процедура, призначена для захисту при передаванні в мережі паролів, автентифікаторів логічних об'єктів і т.ін. Для цього використовуються криптографічні методи і протоколи, засновані, наприклад, на процедурі "трикратного рукостискання". Метою таких протоколів є захист від установлення з'єднання з логічним об'єктом, утвореним порушником або діючим під його керуванням з метою імітації роботи справжнього об'єкта.

authentication process – процес аутентифікації # криптографічні операції і пакети даних для підтримки, які виконують фактичну перевірку автентифікації.

authentication protocol – протокол автентифікації # визначає послідовність повідомлень між об'єктом і верифікатором, що дозволяє верифікатору виконати автентифікацію об'єкта.

authentication, authorization and accounting server – сервер автентифікування, санкціонування та обліку # сервер, який забезпечує автентифікування користувача, санкціонування його доступу до мережі та облік навантаження для нарахування плати.

authenticator – автентифікатор # об'єкт, який полегшує ідентифікацію інших пристроїв, приєднаних до тієї ж локальної мережі

authenticity – автентичність # властивість, що об’єкт саме той, яким себе заявляє.

authenticity – автентичність # властивість, що об’єкт саме той, яким себе заявляє

author’s right – авторське право # див. copyright.

authoritative source – достовірне джерело # сховище, яке визнають як джерело точної та актуальної інформації.

authority – влада # *1.* здатність, право і можливість розпоряджатися будь-ким, будь- чим, здійснювати вирішальний вплив на долі, поведінку і діяльність, мораль і традиції людей за допомогою різного роду засобів – закону, права, авторитету, волі, суду, примусу # *2.* політичне панування над людьми, їхніми спільнотами, організаціями, над країнами і їхніми угрупованнями # *3.* система державних органів # *4.* особи, органи, наділені відповідними державними, адміністративними повноваженнями.

authority setting matrix – матриця встановлення повноважень # матриця, утворена в захищеній ділянці пам’яті системи обчислювальної, елементами якої є біти, що відповідають певним діям, які можуть бути виконані з термінала при зверненні до елемента даних. Якщо необхідно, то елементи матриці можуть містити і покажчик на відповідні процедури. Ці процедури виконуються при кожній спробі доступу з даного термінала до заданого елемента даних і можуть обмежувати доступ до інформації в залежності від певних умов.

authorization – авторизація # *1.* надання сутності офіційної санкції робити щось або бути чимось # *2.* повноваження # установлення відповідності між повідомленням (пасивним об’єктом) і його джерелом (користувачем або процесом, що його створили) # *3.* гарантоване надання привілею доступу програмам, користувачам або процесам, засноване на правах доступу.

authorization user rejection – відмова в доступі законному користувачеві # загроза, яка полягає у відмові системи захисту надання доступу до ресурсів інформаційно-обчислювальної системи

користувачеві, який має на це законне право.

authorized access to information – санкціонований доступ до інформації # доступ до інформації, під час якого не порушуються встановлені правові норми і порядок його здійснення (правила розмежування доступу).

authorized user – авторизований користувач # користувач, що володіє певними повноваженнями.

authorized user – зареєстрований користувач # 1. користувач обчислювальної системи, який має пріоритетний номер в даній системі колективного користування # 2. користувач, включений в графік роботи на ЕОМ.

authorized user – привілейований користувач # авторизований користувач # див. privileged user.

automated radio control complex – автоматизований комплекс радіоконтролю # апаратно-програмний комплекс на основі приймачів скануючих і ПЕОМ, призначений для швидкого панорамного аналізу радіочастотного спектра в діапазоні частот.

automatic calling – автоматичний виклик # виклик, в якому елементи сигналу вибору вводяться в мережу пересилання даних в неперервній послідовності на повній швидкості пересилання даних # сигнал вибору генерують термінальним обладнанням даних. Обмеження може бути накладено критеріями проектування мережі, щоб запобігти більш ніж допустимої кількості спроб виклику до тієї самої адреси протягом певного періоду часу.

automatic check – автоматичний контроль # контроль, що виконують автоматично апаратними засобами.

automatic check – апаратний контроль # функційний контроль, що здійснюють за допомогою апаратних засобів. Виявляє збої або несправності безпосередньо у момент їхнього виникнення. В автоматизованих системах досягається методами контролю по модулю, дублюванням обладнання і т. ін.

automatic function – автоматична функція # машинна функція (службова кодова комбінація) або серія машинних функцій, що контролюються програмою і виконуються без допомоги оператора.

automatic speech recognition – автоматичне розпізнавання мови # сприйняття та аналіз, функційним модулем, інформації, пересланої людським голосом # розпізнавана інформація, може бути словом у визначеній послідовності слів, фонемою заздалегідь визначеної мови, а іноді й ідентичністю людини через її голосові особливості.

automatic speech recognition – автоматичне розпізнавання мовлення # перетворення, функційним модулем, мовленевого сигналу в подання контенту мови # контент для розпізнавання може бути виражений як правильна послідовність слів або фонем.

automatic switching – автоматичне комутувуання # комутація каналів або пакетів в мережі обчислювальній, яка здійснюється автоматично приладами зв'язку у відповідності з одержаною адресною інформацією.

automation – автоматизація # *1.* упровадження автоматичних засобів для реалізації процесів; система заходів, спрямованих на підвищення продуктивності праці людини через заміну частини цієї праці роботою машин. Базують на використанні сучасних засобів обчислювальної техніки і наукових методів та реалізують за допомогою різноманітних систем автоматичних і автоматизованих # *2.* автоматизація процесу оброблення конфіденційної інформації – забезпечення адекватної реалізації у системі комп'ютерній схеми потоків інформаційних і правил керування ними, які існували до застосування комп'ютерних засобів оброблення інформації. Здійснюють послідовним виконанням наступних дій: визначення формального механізму, що адекватно визначає задану схему інформаційних потоків і правила керування ними; побудова моделі безпеки, що відображає заданий порядок оброблення інформації, і, можливо, формальний доказ її безпеки; реалізація системи оброблення інформації у відповідності з пропонованою моделлю; доказ гарантій можливих в автоматизованій системі потоків інформації і правил розмежування доступу вихідній схемі інформаційних потоків і правил керування ними.

availability – **1.** готовність # доступність # надійність # ремонтопридатність та готовність # здатнічть функційного модуля перебувати в стані для виконання потрібної функції за певних умов у заданий момент часу або протягом заданого інтервалу часу, за умови, що надаються необхідні зовнішні ресурси # готовність, що визначають у цьому словнику є внутрішньою готовністю, де зовнішні ресурси крім ресурсів на технічне обслуговування не впливає на доступність функційного модулю, експлуатаційна готовність, з іншого боку, вимагає забезпечення зовнішніми ресурсами # **2.** доступність # *1.* можливість проникнення куди-небудь # *2.* властивість ресурсу системи (комп'ютерної системи, послуги, об'єкта комп'ютерної системи, інформації), яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

awareness rate criterion – показник інформованості # інтегральний показник, що відображає повноту і

достовірність всієї інформації, необхідної для оцінки обстановки.

B

backbone – високошвидкісна мережна магістраль.

backbone network – мережа магістральних ліній зв’язку # у комп'ютерній мережі, підмережа, що з'єднує кінцеві вузли або інші підмережі і характеризує високошвидкісне обмінювання даними.

backing storage – зовнішня пам’ять # пристрій запам’ятовуючий на магнітних дисках, магнітних стрічках або дисках оптичних, призначений для довготривалого зберігання інформації.

backup – резервна копія # стосується процедур, технік або апаратних засобів, що їх застосовують для відновлювання втрачених або зруйнованих даних, або для збереження робочого стану системи.

backup file – резервна копія файлу # файл зробленій для можливого подальшого відновлювання даних # наприклад копія файлу, що збережена на альтернативному сайті.

backup procedure – процедура резервного копіювання # процедура для забезпечення відновлювання даних у разі збою (відмови) або катастрофи # наприклад створення резервних копій файлів.

backward channel – зворотний канал # канал пересилання, пов'язаний з прямим каналом, але з протилежним напрямком пересилання, застосовують для сигналів диспетчерського керування або контролю помилок # у випадку одночасної пересилання даних в обох напрямках, це визначення застосовують щодо джерела даних під час розгляді.

backward LAN channel – зворотний канал ЛМ # в широкосмуговій локальній мережі, канал, призначений для пересилання даних від станцій пересилання даних до головного вузла.

backward recovery – зворотне відновлювання # відновлювання даних більш ранньої версії з використанням даних більш пізньої версії й тих, що записані в журналі.

backward recovery – зворотне відновлювання) # (комп’ютерне програмування вид відновлювання, в якому систему, програму, файл, базу даних, або інший ресурс відновлюють до попереднього стану, в якому можуть виконувати необхідні функції # наприклад відновлювання файлу до заданого стану, за допомогою зміни (повернення) всіх змін, внесених до файлу, оскільки вони були раніше в цьому стані.

bacterium – бактерія # мікроб # (різновид комп’ютерного вірусу) програма, яка поширює себе електронною поштою всім у списку розсилки для кожного отримувача.

Bad-Guy – зловмисник # див. abuser, badguy, intruder.

bad sectoring – дефектна розмітка # методика для захисту від

копіювання, коли дефектні сектори навмисно записані на диску.

badguy – зловмисник # див. abuser, Bad-Guy, intruder.

balanced cable – симетричний кабель # кабель, у якого провідники (жили) виконані з проводу однакового діаметра, мають однакову ізоляцію і розташовані так, що між ними можна провести площину симетрії.

balanced code – збалансований код # код в цифровій лінії передавання, в якому сума значень n рівнів сигналу має скінченні значення.

balanced error – зскомпенсована помилка # помилка,середнє значення множини помилок якої дорівнює нулю, урівноважені помилки, середнє значення множини яких дорівнює нулю.

band – **1.** діапазон # *1.* звуковий обсяг голосу, музичного інструмента, звукоряду, мелодії тощо # *2.* смуга частот (довжин радіохвиль), на яких здійснюється радіоприйом або радіопередача # *3.* межі зміни деякого параметра # **2.** смуга # 1. група доріжок на магнітному барабані або на магнітному диску, всі з яких зчитуються або записуються паралельно # 2. довга вузька частина якого-небудь простору.

bandwidth– діапазон # див. band, range.

bank – банк # *1.* особливий економічний інститут, що акумулює тимчасово вільні кошти, надає кредит, здійснює грошові розрахунки, випускає в обіг гроші, цінні папери # *2.* сукупність однотипних елементів, засобів або пристроїв, взаємно з'єднаних і спільно використовуваних. Наприклад, банк даних — сукупність баз даних і системи керування ними; банк пам'яті – сукупність елементів основної пам'яті в мультипроцесорній ЕОМ; банк програм – сукупність програм.

bar code – штрих-код # код, який представляє символи за допомогою наборів паралельних штрихів різної товщини і розділення, які зчитуються за допомогою оптично поперечного сканування.

base – основа системи числення # в системі числення, число, яке зведено в ступінь, позначають через показник, а потім, помножене на мантису, щоб визначити представлене число # наприклад число 10 у виразі $3{,}15 \times 10^3 = 3150$.

base – основи # найважливіші вихідні положення чого-небудь (науки, теорії і т. ін.).

base computer – базовий комп'ютер # основний (вихідний) комп'ютер сімейства ЕОМ. Решта машин даного сімейства є розвитком базового.

base measure – **1.** базовий показник # показник, визначений в термінах атрибута, та методика отримання його кількісних характеристик. Базовий показник функційно не залежить від інших показників # **2.** основна міра # міра, встановлена відносно атрибута і методу його кількісної оцінки # основна одиниця виміру не є функцією інших одиниць виміру.

base station system GPRS protocol – протокол GPRS системи базових станцій # протокол в інтерфейсі Gb, який забезпечує обмін інформацією керування радіоланкою і доступом до середовища між підсистемою базових станцій BSS (Base Station Subsystem) та обслуговуючим вузлом підтримки служби GPRS (SGSN).

basic – основи # див. base, principle, ground, foundation, fundament, law.

batch processing – пакетне опрацювання # опрацювання даних або виконання завдань, накопичених заздалегідь, таким чином, що користувач не може далі вплинути на їх обробку під час його виконання.

baud – бод # одиниця швидкості модуляції, що дорівнює числу елементів сигнала в секунду, де всі ці елементи мають однакову довжину, і кожен елемент являє собою один або більше бітів # для деяких модемів, що працюють на частоті 1200 біт/с або вище, швидкість модуляції, виражена в бодах, зазвичай менша, ніж швидкість пересилання бітів, оскільки для кожного елемента сигналу передано більше одного біта.

Baudot code – код Бодо # п'ятиелементний код, призначений для передавання букв, цифр і інших знаків по каналах зв'язку телеграфного.

beaconing station – станція аварійної сигналізації # станція пересилання даних в кільцевій мережі, що повідомляє про серйозні збої в сусідніх станціях.

before-image – початковий образ; прообраз # копію блока або запису перед модифікацією.

behaviour – поведінка # система взаємозв'язаних реакцій, що здійснюється живими організмами для пристосування до середовища. Поведінка тварин і людини вивчається етологією, психологією, соціологією.

Bell-LaPadula model – модель Белла-Лападула # формальна автоматна модель політики безпеки, що описує множину правил керування доступом. В цій моделі компоненти системи розподіляються на об'єкти і суб'єкти доступу. Вводиться поняття безпечного стану і доводиться, що коли кожний перехід зберігає безпечний стан (тобто переводить систему з безпечного стану в безпечний), то згідно з принципом індукції система є безпечною.

BER – bit error ratioкоефіцієнт помилкових бітів # частота помилкових бітів.

best effort service – **1.** обслуговування з негарантованою якістю # **2.** обслуговування з максимально можливим зусиллям # найнижчий клас обслуговування, за якого якість залежить від поточних вільних ресурсів мережі і може погіршуватися при встановленні інших з'єднань.

between-the-lines entry – несанкціонований доступ до тимчасово відключеного абонентського терміналу # доступ, отриманий за допомогою активного

перехоплювання неавторизованим користувачем лінії, до миттєво неактивного каналу пересилання, під'єднаного до ресурсу законного користувача.

BGP – border gateway protocol – протокол граничного шлюзу.

bias – зміщення # систематичне відхилення значення величини від контрольного значення.

bias error – систематична помилка зміщення # помилка внаслідок зсуву # наприклад помилка, спричинена скороченням вимірювальної стрічки # наприклад в обчисленнях, помилка викликана урізанням.

biliary encoding – двійкове кодування # 1. процес подання символів алфавіту у вигляді ланцюжка двійкових знаків # 2. кодування числа у вигляді двійкового ланцюжка, в якому і-тий біт, починаючи з кінця, має вагу *2*.

binary code – двійковий код # код з основою *2*. Алфавітом коду є цифри 0 і *1*. Використовується для подання даних в ЕОМ.

binary code information exchange – двійковий код обмінювання інформацією # двійковий восьмибітовий, призначений для внутрішнього оброблення і вводу-виводу символьних даних.

binary decimal code – двійково-десятковий код # представлення чисел, при якому кожна десяткова цифра записується чотирьохбітовим двійковим еквівалентом. Використовується для операцій над цілими числами великої розрядності.

binary digit – двійковий розряд # двійкова позиція # кожна з цифр 0 або 1, під час використанні в двійковій системі.

binary error-correction code – двійковий код з виправленням помилок # код двійковий, надмірність якого забезпечує автоматичне виявлення і виправлення помилок деяких типів в даних, що передаються.

binary error-detecting code – двійковий код з виявленням помилок # код двійковий, надмірність якого забезпечує автоматичне виявлення помилок деяких типів в даних, що передаються.

binary-to-decimal notation – двійково-десяткове кодування # спосіб кодування десяткових чисел, при якому кожна цифра представляється чотирма двійковими розрядами (двійковою тетрадою).

bind – прив'язка # 1.відношення ідентифікатора до іншого об'єкта в програмі # наприклад зв'язати ідентифікатор зі значенням, адресою або інший ідентифікатором, або зв'язати формальні параметри й фактичні параметри # прив'язування # 2. співставлення абсолютної адреси, віртуальної адреси або ідентифікатора обладнання з символічною адресою або міткою в комп'ютерній програмі.

binding – зв'язування # процес співвіднесення ідентифікатора до іншого об'єкту в програмі# див: cryptographic binding.

binding time – час зв'язування # момент часу, в який відбувається зв'язування # мови програмування, призначені як для ефективного виконання, так і для гнучкості, такі як Ada, PL/I та C++, передбачають кілька опцій, що дозволяють обирати час зв'язування.

biometric – **1.** біометричний # стосується використання конкретних атрибутів, які відображають унікальні характеристики особи, такі як відбитки пальців, зразок кровоносних судин ока, або зразок голосу, для перевірки ідентифікаційних даних людини # **2.** біометрія # технологія вимірювання й аналізу людського тіла з метою його автентифікації.

biometric identifier – біометричний ідентифікатор # сіб ідентифікації людей, допущених у зону контрольовану або до носіїв інформації, що використовує інформативні пізнавальні ознаки конкретної людини. У пристроях біометричної ідентифікації використовуються: рисунок капілярних ліній пальців; узори сітківки очей; геометрія руки; динаміка підпису; особливості мови; ритм роботи з клавіатурою. У зв’язку з цим можна виділити наступні біометричні ідентифікатори: пристрій ідентифікації особистості за рисунком капілярних ліній пальця; пристрій ідентифікації особистості за узорами сітківки очей; пристрій ідентифікації особистості за геометрією руки; пристрій ідентифікації особистості за динамікою підпису; пристрій ідентифікації особистості за голосом і т.ін. Біометричні ідентифікатори, забезпечуючи низьку ймовірність помилкової ідентифікації, мають гірші, порівняно з ідентифікаційними картками, показники правильної ідентифікації (упізнавання «своїх»), низьку надійність роботи, високу вартість. При покращенні експлуатаційних характеристик б. і. слід очікувати на їхнє широке застосування в різноманітних системах (комплексах) керування доступом.

biometrical authentication – біометрична автентифікація # методи автентифікації, які засновані на використанні унікальних біологічних характеристик об’єкта. в якості таких характеристик можуть бути використані: відбиток пальця, геометрія обличчя, геометрія руки, сітчатка ока тощо.

bit – біт # двійковий розряд # двійкова позиція # кожна з цифр 0 або 1, під час використанні в двійковій системі.

bit density – щільність бітів # міра кількості бітів, записаних на одиницю довжини або площі.

bit error rate – коефіцієнт помилкових бітів # частота помилкових бітів # кількість помилкових бітів, розділених на загальну кількість бітів, переданих, отриманих або оброблених протягом деякого встановленого періоду часу.

bit pattern – комбінація розрядів # сукупність двійкових розрядів, що

створюють кодову комбінацію або маску.

bit position – позиція біту # позиція символа в слові, коли воно представлено в двійковій нотації.

bit rate – швидкість пересилання бітів # швидкість, з якою передаються біти # швидкість пересилання бітів зазвичай виражають у бітах в секунду, кілобітах в секунду, мегабітах в секунду і т.д.

bit string – рядок бітів # послідовність, яку складено винятково з бітів.

bit-oriented protocol – біт-орієнтований протокол # протокол каналу пересилання, в якому функції керування каналом пересилання даних визначені в конкретних положеннях кадру, що дає змогу передавати дані користувача у вигляді явної послідовності біт # наприклад високорівневий протокол керування каналом пересилання даних.

black data – зашифровані дані # див. enciphered data, cryptographically protected data.

blank – пробіл # символ, який є порожньою позицією в рядку графічних символів # пробіл концептуально відрізняють від символа пробілу, але не може диференціюватися у певному наборі символів # наприклад, деякі набори символів містять пробіл як «нерозривний пробіл», який може застосовуватися між двома графічними символами, без опрацювання його як роздільника.

blank character – знак або символ пробілу # символ, який є порожньою позицією в рядку графічних символів # наприклад, деякі набори символів містять пробіл як «нерозривний пробіл», який може застосовуватися між двома графічними символами, без опрацювання його як роздільника.

blank medium – порожній носій # інформаційний носій даних в якому або на якому не було зареєстровано ні знаків посилань, ні даних користувача.

blind copy recipient – отримувач сліпої копії # закритий отримувач # отримувач, ідентифікаційні дані якого не мажна розголошувати іншим отримувачам того самого повідомлення # скорочення «bcc» застосовуване для позначення отримувача сліпої копії, утворене з англійського виразу «blind carbon copy».

blind copy recipient – отримувач сліпої копії # отримувач, ідентифікаційні дані якого не мають розголошуватися іншим отримувачам того ж самого повідомлення.

blind digital signature – сліпий цифровий підпис # підпис цифровий, при якому абонент, що підписує, не може встановити тотожність між підписаними даними та будь-якими характеристиками процесу підпису цих даних (наприклад, часом, коли цей процес підпису відбувався). На час підпису абонент, що підписує, не має доступу до змісту даних, які він підписує.

block – блок # *1.* сукупність взаємопов'язаних елементів та вузлів пристрою, що виконують певну функцію # *2.* фізичний запис на носії даних # *3.* сукупність даних, що передаються по лінії зв'язку # 4. рядок символів, слів чи записів, які розглядають як єдине ціле для цієї мети.

block check – перевірка блока # частина процедури контролю помилок, що застосовуються для визначення чи структурований блок даних відповідно до заданих правил.

block cipher modes of operation – режим блочних шифрів # варіанти застосування блочного шифру до відкритого тексту, довжина якого більше довжини блока. Найпростіший варіант – відкритий текст розбивають на блоки та шифрують кожний блок окремо. Такий режим іменується режимом електронної кодової книги (Electronic Codebook) (як в DES) або режимом звичайної заміни. Однак цей режим в багатьох практичних застосуваннях має істотні недоліки, пов'язані, наприклад, з тим що однакові блоки відкритого тексту шифруються однаково, незалежно від положення блоків в цілому тексті. Це обумовлює використання таких режимів як режим зчеплення блоків (Cipher Block Chaining), режим шифрування зі зворотним зв'язком за криптотекстом (Cipher Feedbback) та режим шифрування зі зворотним зв'язком за виходом (Output Feedback). Застосування різних режимів блочних шифрів викликане передусім можливістю застосування цих криптографічних примітивів для побудови кодів автентифікації повідомлень, генераторів псевдовипадкових послідовностей, шифрів потокових.

block coding – блочне кодування # спосіб кодування, при якому кожний блок, що передається, кодується окремо.

block encryption – блочне шифрування # спосіб шифрування, при якому кожний блок, що передається, шифрується незалежно.

blockade – блокада # воєнна, політична або економічна ізоляція чи оточення держави (або частини її, групи держав, їхніх збройних сил), насильницьке порушення її зовнішніх зв'язків із метою змусити виконати вимоги організаторів б.

blocked – заблокований # стосується стану задачі виконуваної задачі, в якому задачу затримують або вона очікує події.

blocking – блокування # *1.* ізоляція будь-якого об'єкта з метою наступного його знищення або захоплення при веденні бойових дій тактичного масштабу # *2.* Заборона на виконання наступних операцій до завершення поточної операції; механізм організації контрольованого доступу до спільно використовуваного ресурсу.

blocking for information – блокування інформації # унеможливлення санкціонованого доступу до інформації.

bodies – орган # див. agency.

Boolean expression – булевий вираз # буловий вираз # мовна конструкція, яка визначає обчислення логікового значення.

boot – завантажування комп'ютера # запуск комп'ютера за допомогою завантаження операційної системи і, можливо, очищення пам'яті.

boot virus – завантажувальний вірус # вірус комп’ютерний, призначений для ураження завантажувальних секторів машинної пам’яті. Зараження в. з. відбувається при завантажуванні комп’ютера з носія машинної інформації, що містить вірус. Зараження може відбутися як випадково, наприклад, користувач сам, не підозрюючи про наявність вірусу на носії, запустив його в комп’ютерну систему, так і навмисно, якщо зловмисник (злочинець) знав про його існування і наслідки, які настануть після запуску системи з вірусоносієм. Носій машинної інформації може і не бути системним, тобто не мати файлів операційної системи.

bootstrap – початкове завантажування # коротка програма, яка постійно наявна чи її легко завантажити в комп'ютер, і чиє виконання призводить до завантажування в пам'ять більшої програми, такої як операційна система або її завантажувач.

bootstrap – самозавантажування # виконання початкового завантажування.

bootstrap loader – програма початкового завантажування # коротка програма, яку застосовують для завантажування початкового завантажування.

border gateway protocol – протокол граничного шлюзу # протокол взаємодії різних адміністративних доменів, наприклад, служби GPRS пакетного радіопередавання та мережі обміну даними загального користування.

bottom-up – висхідний # стосується методу або процедури, що починають на найнижчому рівні абстракції і доходить до найвищого рівня.

boundary protection – захист границь # використання обмежувальних регістрів (регістрів захисту пам’яті) для захисту ресурсів комп’ютера.

BPL – broadband power line – широкосмугова лінія електропередавання.

brandmaurer – брандмауер # *1.* вогнестійка капітальна стіна, що запобігає поширенню пожежі # *2.* метод (або принцип) захисту надійної мережі від загроз, що надходять від інших (менш надійних) мереж чи систем, за допомогою централізації доступу до мережі та контролю за ним апаратно-програмними засобами. Цей принцип захисту можна реалізувати за допомогою різних засобів таких як фільтруючий маршрутизатор, міжмережний екран, бастіонний вузол, подвійний шлюз, фільтруючий шлюз, проксі-шлюз, комбінований

шлюз, ізольована підмережа, тощо. Іноді термін брандмауер використовують як синонім файерволу.

BRAS – broadband remote access server – сервер віддаленого широкосмугового доступу.

breach – злам # проникнення # обхід або виведення з ладу будь-якого елемента комп'ютерної безпеки, з виявленням або без, що може призвести до проникнення в систему опрацювання даних.

breakpoint – точка переривання # контрольна точка # точка, в програмі, модулі або операторі, де виконання може бути припинено залежно від конкретної умови або події # точка переривання встановлюються для забезпечення ручного або автоматичного моніторингу продуктивності програми або результатів, може бути більше однієї точки переривання.

bridge – міст # пристрій рівня канального моделі ISO/OSI, який дозволяє з'єднувати між собою пристрої в різних мережах обчислювальних локальних. Міст не залежать від типу протоколу, але визначаються використовуваним обладнанням. Вони можуть з'єднувати мережі з різними протоколами і різними типами обладнання. Прикладом м. є пристрій, що з'єднує мережі Ethernet і TokenRing. Присутність м. для користувачів невидима (на відміну від шлюзів). Мости бувають двох типів: мости локальні і мости віддалені. Міст працює аналогічно як маршрутизатор, різниця тільки в тому, що м. встановлює з'єднання на канальному рівні, а маршрутизатор – на мережному.

broadband – широкосмуговий канал # смуга частот, яку застосовують для застосунку, що вимагає широкого діапазону частот # широкосмуговий канал може бути розділений на кілька більш вузьких смуг, кожна з яких може бути використана для різних цілей, або бути доступною для різних користувачів.

broadband remote access server – сервер віддаленого широкосмугового доступу # сервер (вузол опорної мережі), який забезпечує автентифікацію віддалених користувачів широкосмугового доступу, санкціонує їх доступ, формує політику їх обслуговування, агрегує навантаження та здійснює облік надаваних сервісів.

broadcast – мовлення # 1. спілкування людей за допомогою мови; мовна діяльність # 2. передавання повідомлень по радіо, телебаченню.

broadcast connection – широкомовне з'єднання # з'єднання, яке забезпечує односпрямований розподіл інформації від центрального джерела до необмеженої кількості санкціонованих приймачів.

broadcasting receiver dynamic range – динамічний діапазон радіоприймача # величина, яка характеризує можливості приймача приймати радіосигнали різної потужності. Оцінюється логарифмом відношення

максимального рівня потужності сигналу, що приймається, до його мінімального рівня. Для підвищення динамічного діапазону радіоприймача застосовується пристрій автоматичного регулювання підсилення приймального тракту, який змінює його коефіцієнт підсилення у відповідності до рівня сигналу, що приймається.

brute force attack – силова криптоаналітична атака # криптоаналітична атака, яка проводиться шляхом повного перебирання всіх можливих ключів у кріпи осіістсмі.

brute-force attack – атака перебором # спроба порушити комп'ютерну безпеку, намагаючись отримати можливі значення паролів або ключів методом підбору # відмінна від аналітичної атаки.

BSSGP – base station system GPRS protocol – протокол GPRS системи базових станцій.

B-tree – B-дерево # версія збалансованого дерева, де всі шляхи просування від кореневого вузла до кінцевого вузла мають однакову довжину # B-дерево має такі властивості, де n порядок B-дерева: a) кожен вузол містить не більше 2n елементів; b) кожен вузол, за винятком кореневого вузла, містить щонайменше n елементів; c) кожен вузол є або кінцевим вузлом, або він має m+1 підлеглих вузлів, де m його кількість елементів. B-дерева застосовують для швидкого доступу до даних на зовнішньому накопичувачі. Кількість звернень до кожного елемента даних є [менше або дорівнює] log[нижній індекс n+1] (m)

bug – закладка # див. secret intelligence device.

bug seeding – підсівання несправностей # процес навмисного додавання відомих несправностей у програму з метою моніторингу швидкості виявлення, видалення та оцінювання кількості невідомих несправностей, що залишилися в програмі.

bug [dictophone] detection – виявлення працюючого диктофону # установлення факту несанкціонованого (прихованого) запису мовної інформації на диктофон. Враховуючи конструктивні особливості диктофонів, призначених для прихованого запису, вони можуть бути виявлені за допомогою металодетекторів, або із застосуванням спеціальних виявників шляхом виявлення і аналізу змін параметрів полів, вимірюваних в місці розташування зловмисника. Накопичуючи зміни, є можливість виділити регулярне поле двигуна диктофона на фоні навіть більш потужних випадкових полів інших джерел.

built-in check – вбудований контроль # автоматичний контроль # див. automatic check.

built-in-programmed check – програмно-апаратний контроль # контроль функціонування ЕОМ, який

виконується як програмними, так і апаратними засобами.

burn in – 1. випробування на примусову відмову # процес підвищення надійності нового або оновленого функційного блока, що піддають відновленню за допомогою його експлуатації в заданому середовищі, для виявлення якнайбільш ранніх помилок, а також усунення їх за допомогою коригуючого технічного обслуговування # 2. відбраковування # скринінговий тест, що застосовує функційну експлуатацію неповторюваного функційного модуля # ккринінговий тест призначений для виявлення і видалення дефектних функційних модулів або тих, що можуть проявляти помилки на ранніх етапах.

byte – байт # рядок, складений з кількох бітів, що розглядають як єдине ціле і зазвичай подають символ або частину символа # кількість бітів у байті фіксовано для конкретної системи опрацювання даних # кількість бітів у байті зазвичай становить 8.

C

CA – certification authority – центр [орган] сертифікації # CA абревіатура також застосовується для безпечної асоціативної зв'язності (Connectivity Association).

cable – кабель # один або кілька ізольованих дротів, вміщених у захисну оболонку. Застосовують для передавання електроенергії, звукових, радіо та телевізійних сигналів на великі віддалі тощо.

cable communication line – кабельна лінія зв'язку # лінія зв'язку проводова, основним елементом якої є кабель (симетричний або коаксіальний). Кабельні лінії зв'язку поділяються на підземні, підводні та військово-польові.

calculation process – обчислювальний процес # процес вирішення різноманітних задач на ЕОМ.

call server – сервер викликів # об'єкт мережі, який виконує функції керування викликами у розподіленій пакетній системі комутації.

called-address – адреса викликаного # параметр, що може бути наявним у примітивах запиту сервісу або індикації і який ідентифікує адресу одержувача. У визначенні сервісу конкретного рівня такий параметр може називатися або «адреса викликаного», або «адреса отримувача».

calling-address – адреса викликаючого # параметр, що може бути наявним у примітивах запиту сервісу або індикації і який ідентифікує адресу ініціатора. У визначенні сервісу конкретного рівня такий параметр може називатися або «адреса викликаючого», або «адреса відправника».

camera – апарат # див. apparatus.

camera-recorder – відеокамера # пристрій для перетворення зображення у відеосигнал.

canadian trusted computer product evaluation criterion – канадські

критерії безпеки комп’ютерних систем # національний стандарт інформаційної безпеки, розроблений Центром безпеки відомства безпеки зв’язку Канади (Canadian System Security Centre Communication Security Establishment) в 90 роках. «Канадські критерії» використовуються для розроблення вимог безпеки, специфікацій засобів захисту й сертифікації програмного забезпечення робочих станцій, багатопроцесорних обчислювальних систем, персональних і багатокористувальницьких операційних систем, систем керування базами даних, розподілених, мережіпїх. вбудованих, проблемно-орієнтованих та інших систем. В «канадських критеріях» пропонується оригінальний підхід до опису взаємодії користувачів з комп’ютерною системою, інваріантний по відношенню до політики безпеки. Усі компоненти системи, що знаходяться під керуванням ядра безпеки, називаються об’єктами. Об’єкти можуть знаходитися в одному з наступних трьох станів: об’єкт-користувач, об’єкт-процес, пасивний об’єкт, і в залежності від стану, позначають користувачів, процеси й об’єкти відповідно. При описі критеріїв конфіденційності і цілісності (довільного й нормативного керування доступом і цілісністю) в «канадських критеріях» використовується поняття тег. У критеріях застосований дуальний принцип подання вимог безпеки у вигляді функціональних вимог до засобів захисту і вимоги до гарантій їхньої реалізації. «Канадські критерії» є добре збалансованим конгломератом «помаранчевої книги» і «федеральних критеріїв», посилених вимогами гарантій реалізації політики безпеки, і поряд з іншими стандартами послужили основою для розроблення загальних критеріїв безпеки інформаційних технологій.

capability – **1.** можливість # **2.** функційність # подання ідентифікації об'єкту чи класу об'єктів та набору авторизованих типів доступу для цих об'єктів # наприклад може бути реалізована у вигляді квитка.

capability list – перелік можливостей # перелік, пов'язаний з суб’єктом, який визначає всі типи доступу до суб'єкта для всіх об'єктів # наприклад перелік, пов'язаний з процесом, який визначає всі його типи доступу для всіх файлів та інших захищених ресурсів.

carrier – 1. несуча # електромагнітне коливання, призначене для утворення сигналу радіочастотного шляхом змінювання одного або декількох параметрів цього коливання # 2. носій # пристрій, що несе, переміщає будь-що, а також взагалі те, що охоплює, несе в собі будь-що # 3. частота-носій # хвилі чи коливання, характеристики яких можуть змінюватися сигналом # хвиля чи коливанням можуть бути, наприклад, синусоїдна хвиля або імпульс.

carrier passcode – носій кодів паролів # носії, призначені для запису на них і зчитування кодів паролів. Такими носіями можуть бути перепустки в контрольно-пропускних системах, різного виду картки для ідентифікації особи або оригіналів документів, кредитні картки, пристрої типу Touch Memory і т.ін. Вибір того чи іншого носія визначається вимогами до автоматизованої системи, її призначення, ступеня захисту інформації, кількості користувачів, вартості і т. ін.

carrier password code – носій кодів паролів # див. carrier passcode.

carrier sense – виявлення частоти-носія # в локальній мережі, поточна діяльність станції пересилання даних для виявлення того, чи передає інша станція

casual user – випадковий користувач # користувач обчислювальної системи, який працює з системою нерегулярно, епізодично.

CAT – computer-aided testing – комп'ютеризоване тестування.

catalog – каталог # каталог файлів і бібліотек, з посиланням на їх розташування # у каталозі може міститися інша інформація, така як типи пристроїв, де зберігаються файли, паролі, чинники блокування та інше # див. catalogue.

catalogue – каталог # введена інформація про файли чи бібліотеки в каталозі # див. catalog.

categorization – категоризація # класифікація об'єктів за категоріями.

category – категорія # 1. загальне поняття, що відображає універсальні властивості і відношення об'єктивної дійсності, загальні закономірності розвитку всіх матеріальних, природних і духовних явищ # 2. поняття, що означає розряд предметів # 3. клас, рівень категоризації.

CCITSE – common criterion for information technology security evaluation – загальні критерії безпеки інформаційних технологій.

CCR – commitment, concurrency and recovery – здійснювання, одночасність і відновлювання.

CDMA – code division multiple access – множинний доступ з кодовим розподіленням каналів.

CDPD – cellular digital packet data – стільникове цифрове передавання пакетів даних.

cellular networks fraud – шахрайство в стільникових мережах # неправомочний та навмисний доступ абонента до послуг зв'язку з метою особистої або колективної вигоди. Форми прояву ш. можуть бути різноманітними. Це і зловживання довірою компанії-оператора, у тому числі перепродажа ефірного часу, різноманітного роду переробки стільникових апаратів, підробка ідентифікаторів, викрадення апаратів з наступною їх переробкою.

CEMITS – Common Evaluation Methodology for Information Technology Security – методологія оцінювання безпеки інформаційних технологій загальна.

center – центр # 1. середня частина чогось # 2. зосередження великих і важливих сил # наприклад, науковий центр, промисловий ц. і т. ін.

certificate – сертифікат # 1. документ, який підтверджує, що належним чином ідентифіковані продукт або послуга відповідають вимогам нормативних документів # 2. електронний документ, який зв'язує ідентифікатор власника сертифіката з його ключами відкритими. Звичайно, цей зв'язок реалізується за допомогою механізму підпису цифрового, а у с. містяться і самі значення відкритих ключів # 3. в законодавстві про цифровий підпис електронне посвідчення, яке зв'язує дані, необхідні для верифікації підпису з особою та підтверджує ідентичність цієї особи.

certificate of conformity – сертифікат відповідності # документ, виданий згідно з правилами системи сертифікації, який указує, що забезпечується необхідна впевненість у тому, що потрібним чином ідентифікована продукція, процес чи послуга відповідають конкретному стандартові чи іншому нормативному документові.

certificate of object / subject of acce – сертифікат об'єкта/суб'єкта доступу # загальнодоступна ключова та службова інформація, що використовується в процесі автентифікації.

certificate revocation list – перелік скасованих сертифікатів # список, який містить імена й повноваження користувачів, чиї сертифікати більше не дійсні.

certificate signing request – запит на підпис сертифікату # підписане повідомлення від пристрою до сертифікаційного органу (Certification Authority, CA) із запитом підтвердження сертифіката. Цей варіант визначено в RFC 2986 як CertificationRequest з додатковими специфікаціями, щоб дозволити використання криптографії на еліптичних кривих (ECC).

certification – сертифікація # атестація # 1. діяльність, спрямована на підтвердження відповідності продукції встановленим вимогам # 2. в галузі безпеки інформації – офіційна атестація, що охоплює процедуру всебічної оцінки системи обробки даних, після завершення якої третя сторона, уповноважена на це органом сертифікації, дає гарантії, що частина або система оброблення даних в цілому задовольняє певним вимогам по безпеці інформації, що обробляється нею # див. attestation.

certification – сертифікація # процедура, за допомогою якої третя сторона гарантує, що вся система опрацюванняданих або її частина відповідає вимогам безпеки.

certification authority – орган сертифікації # орган, якому довіряє один або більш користувачів у питанні створення і розподілу сертифікатів відкритого ключа # орган сертифікації може (необов'язково) створювати ключі користувачів # роль органа

сертифікації в цьому процесі полягає в забезпеченні впевненості, що особа, якій виданий унікальний сертифікат, насправді є тією, ким вона себе заявляє. Звичайно це означає, що орган сертифікації має угоду з установою, що надає йому інформацію для підтвердження пред'явленої ідентифікаційної інформації у відношенні особи. Органи сертифікації є критичними компонентом в інформаційній безпеці й електронній комерції, тому що вони гарантують, що дві сторони, що обмінюються інформацією, дійсно є тими, ким вони себе заявляють

certification scheme – схема сертифікації # склад і послідовність дій третьої сторони під час проведення сертифікації.

chain code – ланцюговий код # згортковий код # код, послідовні значення якого можуть бути одержані циклічною перестановкою груп двійкових розрядів слова, що кодується.

chain letter – ланцюговий лист # «лист щастя» # програма, яка поширює себе електронною поштою всім у списку розсилки для кожного отримувача.

change-over system – переналаштовувана система # тимчасова система опрацювання інформації, що її застосовують для полегшення переходу від операційної системи до її альтернативи.

channel – канал # *1.* засіб пересилання сигналів в одному напрямку між двома точками # канал пересилання може бути забезпечений, наприклад, мультиплексуванням частотного поділу чи мультиплексуванням з поділом часу # *2.* частина системи обмінювання даними, яка з'єднує джерело повідомлення з отримувачем повідомлення # кодер може бути вставлений між джерелом повідомлення та входом в канал, та декодером між виходом з каналу і отримувачем повідомлення. Зазвичай ці два блоки не розглядаються як частини каналу # у деяких випадках, однак, їх можна розглядати як частини джерела повідомлення і отримувача повідомлення, відповідно # в теорії інформації, згідно з Шеноном, канал може характеризуватися набором умовних ймовірностей появи усіх повідомлень, отриманих приймачем повідомлень, коли задане повідомлення виходить з джерела повідомлення # *3.* маршрут передачі інформації.

channel (message) switching center – вузол комутації каналів (повідомлень) # сукуність пристроїв, зосереджених в одному місці і об’єднаних загальним пристроєм управління, за допомогою яких здійснюється комутація каналів передавання даних (повідомлень).

channel capacity – пропускна здатність каналу # міра можливостей заданого каналу з урахуванням конкретних обмежень для пересилання повідомлень із зазначеного джерела повідомлень, що виражена або як

максимально можливий усереднений об’єм символів пересланої інформації чи як максимально можлива середня швидкість пересланої інформації, яка може досягатися з довільною малою вірогідністю помилки під час використанні відповідного коду.

channel level – канальний рівень # другий рівень архітектури мережі обчислювальної, що забезпечує передавання даних каналами інформаційними.

channel of information leakage – канал витоку інформації # сукупність носіїв інформації, середовища її поширення та засобів технічної розвідки.

channel vocoder – смугові вокодери # вокодери, в яких аналізується форма мовного сигналу з періодом аналізу 10-30 мс, виділяються і передаються телефонним каналом у цифровому вигляді: значення амплітуд обмеженого числа частотних смуг спектра мовного сигналу, величина періоду основного тону для вокалізованих звуків і рішення тон/шум, що відповідає наявності або відсутності вокалізованої ділянки в мовному сигналі. У приймальному вокодері синтезуються звуки з переданими параметрами. У більшості практичних випадків аналіз мовних сигналів здійснюється з періодом 20 мс для 16-20 частотних смуг, що виділяються смуговими фільтрами, а параметри мови передаються із швидкістю 2400 біт/с. При зниженні вимог до якості синтезованої мови швидкість передавання мовної інформації може бути зменшена до 1200— 1800 біт/с.

chaos measure in making decisions – міра хаосу в прийнятті рішень # надлишок зв’язків, потенційно здатних ускладнити процес прийняття рішення, в першу чергу за рахунок збільшення часу оброблення вхідних даних.

character – **1.** символ # член сукупності елементів, який застосовують для подання, організації, чи керування даними # див. symbol # **2.** характер # 1. сукупність стійких психічних властивостей людини, що формуються в процесі її виховання, навчання, праці, громадської діяльності; вдача # 2. твердість, сила волі, наполегливість у досягненні мети # 3. образ, що узагальнює типові риси певної групи людей.

character recognition – розпізнавання символів # ідентифікація символів за допомогою автоматичних засобів.

character set – набір символів # кінцева множина символів, яка є повною для заданої мети.

character string – рядок символів # рядок, що складено тільки з символів.

character type – тип символа # порядковий тип, кожен об'єкт якого представляє символ.

characteristic – характеристика # опис, певних явищ, відмітних особливостей когось або чогось.

characteristic of observation means in optical range – характеристика засобів спостереження в оптичному діапазоні # числові величини

параметрів, що характеризують можливості засобів спостереження в оптичному діапазоні. Основними з них є: діапазон довжин хвиль світлових променів, що сприймаються засобом спостереження (засоби створюються для видимої частини оптичного діапазону або окремих його частин, а також для різноманітних ділянок інфрачервоного діапазону); чутливість (оцінюється мінімальним рівнем енергії світлового променя, при якому забезпечується необхідна якість зображення об'єкта спостереження); роздільна здатність (мінімальні лінійні або кутові розміри між двома сусідніми точками зображення, які можуть спостерігатися як окремі); поле (кут) зору зображення.

characteristics of information weapons – характеристики інформаційної зброї # відмітні особливості, що характеризують основні риси застосування зброї інформаційної: низька вартість (на відміну від традиційних воєнних технологій, розроблення інформаційної зброї не потребує значних фінансових ресурсів – достатньо мати досвід роботи в системах інформаційних і доступ у глобальні та відомчі мережі); відсутність традиційних кордонів (відмінності між суспільним і особистим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючою взаємозв'язаністю інфраструктур інформаційних); нові можливості для керування суспільною думкою (сучасні інформаційні технології надають широкі можливості для маніпулювання свідомістю людей і затрудняють державі роботу з політичної підтримки ініціатив у галузі забезпечення безпеки); нові завдання перед органами розвідки (неправильне розуміння ролі, можливостей і цілей інформаційної зброї знижує ефективність традиційної розвідувальної діяльності – необхідні нові форми розвідки, що концентруються назброї інформаційній стратегічній); складність оцінки загроз і формування системи попередження (на даний час не існує систем попередження, які дозволили би відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в інформаційному просторі, включаючи шпіонаж і випадкові помилки); труднощі при створенні й підтримці коаліцій (коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки); уразливість власних територій (так як інформаційні технології не обмежені в географічному плані, то інформаційною зброєю можуть уражатися цілі як на віддаленому театрі воєнних дій, так і усередині країни).

check – контроль # 1. перевірка, облік, спостереження за чим-небудь # 2.

установи, особи, що перевіряють діяльність будь-якої іншої організації або відповідної особи, звітність тощо # 3. заключна функція керування.

check authenticity with artificial informational redundancy – контроль достовірності зі штучною інформаційною надмірністю # контроль достовірності, здійснюваний за допомогою введення додаткових інформаційних розрядів у цифровому представленні даних і додаткових операцій у процедурі їхнього оброблення, які мають математичний або логічний зв'язок з алгоритмом оброблення даних. На основі аналізу результатів додаткових операцій і процедур оброблення даних, а також додаткових інформаційних розрядів виявляється наявність або відсутність помилок певного типу, а також можливість їхнього виправлення.

check authenticity with natural informational redundancy – контроль достовірності з природною інформаційною надмірністю # контроль достовірності з виявленням об'єктивно існуючих зв'язків між елементами оброблення, які дозволяють робити висновок про достовірність інформації.

check authenticity with structural redundancy – контроль достовірності зі структурною надмірністю # контроль достовірності за рахунок уведення у склад автоматизованої системи оброблення даних додаткових елементів, що реалізують резервування інформаційних масивів і програмних модулів, виконання одних і тих же функцій різними програмами, схемний контроль у технічних засобах і т. ін.

check authenticity with time redundancy – контроль достовірності з часовою надмірністю # контроль достовірності, заснований на можливості неодноразового повторення певного контрольованого етапу оброблення даних. Як правило, етап оброблення повторюють неодноразово і результати оброблення порівнюють між собою. У випадку виявлення помилки здійснюють виправлення і повторне оброблення.

check code – контрольний код # код, який дозволяє автоматично виявляти, локалізувати і виправляти помилки в даних, що передаються.

check digit – контрольна цифра # цифра, що доповнює блок даних, які передаються, і дозволяє контролювати за певним алгоритмом їхню достовірність.

check frequency band – контрольна смуга радіочастот # смуга частот, за верхнім і нижнім краями якої будь-яка складова має послаблення на 30 дБ і більше відносно рівня випромінювання, прийнятого за 0 дБ.

check number – контрольне число # число, що використовується для контролю достовірності даних, що передаються.

check of authenticity – контроль достовірності # в системах автоматизованих – процес контролю достовірності оброблення інформації

(даних). Методи контролю при обробленні інформації в системах оброблення інформації автоматизованих класифікують по різних параметрах: за кількістю операцій, що охоплюється контролем, – одиночний (одна операція), груповий (група послідовних операцій), комплексний (контролюється, наприклад, процес збирання даних); за частотою контролю – безперервний, циклічний, періодичний, разовий, вибірковий, по відхиленню; за часом контролю – до виконання основних операцій, одночасно з ними, у проміжку між основними операціями, після них; за видом обладнання контролю – вбудований, контроль за допомогою додаткових технічних засобів, без апаратний; за рівнем автоматизації – "ручний", автоматизований, автоматичний. Розрізняють методи контролю достовірності системні, програмні і апаратні. Всі перелічені методи контролю базуються на використанні певної надмірності: структурної, часової або інформаційної, яка у свою чергу може бути природною або штучною.

check of information security – контроль захисту інформації # процес визначення (вимірювання) показників ефективності захисту інформації і порівняння цих показників з нормативними. Складовою частиною контролю захисту інформації є контроль технічного захисту інформації. Застосовують наступні види контролю: попередній, періодичний, постійний.

check technical information protection – контроль технічного захисту інформації #сукупність заходів організаційних і технічних, що проводяться з метою перевірки виконання встановлених вимог і норм захисту інформації технічного.

checking code – перевірка коду # машинні команди, які зчитують частину диску для визначення чи є він несанкціонованою копією.

checking program – перевірка програми # діагностична програма, яка аналізує початкові програми чи дані на рахунок некоректного синтаксису, семантики, чи невідповідність вказаним вимогам.

checkpoint – контрольна точка # точка в програмі, що відповідає виконанню переривання цієї програми, в якій встановлюють послідовність команд, щоб записати стан і результати, їх перевірку та перезапуск.

chip – чіп # кристал напівпровідника разом із нанесеною на ньому схемою інтегральною.

chip-in card – інтелектуальна картка # смарт-картка # див. smart card, intelligent card, integrated circuit card.

chosen cryptogram attack – криптоаналітична атака з вибраним криптотекстом # атака криптоаналітична, при якій крипто аналітик має можливість обирати криптотексти та отримувати з них відкриті тексти.

chosen key attack – криптоаналітична атака з вибраним ключем # криптоаналітична атака , при якій крипто аналітик використовує деяку інформацію про взаємозв'язки між різноманітними ключами.

chosen plaintext attack – криптоаналітична атака з вибраним відкритим текстом # криптоаналітична атака, при якій крипто аналітик має можливість сам обирати пари відкритого тексту та відповідного йому шифртексту. Частковим випадком цієї криптографічної атаки є диференційний метод криптоаналізу.

chosen-plaintext attack – атака з вибором відкритого тексту # аналітична атака, в якій криптоаналітик може відправляти необмежену кількість повідомлень відкритого тексту і перевіряти відповідний зашифрований текст.

chunking – фрагментація # групування даних в єдине ціле на більш високому концептуальному рівні для зберігання і пошуку.

cipher – шифр # сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка знаходиться у повідомленні.

cipher composition – композиція шифрів # криптографічне перетворення, яке полягає у зашифровуванні тексту відкритого за допомогою одного шифру, а потім застосуванні до отриманого шифртексту послідовно ще одного чи декількох шифрів.

cipher stability – стійкість шифру # здатність шифру погано піддаватися розкриттю. Ніякий шифр не є абсолютно стійким. Стійкість шифру визначається часом, необхідним для його дешифрування. Хорошими є шифри, для розкриття яких потрібні роки. За цей час засекречена за допомогою шифру інформація втратить свою актуальність, або вартість дешифрування перевищить вартість самої інформації.

cipher strength – криптостійкість # див. cryptosecurity, resistance to cryptoanalysis, cryptological hardness.

cipher suite – набір шифрів # набір з одного або декількох алгоритмів, призначених для забезпечення будь-якої кількості наступних дій: конфіденційність даних, достовірність даних, цілісність даних, захист від копіювання.

ciphered message – шифровка # шифрограма # який-небудь зашифрований текст (телеграма, лист і т. ін.) # див. ciphertext, cryptogram.

ciphersystem – **1.** шифросистема # шифрувальна система # документація, пристрої, обладнання та пов'язані з ними методи, що застосовуються разом для забезпечення процесу шифрування чи дешифрування # **2.** криптосистема # документація, пристрої, обладнання та пов'язані з ними методи, що застосовуються разом для забезпечення процесу шифрування чи дешифрування.

ciphertext – **1.** зашифрований текст # **2.** криптограма # дані, одержані в результаті застосування шифрування. Семантичний вміст отриманих у результаті шифрування даних недоступний. Зашифрований текст може сам по собі слугувати вхідним у процес шифрування, у результаті чого формується суперзашифрований вихідний текст.

ciphertext – шифртекст # дані, отримані у результаті зашифровування тексту відкри-

ciphertext-only attack – атака з використанням лише криптограми # аналітична атака, в якій криптоаналітик володіє тільки криптограмою.

circuit – схема # див. schema, scheme.

circuit switching – комутування каналів # комутація, яка забезпечує приєднання каналів вторинної мережі електрозв'язку для створення каналу передавання даних.

claim – претензія # твердження про те, що щось відбувається, без змоги надати доказ цього.

claim authentication information – заява про підтвердження автентичності.

class – клас # сукупність, розряд, група предметів або явищ, що мають спільні ознаки, якість.

class ACM: Configuration Management – клас вимог гарантій беспеки: керування проектом # клас вимог гарантій беспеки, що охоплюють наступні розділи вимог гарантій беспеки: засоби керування проектом; керування версіями; конфігурація проекту.

class ADO: Delivery and Operation – клас: дистрибуція # клас вимог гарантій беспеки, що охоплює наступні розділи вимог гарантій беспеки: постачання; установка, настройка, запуск.

class ADV: Development – клас вимог гарантій беспеки: розробка # клас вимог гарантій беспеки, що охоплює наступні розділи вимог гарантій беспеки: загальні функціональні специфікації; архітектура захисту; форма подання продукту на сертифікацію; структура засобів захисту; часткові специфікації засобів захисту; відповідність описів різного рівня; політика безпеки.

class AGD: Guidance Documents – клас вимог гарантій беспеки: документація # клас имог гарантій беспеки, що охоплює наступні розділи мог гарантій беспеки: керівництво адміністратора; керівництво користувача.

class ALC: Life Cycle support – клас вимог гарантій беспеки: процес розробки # клас вимог гарантій беспеки, що охоплює наступні розділи вимог гарантій беспеки: безпека середовища розробки; виправлення помилок і ліквідація уразливостей; технологія розробки; засоби розробки.

class ATE: TEsts – клас вимог гарантій беспеки: тестування # клас вимог гарантій беспеки, що охоплює наступні розділи вимог гарантій беспеки: повнота тестування;

глибина тестування; методика тестування; незалежне тестування.

class AVA: Vulnerability Assessment – клас вимог гарантій беспеки: оцінка захисту # клас вимог гарантій беспеки , що охоплює наступні розділи вимог гарантій беспеки: аналіз схованих каналів; аналіз можливостей неправильного використання засобів захисту; аналіз стійкості засобів захисту; аналіз продукту на наявність уразливостей.

class FAU: security Audit – клас функційних вимог безпеки: аудит # клас функційних вимог безпеки , що охоплює наступні розділи функційних вимог безпеки: автоматичне реагування на спроби порушення безпеки; реєстрація й облік подій; аналіз протоколу аудита; доступ до протоколу аудита; відбір подій для реєстрації й обліку; протокол аудита.

class FCO: Communication – клас функційних вимог безпеки: причетність до приймання/передавання # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: попередження відмови від факту передавання інформації; попередження відмови від факту приймання інформації.

class FCS: Cryptographic Support – клас функційних вимог безпеки: криптографія # клас функційних вимог безпеки, що що охоплює наступні розділи функційних вимог безпеки: керування ключами; криптографічні засоби.

class FDP: user Data Protection – клас функційних вимог безпеки: захист інформації # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: політики керування доступом; засоби керування доступом; автентифікація інформації; експорт інформації із системи; політики керування інформаційними потоками; засоби керування інформаційними потоками; імпорт інформації; захист інформації при передаванні внутрішніми каналами; знищення залишкової інформації; відкіт; контроль цілісності інформації в процесі зберігання; захист внутрішньосистемного передавання інформації при використанні зовнішніх каналіц цілісність внутрішньосистемного передавання інформації при використанні зовнішніх каналів

class FIA: Identification and Authentication – клас функційних вимог безпеки: ідентифікація і автентифікація # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: реакція на невдалі спроби автентифікації; атрибути безпеки користувачів; автентифікаційні параметри; автентифікація користувачів; ідентифікація користувачів; відповідність користувачів і суб’єктів.

class FMT: security Manegement – клас функційних вимог безпеки:

керування безпекою # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: керування засобами захисту; керування атрибутами безпеки; керування параметрами і конфігурацією засобів захисту; відкликання атрибутів безпеки; обмеження терміну дії атрибутів безпеки; адміністративні ролі.

class FPR: PRivacy – клас функційних вимог безпеки: конфіденційність роботи в системі # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: анонімність користувачів; використання псевдонімів; анонімність сеансів роботи з системою; захист від моніторингу сеансів роботи із системою.

class FPT: Protection of the TSF – клас функційних вимог безпеки: надійність засобів захисту # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: тестування апаратно-програмної платформи; захист від збоїв; готовність засобів захисту до обслуговування віддалених клієнтів; конфіденційність інформації, що передається, при роботі з віддаленими клієнтами; цілісність інформації, що передається, при роботі з віддаленими клієнтами; захист внутрішніх каналів інформаційного обміну між засобами захисту, фізичний захист; безпечне відновлення після збоїв; розпізнавання повторного передавання інформації та імітація подій; моніторинг взаємодій; розподіл доменів; синхронізація; час; погодженість обміну інформацією між засобами захисту; реплікація інформації, що використовується засобами захисту, самотестування засобів захисту.

class FRU: Resource Utilisation – клас функційних вимог безпеки: контроль за використанням ресурсів # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: стійкість до відмов; розподіл ресурсів на основі пріоритетів; квотування ресурсів.

class FTA: TOE Access – клас функційних вимог безпеки: контроль доступу до системи # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: обмеження на використання атрибутів безпеки; обмеження числа одночасних сеансів; блокування сеансу роботи із системою; об’яви, попередження, запрошення і підказки; протокол сеансів роботи із системою; керування сеансами роботи із системою.

class FTP: Trusted Path/channels – клас функційних вимог безпеки: пряма взаємодія # клас функційних вимог безпеки, що охоплює наступні розділи функційних вимог безпеки: пряма взаємодія між засобами захисту; пряма взаємодія між користувачами.

class introduction – опис класу.

class name – назву класу.

class of service – клас обслуговування # обслуговування, визначене вичерпним набором параметрів функціонування мережі та їх визначеними значеннями, межами чи діапазонами.

classical cryptosystem – симетрична криптосистема # див. symmetric cryptosystem, one-key cryptosystem, secret-key cryptosystem.

classification – класифікація # процес розподілу об’єктів (предметів, явищ, процесів, понять) за класифікаційними групами у відповідності з певними ознаками # див. classifying, cryptment, scrambling, security.

classified object – категорійований об’єкт # об’єкт, в якому обговорюється, формується, пересилається, приймається, перетворюється, накопичується, обробляється, відображається і зберігається інформація з обмеженим доступом.

classifier – класифікатор # систематизоване зведення найменувань класифікаційних груп та їхніх кодових позначень. Класифікатор є одним з основних засобів забезпечення автоматизованих інформаційних систем лінгвістичних.

classifying – засекречування # дія, спрямована на встановлення будь-чого секретним, недоступним для сторонніх осіб.

clear – обнулення # примусове встановлення одного чи кількох комірок пам’яті в заданий стан, що, зазвичай, відповідає нулю чи значенню символа пробілу.

clear all function – обнулення всіх функцій # функція, яка дає змогу скасувати дані в робочих регістрах і запам’ятовувальних пристроях.

clear memory function – функція очищання пам'яті # функція, яка дає змогу скасувати дані в запам’ятовувальних пристроях, застосовуючи клавіші # може бути застосовано й інші «чисті» клавіші на калькуляторі для скасування заданих функцій.

clear threat – загроза явна # вхідні дані, що усвідомлюються системою інформаційною як загроза.

clearance – **1.** дозвіл # допуск # дозвіл, наданий фізичній особі для доступу до даних або інформації на певному рівні безпеки або нижче # **2.** рівень допуску # ієрархічна частина категорії доступу користувача або процесу, що визначає максимальний рівень доступу пасивного об’єкта, до якого може одержати доступ користувач або процес.

clearing – очищання # перезаписування сегментованих даних на носіях даних, що мають певні класифікації і категорії безпеки, так що ці носії даних можна повторно застосовувати для запису за тією самою класифікацією та категорією безпеки.

cleartext – відкритий текст # дані, семантичний вміст яких доступний

без застосування криптографічних методів.

CLID – calling line identifier – ідентифікатор лінії виклику.

client – клієнт # *1.* логічний об'єкт протоколу, який використовує сервіс # *2.* роль, яку виконує процесор, коли він запитує послуги, які надає інший процесор # *3.* особа, що доручила ведення своєї справи адвокатові, нотаріусові тощо # *4.* постійний відвідувач, замовник, тощо.

client-server – клієнт-сервер # архітектура стосується методу розподіленого опрацювання, за який клієнт отримує сервіси від сервера.

client-server relationship – відношення між клієнтом і сервером # відношення між клієнтом і сервером, яке встановлюється в момент запиту послуги клієнтом, яку надає сервером.

CLNP – connectionless network protocol – мережний протокол без установлення з'єднання.

closed guard – завершена охорона # охорона, стан якої оцінюють як відсутня.

closed user group – обмежене коло користувачів # група зазначених користувачів мережі пересилання даних, яким назначена абонентська послуга, що дає змогу їм спілкуватися один з одним, але забороняє доступ до чи від інших користувачів мережі пересилання даних # термінальне обладнання користувача може належати більш ніж одній замкнутій групі користувачів.

closed user group with incoming access – обмежене коло користувачів із вхідним доступом # користувацькі засоби, які дозволяють термінальному обладнанню даних (ТОД), що належить до одного чи кількох обмежених кіл користувачів (ОКК) приймати виклики з ТОД за межами цих ОКК.

closed user group with outgoing access – обмежене коло користувачів із вихідним доступом # користувацькі засоби, які дозволяють термінальному обладнанню даних (ТОД), що належить до одного чи кількох обмежених кіл користувачів (ОКК) ініціювати виклики для ТОД за межами цих ОКК.

closed-security environment – замкнене безпечне середовище # середовище, в якому особливу увагу приділяють (у формі дозволів, рівнів захисту, засобів контролю конфігурацій тощо) для захисту даних і ресурсів, від випадкових або зловмисних шкідливих дій.

cloud application portability – переносимість хмарного додатка # можливість міграції додатки від однієї служби хмарних обчислень до іншого службі хмарних обчислень.

cloud auditor – аудитор хмари # партнер служби хмарних обчислень, відповідальний за проведення аудиту надання та використання служб хмарних обчислень.

cloud capabilities type – тип можливостей хмари # класифікація функціональності, наданої службою хмарних обчислень споживачеві

служби хмарних обчислень, заснована на використовувані ресурси # типи можливостей хмари – це тип можливостей додатків, тип можливостей інфраструктури і тип можливостей платформи.

cloud computing – хмарні обчислення # парадигма для надання можливості мережевого доступу до масштабованості і еластичному пулу загальних фізичних або віртуальних ресурсів з наданням самообслуговування і адмініструванням на вимогу. # Приклади ресурсів включають сервери, операційні системи, мережі, програмне забезпечення, програми та обладнання для зберігання даних.

cloud data portability – переносимість хмарних даних # переносимість даних від однієї служби хмарних обчислень до іншого службі хмарних обчислень.

cloud deployment model – модель розгортання хмарних обчислень # спосіб організації хмарних обчислень, заснований на управлінні і спільне використання фізичних або віртуальних ресурсів # моделі розгортання хмарних обчислень включають в себе суспільне хмара, гібридне хмара, приватна хмара і публічне хмара.

cloud service – служба хмарних обчислень # одна або більше можливостей, що надаються через хмарні обчислення, що викликається за допомогою певного інтерфейсу.

cloud service broker – брокер служби хмарних обчислень # Партнер служби хмарних обчислень, який погоджує відносини між споживачами служби хмарних обчислень) і постачальниками служби хмарних обчислень.

cloud service category – категорія служб хмарних обчислень # Група служб хмарних обчислень, що володіють деяким набором загальних якостей # категорія служб хмарних обчислень може включати можливості одного або більше типів можливостей хмари.

cloud service customer data – дані споживача служби хмарних обчислень # клас об'єктів даних, що знаходяться під керуванням, з юридичних або інших причин, споживача служби хмарних обчислень, які були введені в службу хмарних обчислень або отримані в результаті реалізації можливостей служби хмарних обчислень споживачем служби хмарних обчислень або від його імені через опублікований інтерфейс служби хмарних обчислень # приклад юридичних засобів керування – авторське право # може трапитися так, що служба хмарних ви Ісленьев буде містити або впливати на дані, які не є даними споживачів служби хмарних обчислень; це можуть бути дані, надані постачальниками служби хмарних обчислень або отримані з іншого джерела, або це можуть бути загальнодоступні дані. Однак будь-які вихідні дані, отримані завдяки діям споживача служби хмарних

обчислень з використанням можливостей служби хмарних обчислень над цими даними, ймовірно, будуть даними споживача служби хмарних обчислень внаслідок загальних принципів авторського права, якщо тільки про іншому не буде вказано в угоді про службу хмарних обчислень.

cloud service customer споживач служби хмарних обчислень # сторона, яка знаходиться в ділових відносинах з метою використання служб хмарних обчислень # ділові відносини не обов'язково мають на увазі фінансові угоди.

cloud service derived data – похідні дані служби хмарних обчислень # клас об'єктів даних, керованих постачальником служби хмарних обчислень, які отримані споживачем служби хмарних обчислень в результаті взаємодії зі службою хмарних обчислень # похідні дані служби хмарних обчислень включають дані журналів подій, що містять записи про те, хто використовував даний сервіс, в який час, які функції і типи даних були задіяні і т.д. Також може бути включена інформація про кількість авторизованих користувачів і їх ідентифікатори. Крім того, вони можуть включати дані про конфігурацію або налаштування в випадках, коли у служби хмарних обчислень є можливості конфігурації і настройки.

cloud service partner – партнер служби хмарних обчислень # сторона, яка займається підтримкою або допоміжною діяльністю по відношенню до діяльності постачальника служби хмарних обчислень або споживача служби хмарних обчислень, або обох.

cloud service provider – постачальник служби хмарних обчислень # сторона, яка забезпечує доступ до служб хмарних обчислень.

cloud service provider data – дані постачальника служби хмарних обчислень # клас об'єктів даних, специфічних для операцій служби хмарних обчислень, що знаходяться під керуванням постачальника служби хмарних обчислень # дані постачальника служби хмарних обчислень включають, зокрема, інформацію про конфігурацію і використанні ресурсів, відомості про виділення службам хмарних обчислень віртуальних машин, ресурсів сховища і мережевих ресурсів, дані про повну конфігурації і завантаженні центру обробки даних, частотах відмов фізичних і виртуал родних ресурсів, експлуатаційних витратах і так далі.

CMIP – common management information protocol – протокол обміну інформацією керування.

CMIPM – common management information protocol machine – кінцевий автомат протоколу обміну інформацією керування.

CMIS – common management information service – сервіс загальної інформації адміністрантивного керування.

CMIS – common management information service – сервіс обміну інформацією керування.

CMISE – common management information service element – сервісний елемент обміну інформацією керування.

coaxial cable – коаксіальний кабель # кабель, у якого два провідники: центральний дріт та циліндричний заземлений екран. Екран ізолюється від центрального проводу за допомогою різноманітних матеріалів і конструкцій. Для ізоляції використовується поліетилен, фторлан (фторопласт), поліпропілен, гума, неорганічна ізоляція. Для забезпечення гнучкості коаксіального кабеля екран виготовляється з мідної або залізної сітки, а для захисту від зовнішніх впливів покривається шаром ізолятора (поліхлорвінілу). Коаксіальний кабель мінімізує електричні та радіочастотні завади: сигнали у коаксіальному кабелі не впливають на сусідні компоненти, потенційні завади від цих компонентів не впливають на сигнал, що передається кабелем.

code – **1.** код # *1.* система символів для передавання, оброблення й зберігання (запам'ятовування) інформації # *2.* множина слів (кодових комбінацій) в деякому алфавіті, поставлена у взаємно-однозначну відповідність іншій множині (що кодується) #. *3.* ключ до способу зашифровування чи розшифровування тексту # *4.* позначення об'єкта обліку знаком або системою знаків за правилами, встановленими псиною системою кодування # *5.* програма на машинні # **2.** кодувати # перетворення даних за допомогою коду таким чином, що можливе зворотне перетворення до вихідної форми.

code ASCII –ASCII #американський стандартний код для обміну інформацією (від American Standard Code for Information Interchange).

code breakpoint – код точки переривання # точка зупину, яка залежить від виконання конкретної інструкції.

code combination – кодова комбінація # слово коду; скінченна послідовність знаків алфавіту, поставлена у взаємно-однозначну відповідність кодованому значенню.

code composition – композиція шифрів # див. cipher composition.

code division multiple access – множинний доступ з кодовим розділенням каналів.

code element – елемент коду # результат застосування коду до елемента кодованого набору # наприклад «CDG», що представляє аеропорт Шарля-де-Голя в Парижі в коді трьохлітернного подання найменуваннях аеропортів; шістнадцяткове число 0041, що представляє «латинську велику букву А».

code element set – набір елементів коду # результат застосування коду до всіх елементів кодового набору #

наприклад всі трилітерні познаки назв аеропортів.

code extension character – символ розширення коду # керувальний символ, який застосовують для позначення того, що один чи кілька наступних значень кодів мають інтерпретуватися відповідно до іншого коду.

code ISO – код ISO # стандартний символьний код обміну інформацією, в якому кожний символ кодується сімома бітами (від International Organization for Standartization). Використовується для обміну даними між основною пам'яттю ЕОМ і зовнішніми пристроями і для передавання даних лініями зв'язку.

code lock – кодовий замок # замок, ключем до якого служить певний код. Кодові замки бувають механічними, електромеханічними, електронними.

code sequence – кодова послідовність # послідовність кодованих символів, одержана за певними правилами. Може бути скінченною або нескінченною # див. code word.

code set – кодовий набір # результат застосування коду до всіх елементів кодового набору.

code value – значення коду # результат застосування коду до елемента кодованого набору.

code word – кодова комбінація # див. code combination.

coded character set – набір закодованих символів # кодований набір, елементи якого є поодинокими символами # наприклад символи абетки, коли вони відображаються на набір 7-бітових рядків.

coded image – закодоване зображення # кодоване подання зображення на дисплеї для зберігання чи опрацювання # наприклад результат шифрування оцифрованого зображення.

coded message – шифровка # див. ciphered message.

coded set – закодований набір # набір елементів, який відображають на інший набір згідно з кодом # наприклад список найменувань аеропортів, які відображені на відповідний набір трилітернних скорочень.

code-independent data communication – кодонезалежне пересилання даних # режим пересилання даних, який застосовує символьнозорієнтований протокол, що не залежить від набору символів або коду застосовуваних джерелом даних.

coder – кодер # 1. кодувальний пристрій # 2. програміст, який складає програми за готовими детальними специфікаціями.

code-transparent data communication – кодопрозоре пересилання даних # режим пересилання даних, який застосовує бітзорієнтований протокол, що не залежить від структури бітової послідовності застосовуваної джерелом даних.

coding – кодування # 1. операція ототожнення символів чи груп одного коду із символами чи групами символів іншого коду # 2. ототожнення даних з їхніми

комбінаціями кодовими; установлення відповідності між елементом даних та кодовою комбінацією (словом коду) # 3. процес подання програми на мові програмування.

coding scheme – схема кодування # сукупність правил, яка відображає елементи першого набору на елементи другого набору # елементи будь-якого набору можуть бути символами чи символьними рядками # перший набір називають кодованим набором, а другий набір називають набором кодів # кожен елемент набору коду може бути пов'язаний з більш ніж одним елементом кодового набору, але зворотне невірно.

coding theory – теорія кодування # розділ теорії інформації, що вивчає способи ототожнення повідомлень з сигналами # див. coding, encoding.

cognition – пізнання # процес відображення й відтворення дійсності вмисленні, зумовлений суспільно-історичним розвитком; взаємодія суб'єкта і об'єкта, результатом якої є нове знання про світ.

cohesion – зв'язаність # спосіб та ступінь, в якій діяльність одного модуля пов'язана з іншими.

cold site – резервне приміщення для розміщення обчислювальних засобів у випадку стихійного лиха # технічні засоби, принаймні з обладнанням, необхідним для підтримки встановлення і експлуатації альтернативної системи опрацювання даних.

cold standby – холодний резерв # конфігурація, в якій резервний функційний модуль може бути введений в експлуатацію з деякою затримкою, якщо основний функційний модуль вийде з ладу.

collection – збирання # див. acquisition.

collection connection – збиральне з'єднання # односпрямоване з'єднання (на вимогу, резервоване чи постійне), яке переносить інформацію користувачів від визначеної кількості кінцевих точок до однієї кінцевої точки.

collision – **1.** колізія # 1. зіткнення протилежних сил, інтересів, прагнень # 2. розходження між правовими нормами, що регулюють однакові правовідносини # **2.** конфлікт # 1. виникнення того самого значення геш-функції для двох або більше різних ключів # 2. стан, який виникає в результаті одночасних пересилань у середовищі пересилання.

collision enforcement – контроль за розв'язанням конфліктів # в мережі CSMA/CD, пересилання станцією пересилання даних сигналу наявності конфлікту після того, як вона виявила конфлікт, для гарантування того, що всі інші станції дізнаються про конфлікт.

collision resolution – розв'язання конфліктів # процес застосування додаткових обчислень або інших засобів для розв'язання конфліктів.

comb – гребінець # в блоці магнітного диска, збірка важелів доступу, які переміщаються як єдине ціле.

combination – комбінація # взаємно зумовлене розташування чого-небудь.

combination lock – кодовий замок # див. code lock.

combiner virus – комбінований вірус # вірус комп'ютерний, що має окремі ознаки інших вірусів у певній алгоритмічній сукупності.

comformity – відповідність # виконання вимоги.

comment – коментар # мовна конструкція, що її застосовують винятково для вмісту тексту, який ніяк не впливає на виконання програми.

comment [ату] – коментар # 1. тлумачення певного тексту або книги # 2. вид програми радіомовлення, в якій приводиться думка (або декілька різних думок) фахівців, які розкривають суть проблеми. В коментарях фахівці висловлюють свої міркування у відповідності до того, що вони вважають важливим донести до слухачів і що відповідає меті психологічного впливу.

commercial intelligence agency – орган комерційної розвідки # органи розвідки, створені комерційною структурою для забезпечення її інформацією, необхідною для успішної діяльності на ринку в умовах гострої конкурентної боротьби. Органи комерційної розвідки входять до складу служби безпеки комерційної структури.

commercial secrets protection – захист комерційної таємниці # запобігання витоку, викраденню, втрати, викривлення, підробки інформації, що складає таємницю комерційну.

commitment, concurrency and recovery – здійснювання, одночасність і відновлювання # елемент сервісу прикладного рівня, який контролює операції, що виконуються двома чи більше прикладними процесами над загальними даними для гарантування того, що операції виконуються або повністю, чи взагалі не виконуються.

common criterion for information technology security evaluation – загальні критерії безпеки інформаційних технологій # стандарт інформаційної безпеки (версія 2.1 стандарту видана у серпні 1999 року), що узагальнює зміст і досвід використання «помаранчевої книги». В ньому розвинені «європейські критерії», втілена в реальні структури концепція типових профілів захисту «федеральних критеріїв» США і відповідно до «канадських критеріїв» представлена однакова основа для формулювання розробниками, користувачами і і оцінювачами інформаційних технологій (експертами з кваліфікації) вимог, метрик і гарантій безпеки. Матеріали стандарту являють собою енциклопедію вимог і гарантій з інформаційної безпеки, які можуть відбиратися й реалізовуватися у функціональні стандарти (профілі захисту) забезпечення інформаційної безпеки для конкретних систем, мереж і засобів як користувачами (по відношенню до того, що вони хочуть

одержати в продукті, що пропонується), так і розробниками і операторами мереж (по відношенню до того, що вони гарантують в продукті, що реалізується). Основними компонентами безпеки «загальних критеріїв» є: потенційні загрози безпеці обчислювальних систем і завдання захисту; політика безпеки; продукт інформаційних технологій; профіль захисту; проект захисту; функціональні вимоги безпеки; вимоги гарантій безпеки; рівні гарантій. Стандарт «загальних критеріїв» описує тільки загальну схему проведення аналізу кваліфікаційного і сертифікації, але не регламентує процедуру їх здійснення. Питаннями методології кваліфікаційного аналізу й сертифікації присвячений окремий документ авторів «загальних критеріїв» – «методологія загального оцінювання безпеки інформаційних технологій», який є додатком до стандарту.

common evaluation methodology for information technology security – методологія оцінювання безпеки інформаційних технологій загальна # додаток до стандарту інформаційної безпеки «загальні критерії безпеки інформаційних технологій», в якому приведена методологія аналізу кваліфікаційного і сертифікації захищених систем оброблення інформації.

common management information service – сервіс загальної інформації адміністрантивного керування # сервіс прикладного рівня, який забезпечує загальний механізм обмінювання інформацією та командами з метою керування системами в централізованому чи децентралізованому середовищі керування.

common name – загальне ім'я # атрибут адреси відправника/отримувача, що визначає користувача чи список розсилання щодо деякого об'єкта, зазначеного іншим атрибутом # наприклад назва посади в організації, наприклад, «наглядач», «адміністратор», «директор по маркетингу» # в адресі відправника/отримувача обов’язково має бути загальне ім'я чи особисте ім'я.

communication channel pass band – смуга пропускання каналу зв’язку # яку пропускає канал зв’язку. За шириною смуги частот канали зв’язку поділяються на вузькосмугові і широкосмугові.

communication channel transmission band – смуга пропускання каналу зв’язку # див. communication channel pass band.

communication circuit – лінія зв’язку # сукупність технічних пристроїв і середовища розповсюдження сигналів, що забезпечує створення одного (одноканальна лінія зв’язку) або кількох (багатоканальна лінія зв’язку) каналів зв’язку (передавання сигналів у заданих напрямках з необхідною якістю і надійністю). В залежності від сигналів, що використовуються, лінії зв’язку

можуть бути електричними, звуковими (акустичними) або оптичними (світловими). В залежності від засобів та середовища, що використовуються, електричні лінії зв'язку поділяються на лінії радіозв'язку (радіорелейні, іоносферні, метеорні, космічного радіозв'язку), проводові, комбіновані. Існують лінії прямого зв'язку і лінії зв'язку з ретрансляційними підсилювальними та комутаційними пунктами.

communication environment – комунікаційне середовище # сукупність технічних і програмних засобів системи передавання даних.

communication line – лінія зв'язку # див. communication circuit, communication link.

communication link – лінія зв'язку # див. communication circuit, communication line.

communication network – мережа зв'язку # комунікаційна мережа # мережа передавання даних, утворена множиною взаємозв'язаних комунікаційних модулів – вузлів зв'язку і пунктів абонентських.

communication node – вузол обміну даними # елемент системи зв'язку, що забезпечує створення та комутацію групових трактів, каналів, повідомлень, пакетів, цифрових потоків, а також інших функцій в системі зв'язку.

communication overload – комунікаційне перевантаження # фізичний стан одержувача інформації (настільки насиченого нею), що він уже не може сприймати її значення.

communications linkage – комунікаційне з'єднання # засоби обміну даними між комп'ютерними системами або між користувачем та комп'ютерними системами.

communications security – безпека обмінювання даними # комп'ютерна безпека щодо пересилання даних.

compact – ущільнювати # зменшення інформаційного простору, прийняте на носієві даних за допомогою кодування чи видалення повторюваних символів.

companion virus – вірус-супутник # комп'ютерний вірус , який не змінює програмні файли. Алгоритми роботи таких вірусів полягають у тому, що вони створюють для командних файлів запуску файли-супутники, що мають те ж ім'я, але з розширенням більш високого командного порядку. Після запуску такого файла ЕОМ першою запускає файл, що має найвищий рівень порядку, тобто вірус, який потім запустить і командний файл.

compartmentalization – секціонування # компартменталізація # поділ даних на ізольовані (окремі) блоки з окремими заходами убезпечення з метою зниження ризику # наприклад поділ даних щодо основного проекту на блоки, які відповідають підпроектам, зі своїми власними заходами убезпечення, для обмеження впливу основного проекту.

compatibility – сумісність # властивість різноманітних за конструкцією пристроїв виконувати ідентичні функції.

competence – компетентність # компетенція # здатність застосовувати знання та навички для досягнення бажаних результатів.

complementary keys – комплементарні ключі # пара ключів для виконання зашифровування та розшифровування.

completeness – повнота # наявність чого-небудь у достатній мірі, вища ступінь насиченості чим-небудь.

completeness acquired information – повнота добутої інформації # повнота інформації, що поступає від органів добування інформації, яка повинна забезпечувати знання проблеми, необхідне для обґрунтованого прийняття рішення керівництвом. Характеризується наступними показниками: відповідністю обсягу добутих відомостей, даних обсягу всієї добутої інформації; відношенням розкритих проблем (питань) до загального числа поставлених проблем (питань).

complex – комплекс # 1. сукупність предметів чи явищ, що становлять єдине ціле # 2. два чи більше вироби, не з'єднаних на підприємстві-виробнику складальними операціями, але призначені для виконання взаємозв'язаних експлуатаційних функцій.

complex of automation tools – комплекс засобів автоматизації # територіально-зосереджений комплекс апаратних і програмних засобів, що виконують спільне завдання автоматизованого оброблення інформації: система обчислювальна , вузол комутації, пункт абонентський, система телеоброблення даних і т. ін.

complex of communication facilities – комплекс засобів зв'язку # сукупність організаційно, функціонально та конструктивно взаємопов'язаних засобів зв'язку.

complex of tools and mechanisms of protection – комплекс засобів і механізмів захисту # організаційні, технічні, програмні, соціальні, правові та інші засоби і механізми, що забезпечують локалізацію, запобігання і ліквідацію загроз інформаційній безпеці особистості, суспільства, держави.

complexing – комплексування # об'єднання в єдине ціле сукупності предметів чи явищ.

complexing computer aids – комплексування засобів обчислювальної техніки # комплекс робіт, спрямований на формування конфігурації системи обчислювальної, що відповідає завданню замовника. Виконується шляхом компонування і взаємоув'язки технічних і програмних засобів та розробки документації технічної.

complexing of information leakage channels – комплексування каналів витоку інформації # комплексне використання каналів витоку

інформації, засноване на наступних принципах: канали, що комплексуються, доповнюють один одного за своїми можливостями; ефективність комплексування підвищується при зменшенні залежності між джерелами інформації каналів і ознаками демаскуючими в різних каналах. Комплексування каналів витоку інформації забезпечує: збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їхніх поточних структур ознакових; підвищення вірогідності інформації семантичної і точності вимірювання ознак, особливо у випадку добування інформації з недостатньо надійних джерел. Коли виникають сумніви у вірогідності інформації, то з метою виключення дезінформації, одержані відомості і дані повторно перевіряють іншим каналом. Можливі два основних види комплексування каналів витоку інформації – забезпечення витоку інформації від одного джерела декількома паралельно функціонуючими каналами (комплексування каналів витоку інформації паралельне) і від різних джерел (комплексування каналів витоку інформації від різних джерел).

component – компонент # 1. складова частина чогось # 2. складова частина пристрою, програми, системи, даних.

composite number – складене число # натуральне число *n*, яке більше *1* та ділиться націло на деяке натуральне число $1<x<n$ # див. prime number.

composition – композиція # метод послідовного об'єднання об'єктів (процесів, явищ) в єдине ціле за певними правилами.

compress – стискувати # зменшення інформаційного простору, прийняте на носієві даних за допомогою кодування чи видалення повторюваних символів.

compromise – порушення нормального функціювання системи безпеки # порушення комп'ютерної безпеки, внаслідок чого програми чи дані, можуть бути змінені, знищені чи надані несанкціонованим об'єктам.

compromised key – скомпрометований ключ # ключ, конфіденційність або цілісність якого порушена.

compromising emanation – випромінення, що несе конфіденційну інформацію # сигнали, які ненавмисно випромінюються, і, якщо їх перехоплюють і аналізують, можуть містити конфіденційну інформацію, яку опрацьовують чи передають # наприклад акустичне випромінення, електромагнітне випромінення.

COMPUSEC – computer security – комп'ютерна безпека.

computation center – обчислювальний центр # 1. науково- дослідний заклад, який займається розробкою забезпечення програмного ЕОМ, методів вирішення прикладних задач в різноманітних галузях науки, науки, техніки, управління. Обчислювальний центр надає також

послуги з виконання обчислювальних робіт зовнішнім замовникам # 2. заклад, призначений для виконання складних і трудомістких обчислювальних робіт з допомогою ЕОМ.

computation network – мережа електрозв'язку # технологічні системи, які забезпечують один або декілька видів передач: телефонну, телеграфну, факсимільну, передачу даних і інших видів документальних повідомлень, в тому числі й обмін між ЕОМ, телевізійне, звукове та інші види радіо- і проводового мовлення.

computational resources – обчислювальні ресурси # сукупність апаратних, програмних і інформаційних засобів даного закладу, підприємства, обчислювального центру або окремого користувача.

computationally cryptosecurity – практична криптостійкість # криптостійкість, яка визначається для шифру, який не є ідеальним шифром, тобто може бути дешифрований за скінченний час. Інша назва криптостійкість у обчислювальному сенсі.

compute algorithm –обчислювальний алгоритм # алгоритм точного або наближеного розв'язання задач прикладної математики на ЕОМ.

compute environment – обчислювальне середовище # засоби апаратні, забезпечення програмне і набори даних (файлів).

computer – комп'ютер # електронна обчислювальна машина # ЕОМ.

computer abuse – комп'ютерна злочинність # самовільна чи недбала несанкціонована діяльність, яка впливає чи пов'язана з комп'ютерною безпекою системи опрацювання даних.

computer code – програмний код # машинний код # 1. двійковий код , що використовується для кодування машинних команд за правилами, передбаченими в даному типі ЕОМ # 2. програма на машинній мові.

computer complex – обчислювальний комплекс # сукупність двох або більше ЕОМ, що працюють як єдина система.

computer crime – комп'ютерний злочин # передбачені кримінальним законом суспільно небезпечні дії, що здійснюються з використанням засобів електронно-обчислювальної (комп'ютерної) техніки. До суспільно небезпечних дій відносять: неправомірний доступ до комп'ютерної інформації, що охороняється законом (інформації на машинному носії, в ЕОМ, в системі ЕОМ або їхньої мережі), якщо ці дії спричинили знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхньої мережі; створення програм для ЕОМ або внесення змін в існуючі програми, якщо це явно привело до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення

роботи ЕОМ, системи ЕОМ або їхні мережі, а також використання або розповсюдження таких програм або машинних носіїв з такими програмами; порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі особою, що має доступ до ЕОМ, системи ЕОМ або їхньої мережі, що викликало знищення, блокування або модифікацію інформації ЕОМ, що охороняється. Способи здійснення комп'ютерного злочина можна розділити на п'ять основних груп: вилучення засобів комп'ютерної техніки; перехоплення інформації; доступ несанкціонований до засобів комп'ютерної техніки; маніпулювання даними і управляючими командами; комплексні методи.

computer crime – комп'ютерний злочин # *1.* злочин, скоєний за допомогою використання, модифікації чи знищення апаратного забезпечення, програмного забезпечення чи даних # *2.* злочин, скоєний за допомогою чи за безпосередньої участі, системи опрацювання даних або комп'ютерної мережі.

computer crime struggle – боротьба з комп'ютерною злочинністю # профілактика та попередження злочинів комп'ютерних. Боротьба з комп'ютерною злочинністю передбачає: створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного та програмного захисту інформації; створення спеціалізованих організаційних структур, завданням яких є забезпечення надійного функціонування засобів захисту, засобів генерації ключів та паролів, їхнього розподілу, контролю за використанням, зміною та знищенням; підготовку кваліфікованих кадрів для правоохоронних органів, а саме для органів дізнання та розшуку, судів, служб безпеки комп'ютерних та телекомунікаційних мереж і систем.

computer espionage – комп'ютерний шпіонаж # приєднання до комп'ютерів без відома власників з метою зняття або ушкодження даних, що містяться в них.

computer fraud – комп'ютерне шахрайство # шахрайство, вчинене за допомогою чи за безпосередньої участі системи опрацювання даних або комп'ютерної мережі.

computer intruder – комп'ютерний злочинець # особа, що здійснила злочин комп'ютерний.

computer network – обчислювальна мережа # сукупність мережі передавання даних, взаємозв'язаних з нею ЕОМ та необхідних для реалізації цього зв'язку програмного забезпечення і (або) технічних засобів та призначена для розподіленого оброблення даних (інформації).

computer platform – комп'ютерна платформа # тип комп'ютера персонального (PC, Macintosh, Atary, Sincler і т. ін.), на якому може бути встановлений даний програмний продукт.

computer science – інформатика # наука, яка займається вивченням законів, методів і способів одержання, зберігання, перетворення, передавання і використання інформації. Об'єктом дослідження інформатики є інформація. Поділ інформатики на основні напрямки опирається на внутрішню єдність завдань, що вирішуються в них, і підходів до розуміння суті інформації. Виділяють вісім основних напрямків інформатики: інформатика теоретична, кібернетика, програмування, інтелект штучний, системи інформаційні, техніка обчислювальна, інформатика у природі та суспільстві.

computer security – безпека комп'ютерних [обчислювальних] систем # захист даних і ресурсів від випадкових або зловмисних дій, зазвичай, за допомогою прийняття відповідних заходів # ці дії можуть охоплювати модифікацію, знищення, доступ, розголошенням або придбанням, якщо вони не є авторизованими.

computer system – комп'ютерна система # набір апаратного забезпечення, який керується як єдиний елемент програмним забезпеченням, таким як операційна система, яка може також надавати загальні послуги, такі як контроль доступу, комунікація між процесами та графічний користувацький інтерфейс.

computer system domain – домен комп'ютерної системи # ізольована логікова область комп'ютерної системи, яку характеризують унікальним контекстом, де усередині об'єкти комп'ютерної системи володіють певними властивостями, повноваженнями і зберігають певні відносини між собою.

computer system security – захист інформації в автоматизованій системі # information protection in automated system.

computer systems protection mechanism – механізм захисту обчислювальних систем # сукупність засобів та заходів, за допомогою яких реалізується безпека обчислювальних систем.

computer virus – комп'ютерний вірус # спеціальна програма, що здатна самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій. Після запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів, модифікування програмного забезпечення, спотворення результатів обчислень, засмічування або стирання пам'яті, створення завад при роботі ЕОМ, наприклад, різних аудіо- та відеоефектів. Програми вірусів складаються (виконуються, пишуться), в основному, на мові

програмування “асемблер” і при виконанні не створюють ніяких аудіовізуальних відображень у комп’ютерній системі. В. к. переноситься при копіюванні програм або даних спеціального формату або розповсюджується по мережі обчислювальній. В. класифікуються на певній основі і розбиваються на декілька узагальнених груп: віруси завантажувальні (системні), віруси файлові і комбіновані віруси, або на дві групи, що мають підгруповий поділ, а саме: за способом зараження засобів комп’ютерної техніки поділяються на резиденті та нерезиденті: за алгоритмом їхньої побудови і виявлення на віруси вульгарні та роздроблені.

computer virusology – комп’ютерна вірусологія # наука, що займається вивченням вірусів комп’ютерних.

computer-aided testing – комп’ютеризоване тестування # тестування і перевірка продукту чи його частин за допомогою систем опрацювання даних # комп’ютеризоване тестування є одним з аспектів комп'ютерного забезпечення якості.

computer-system audit – аудит комп'ютерної системи # дослідження процедур, що їх застосовують в системі опрацювання даних для оцінення її ефективності та правильності, і надання рекомендацій щодо поліпшення.

computing center – обчислювальний центр # див. computation center.

computing system user – користувач обчислювальної системи # 1. фізична або посадова особа, яка має право використання ресурсів системи обчислювальної для виконання своїх службових обов’язків (для одержання інформації або вирішення різних завдань). Розрізняють наступні категорії к.: аналітик, програміст системний, програміст прикладний, адміністратор автоматизованої системи, оператор ЕОМ, користувач кінцевий # 2. програма або система, що використовує ресурси іншої системи.

computing task – обчислювальна задача # розрахункова задача # задача, яка потребує виконання обчислювальних – арифметичних і логічних операцій.

COMSEC – communications security – безпека обмінювання даними.

concept – концепція # див. conception.

concept – концепція # принцип # див. principle, approach.

concept – поняття # 1. одна з форм мислення, результат узагальнення суттєвих ознак об’єкта дійсності # 2. розуміння кимсь чого-небудь, що склалося на основі якихось відомостей, власного досвіду.

conception – концепція # система поглядів на певне явище; спосіб розуміння, тлумачення певних явищ, основна ідея будь-якої теорії.

condition – умова # 1. обставина, від якої будь-що залежить # 2. обстановка, в якій відбувається, здійснюється що-небудь.

conditional-passive attack – умовно-пасивна атака # атака на мережу

обміну інформацією віддалена, яка має за мету підготовку до атаки активної і охоплює заходи ведення комп'ютерної розвідки та подолання системи захисту інформації мережі.

conductor – кабель # див. cable.

conectionless-mode-transmission – передавання у режимі без установлення з'єднання # передавання даних поза контекстом з'єднання n-го рівня, яка не потребує установлення логічного взаємозв'язку між сервісними блоками даних n-го рівня.

confidential data – секретні дані #дані з обмеженим доступом # закриті дані, коло користувачів якими визначається відповідними нормативними документами.

confidential information – конфіденційна інформація # інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава ф порядок доступу до якої встановлюється ними.

confidentiality – конфіденційність # властивість даних [інформації] бути недоступними або закритими для неавторизованих приватних і юридичних осіб, сутностей або процесів.

confidentiality classification label – гриф конфіденційності # гриф, що найчастіше застосовується для позначення ступеню конфіденційності інформації комерційної (інформації, що містить таємницю комерційну). Для грифування комерційної інформації застосовують різноманітні шкали, засновані на відповідному критерії. Розповсюджена шкала: «комерційна таємниця – суворо конфіденційно», «комерційна таємниця – конфіденційно», «комерційна таємниця». Відома також шкала «суворо конфіденційно особливий контроль», «суворо конфіденційно», «конфіденційно», застосовується також шкала з двох рівнів: «комерційна таємниця» та «для службового використання».

configuration – конфігурація # сукупність процесів, які мітить інформаційна система та спосіб, яким ці процеси пов'язуються.

configuration control board – група контролювання конфігурації # кваліфікований персонал, який оцінює, схвалює чи відхиляє усі запропоновані зміни до поточної базової лінії розвитку.

configuration management – керування конфігурацією # діяльність, пов'язана з керуванням конфігурацією інформаційної системи на протязі її життєвого циклу.

configuring – конфігурування # настройка системи операційної на конкретну конфігурацію обладнання і адаптація до потреб користувача, що виконуються при завантаженні ОС за вказівками, заданими в файлі конфігурації.

conflict information relations – конфліктні інформаційні відносини # відносини інформаційні, спрямовані

на забезпечення захисту інформаційного і інформаційного суперництва реальних систем інформаційних. Складають зміст боротьби інформаційної. Реалізуються інформаційно-ударними угрупованнями сил та засобів.

conflict resolution – розв'язання конфліктів # розв'язання проблеми повторюваних відповідностей в заснованій на правилах системі, на основі вибору найбільш відповідного правила # повторювані відповідності можуть виникнути під час зіставленні з шаблонами чи в лівій частині правила, де два правила створюють суперечливі твердження.

conformance – див. conformity.

conformity – відповідність # виконання вимоги # термін conformance є синонімом, але не рекомендований для застосування.

confrontation – протиборство # боротьба проти будь-чого, будь-кого, протидія.

connection admission control – керування допустимості з'єднання # сукупність дій мережі на фазі встановлення з'єднання, яка визначає, чи сприймати з'єднання, чи скидати його, щоб не погіршити якість обслуговування у вже існуючих з'єднаннях.

connectivity-oriented interconnection – в аємоз'єднання, орієнтоване на зв'язність # фізичне та логічне зв'язування вузлів операторів і постачальників сервісів на базі простої IP-з'єднаності незалежно від рівнів взаємодії.

connection-endpoint кінцевий – пункт з'єднання # кінцевий елемент на кінці з'єднання в пункті доступу до сервісу.

connectionless service – сервіс без встановлення з'єднання # сервіс, який дозволяє переносити інформацію між користувачами без встановлення з'єднання з кінця в кінець.

connection-mode transmission – передавання у режимі з установленням з'єднання # передавання даних у контексті з'єднання n-го рівня.

connection-oriented service – сервіс, орієнтований на з'єднання # сервіс, який вимагає встановлення з'єднання з кінця в кінець для перенесення інформації між користувачами.

connectivity – під'єднуваність # 1. здатність системи або пристрою бути під'єднаним до заданої комп'ютерної мережі # *2.* властивість комп'ютерної мережі, за якої завжди можна під'єднати будь-які два пристрої цієї мережі # *3.* здатність системи або пристрою бути під'єднаним до інших систем або пристроїв без внесення змін.

consequence – наслідок # результат події, яка впливає на об'єкт. Подія може спричинити ряд наслідків. Наслідок може бути безперечним або сумнівним і в контексті інформаційної безпеки зазвичай негативним. Наслідки може бути визначено на якісному або

кількісному рівні. Початкові наслідки можуть збільшуватися внаслідок ударного ефекту.

constant check of information security – контроль захисту інформації постійний # контроль захисту інформації, який здійснюється вибірково силами служби безпеки з притягненням співробітників організації з метою об'єктивної оцінки рівня захисту інформації і, насамперед, виявлення слабких місць в системі захисту. Такий контроль здійснює психологічний вплив на співробітників організації, що примушує їх більш ретельно виконувати вимоги забезпечення захисту інформації.

constant ratio code – код з постійною вагою # код, в якому всі знаки являють комбінації двійкових цифр, що мають постійне співвідношення нулів і одиниць.

constant-length code – рівномірний код # код, в якому всі комбінації кодові мають однакову довжину.

constraining rule – правило обмеження # правило, яке є частиною засобів моделювання даних та яке керує специфікацією обмежень, які можуть бути представлені через набори даних.

constraint – обмеження # обмеження на значення, припустимі для наданого набору даних.

construction – конструкція # 1. будова, взаємне розташування частин машини, апарата, приладу тощо; структура # 2. споруди складної будови, а також частини споруд.

construction engineering protection of object – конструкція інженерного захисту об'єкта # елементи підсистеми інженерного захисту, призначені для механічного запобігання проникненню зловмисника до джерел інформації. В найбільш загальному випадкові до інженерних конструкцій і споруд відносяться: природні і штучні перепони (бар'єри) на можливому шляху пересування зловмисника до джерел інформації або інших цінностей; двері і вікна будівель і приміщень; пункти контрольно-пропускні для контрольованого пропускання на територію, що охороняється, людей і транспорту; шафи і робочі столи з ящиками, що закриваються на ключ; сховища, металеві шафи і сейфи.

contact – контакт # безпосереднє спілкування, стикання з будь-ким.

contact bounce – вібрація контактів # небажане встановлення та розрив з'єднання під час розмиканні чи замиканні контакту.

contact protection – захист контактів # захист механічного контакту від надструму чи перенапруги.

contagious program – вірусоносій # в обчислювальній техніці – програма, заражена вірусом комп'ютерним.

container – контейнер # 1. пристрій для зберігання та транспортування будь-чого # 2. у стеганографії – відкрите повідомлення, частина якого є принципово випадковою або шумовою (наприклад, дані вимірів, випадкові завади в графічних та

звукових файлах, похибки заокруглення при різних перетвореннях даних).

contamination – змішування даних різних категорій таємності; контамінація # введення даних однієї класифікації безпеки чи категорії безпеки до даниих нижчої класифікації безпеки чи іншої категорії безпеки.

content of information impact – вплив змісту інформації # складова частина впливу переконуючого, ефективність якої в певній мірі залежить від характеристик змісту інформації: доказовості і переконливості; підбору, побудови й подання аргументації; підбору й подання закликів; форми впливу.

contention – конфлікт # *1.* ситуація, коли протокол керування доступом до середовища дає змогу двом або більше станціям пересилання даних розпочати одночасне пересилання й, таким чином, створити ризик конфлікту # *2.* стан, що виникає, коли дві чи більше станції пересилання даних намагаються одночасно передавати через один і той самий канал пересилання.

context – контекст # середовище з визначеними граничними умовами, в якому існують і взаємодіють об'єкти.

contingency plan – резервний план # план щодо процедур резервного копіювання, екстреного (аварійного) реагування та післяаварійного відновлювання.

contingency procedure – процедура реагування на аварійні ситуації # процедура, яка є альтернативою нормальному перебігу процесу, якщо відбувається незвичайна, але передбачувана ситуація.

continual improvement – постійне вдосконалення # повторювані дії для покращення ефективності результативності.

contrast – контрастність # різко окреслена протилежність в чомусь.

control – **1.** керування # *1.* направлення ходу, руху кого-, чого-небудь # *2.* процес цілеспрямованої дії на об’єкт, що здійснюється з метою організації його функціонування згідно заданої програми # див. management, agency # **2.** керування доступом # контроль доступу # заходи для забезпечення доступу або запобігання несанкціонованому доступу до ресурсів системи опрацювання даних тільки авторизованим суб’єктам авторизованим способом або запобігання несанкціонованому доступу до ресурсів неавторизованих суб’єктів несанкціонованим способом # заходи для гарантії того, що доступ до ресурсів СУІБ є авторизованим та обмеженим на основі вимог бізнесу та безпеки # **3.** засіб керування # вживання заходів, які змінюють ризик # до засобів керування відноситься будь-який процес, політику, пристрій, усталена практика чи інші дії, які змінюють ризик # засоби керування не завжди можуть призводити до запланованих або передбачуваним змінам # **4.** заходи безпеки # заходи, які модифікують ризик. Заходи безпеки

містять будь-які процеси, політику, механізми, практику або інші дії, які модифікують ризик**.** Заходи безпеки не завжди призводять до наперед задуманого чи передбаченого ефекту модифікації ризику.

control breakpoint – контрольна точка переривання # точка зупину, яка залежить від виконання конкретної інструкції.

control object – об'єкт керування # 1. система, в якій відбуваються процеси, що підлягають керуванню. Як об'єкти керування можуть виступати не тільки фізичні (технічні) системи, але і біологічні, екологічні, економічні, організаційні, інформаційні і т.ін. # 2. пасивний інформаційний діяч.

control objective – мета керування # опис того, що повинно бути досягнуто в результаті застосування засобів керування.

control objective – ціль заходу безпеки # твердження, яке описує, чого саме має бути досягнуто в результаті застосування заходу безпеки.

control segment – підсистема керування # частина системи охорони об'єктів, що забезпечує функціонування системи і керування її елементами в різноманітних ситуаціях.

control station – керівна станція # станція керування # у базовому режимі керування каналом зв'язку, станція пересилання даних, яка призначає головну станцію, і контролює процедури опитування, вибору, запиту та відновлювання.

controlled maintenance – контрольоване технічне обслуговування # технічне обслуговування на основі схеми керування, згідно з якою бажана якість обслуговування може підтримуватися з мінімальними чи зменшеними витратами на технічне обслуговування.

controlled zone – контрольована зона # фізично огороджена або умовно (в документах) позначена територія, в межах якої забезпечується захист інформації або проводяться заходи захисту інформації. Зовнішньою межею контрольованої зони є межа території підприємства, організації державних або комерційних структур. Межами з. к. держави є державний кордон.

convergence – конвергенція # збіг ознак, властивостей у явищах, між собою не пов'язаних, незалежних.

convergence branches of information industry – конвергенція галузей інформаційної індустрії # процес об'єднання різних технологій, ринків, форм регулювання різноманітних галузей індустрії інформаційної. В цьому випадку здійснюється розмивання границь між секторами інформаційної індустрії, такими як виробництво телекомунікаційного обладнання, комп'ютерів, надання телекомунікаційних мережіпїх послуг, розроблення програмного забезпечення, мультимедійні (аудіовізуальні) розподільчі мережі, виробництво змісту. В умовах

конвергенції підвищується регулююча роль держави в таких галузях, як керування радіочастотним спектром з метою розподілу частот між конкурентами, забезпечення технічними стандартами для сумісності систем, сприяння досягненню національних інтересів в сфері політики інформаційної.

conviction – переконаність # глибока упевненість в істинності засвоєних ідей, уявлень, понять, образів. Вона дозволяє приймати однозначні рішення і здійснювати їх без вагань, займати тверду позицію в оцінках цих чи інших фактів і явищ. На основі упевненості формуються установки людей, які визначають їхню поведінку в конкретних ситуаціях. Важлива характеристика переконаність – її глибина. Вона зв'язана з попереднім вихованням людей, їхньою інформованістю, життєвим досвідом, здатністю аналізувати явища навколишнього світу. Глибока упевненість характеризується великою стійкістю, щоб її похитнути недостатньо тільки логічних висновків.

convincingness – переконливість # характеристика змісту інформації доводити що-небудь комусь, змушувати кого-небудь повірити у щось, погодитися з ким- чим-небудь. Переконливість залежить у значній мірі від урахування притаманних об'єкту впливу установок, переконань, інтересів, потреб, його напряму думок, національно-психологічних особливостей і своєрідності мови. Переконливість не входить до доказовості автоматично. її може забезпечити тільки правильна пропорція між логічною і емоційною компонентами інформаційного повідомлення. При розробці впливу змістом інформації виходять із того, що: зміст інформаційно-пропагандистських матеріалів повинен бути добре обдуманим і відповідати законам формальної логіки; конкретне у змісті інформаційного повідомлення є переконливішим за абстрактне; чим більш динамічніший текст, тим яскравіші і різноманітніші в ньому факти, тим більше він привертає увагу; краще сприймається те, що є ближчим до інтересів і потреб об'єкта впливу; краще осмислюється те, що подається невеликими смисловими частинами (блоками); краще засвоюється те, що викликає відгук у об'єкта впливу; краще сприймається, осмислюється й засвоюється матеріал (інформація), який подається у відповідності до національних традицій сприйняття об'єкта.

cooperation – взаємодія # див. interaction.

co-operation – кооперація # 1. форма організації праці, за якої певна кількість людей спільно бере участь в одному й тому ж або різних, або зв'язаних між собою, виробничих процесах # 2. добровільні об'єднання людей для спільної господарської діяльності.

coordination – взаємодія # див. interaction.

copy – копіювати # зчитати дані з початкового носія даних, залишаючи вихідні дані незмінними, і записати ті самі дані на цільовий носії даних, який може відрізнятися від початкового носія # наприклад: копіювання файлу з магнітної стрічки на магнітний диск.

copy protection – захист від копіювання # використання спеціальних методів для виявлення чи запобігання несанкціонованому копіюванню даних, програмного забезпечення чи вбудованого мікропрограмного забезпечення.

copyright – авторське право # сукупність законодавчих норм, що визначають правове положення автора по відношенню до створених ним об'єктів авторського права. Авторське право не розповсюджують на ідеї, методи, процеси, системи, способи, концепції, принципи, відкриття, факти. Авторові по відношенню до його творів належать особисті немайнові права (право авторства, право на ім'я, право на обнародування творів, право на захист своєї репутації) і майнові права (виключні права на використання твору в будь-якій формі і будь-яким способом, зокрема право на відтворення, право на розповсюдження, право на публічний показ, право на передачу в ефір, право на переклад, право на перероблення). Власник виняткових авторських прав для повідомлення про свої права вправі застосувати знак охорони авторського права, який розташовується на кожному екземплярі твору і складається з трьох елементів: латинської букви «С» в колі ©; імені (найменування) власника виключних авторських прав; року першого опублікування твору.

copyright legislation – законодавство про інтелектуальну власність # галузь законодавства інформаційного, основою якого є норми інформаційно-правові про захист законом власності інтелектуальної, а також про право кожного вільно шукати, одержувати, передавати, створювати і розповсюджувати інформацію будь-яким законним способом, гарантії для кожного свободи літературного, художнього, наукового, технічного та інших видів творчості, викладання. Результати творчої діяльності охороняються правом авторським, законодавством про промислову власність і про ноу-хау. Право про інтелектуальну власність закріплюється: фактом створення твору; шляхом реєстрації формули (змісту) винаходу; шляхом фіксації і зберігання в таємниці результату творчості. В перших двох випадках інформація, що створюється в процесі творчості і супроводжує цей процес, не потребує додаткового захисту, оскільки вона або сама є таким результатом або містить опис результату творчості. Додаткового захисту потребує інформація, що

відображає секрети виробництва або секрети науки. Законодавство про інтелектуальну власність можна поділити, в свою чергу, на: законодавство про авторське право і суміжні права, патентне законодавство і законодавство про ноу-хау.

copyright object – об’єкт авторського права # первинні твори, в тому числі літературні (включаючи програми для ЕОМ), і так звані вторинні, тобто похідні твори (переклади, обробки, анотації, реферати, резюме, огляди, інші переробки творів науки, літератури і мистецтва), а також збірники та інші складені твори, що являють собою за підбором і розташуванням матеріалу результати творчої праці (енциклопедії, антології, бази даних). Не є об’єктами авторського права офіційні документи, їхні офіційні переклади; повідомлення про події і факти, що мають інформаційний характер.

core image – відображення пам'яті # представлення комп'ютерної програми та пов'язаних з нею даних, які існують на той час, коли вони знаходяться в оперативній пам'яті.

core network – опорна мережа # частина системи доставки інформації, що утворена з мереж, обладнання систем та інфраструктур, яка з’єднує постачальника сервісу з мережею доступу.

corner reflector – кутовий відбивач # див. angle reflector.

corporate information computer network – інформаційно-обчислювальна корпоративна мережа # основна складова частина системи керування корпорації автоматизованої, що об’єднує наступні елементи: мережі обміну інформацією; мережі обчислювальні локальні і комплекси засобів автоматизації регіональних представництв, підключених до базової мережі; підмережі і комплекси засобів автоматизації підприємств; підмережі робочих груп і т.ін. До особливостей інформаційно-обчислювальної корпоративної мережі можна віднести: різнорідність технічних засобів і програмного забезпечення; висока доля різнорідних мережі її їх інформаційних технологій; широкий спектр послуг і, як наслідок, збільшення обсягів і якісної різноманітності інформації, що зберігається, обробляється і передається в мережі. Для інформаційно-обчислювальної корпоративної мережі можуть бути актуальними: з’єднання з глобальними мережами типу Інтернет; приєднання до мереж інших корпорацій в результаті розширення співробітництва (наприклад, міжнародного). Перелічені особливості інформаційно-обчислювальної корпоративної мережі обумовлюють високу ступінь уразливості інформації, що зберігається, обробляється й передається в такій мережі.

corporate information security policy – корпоративна політика інформаційної безпеки # документ, що відображає напрямок менеджменту та забезпечення інформаційної безпеки відповідно до бізнес-вимог організації та відповідає правовим і регулюючим нормам # документ описує високорівневі вимоги інформаційної безпеки, які мають виконуватися усюди в організації

corporative – корпоративний # той, що належить до корпорації, властивий, характерний якійсь корпорації; вузькогруповий, відособлений.

correct misinformation – правильне дезінформування # передавання органу керування неспотвореної інформації про неправдиву обстановку.

correcting code – коректувальний код # код, який дозволяє виявляти і виправляти помилки при передаванні і обробленні інформації.

correction – корекція # дії для усунення виявленої невідповідності.

corrective action – коригувальні дії # дії для усунення причини виявленої невідповідності і запобігання її повторної прояви.

corrective maintenance – корегувальне [технічне] обслуговування # технічне обслуговування з усуванням несправностей # технічне обслуговування, яке виконують після виникнення помилки чи виявлення несправності, щоб повернути функційний блок до стану, коли він зможе виконати необхідну функцію.

correctness estimation of information – оцінки вірогідності інформації # дані, що враховують вірогідність джерела інформації, оцінка автора та методів, що використовуються в роботі інформаційній.

correctness proving – перевірка достовірності формальна математична демонстрація того, що семантика програми відповідає специфікаціям цієї програми.

CoS – class of service – **1.** клас сервісу # **2.** клас обслуговування.

cosmic apparatus – космічний апарат # технічні пристрої для виконання завдань у космосі (космічний корабель, орбітальна станція, міжпланетна автоматична станція, і т. ін.). За способом участі людини у функціонуванні космічного апарата їх поділяють на автоматичні, пілотовані і комбіновані; за призначенням – на науково-дослідницькі і прикладні (метеорологічні, навігаційні, розвідувальні, зв’язку і т. ін.).

count check – контроль підрахунком # перевірка правильності передавання даних підрахунком кількості переданих повідомлень і порівнянням його з вказаним числом.

counteraction – протидія # дія, що перешкоджає іншій дії.

counteraction eavesdropping – протидія підслухуванню # сукупність дій, спрямованих на блокування будь-яких каналів (акустичних і складених), за допомогою яких здійснюється витік інформації акустичної. У відповідності до

загальних методів захисту інформації для захисту від підслухування застосовуються наступні способи: приховування інформаційне мовної інформації; приховування енергетичне акустичних сигналів; запобігання витоку інформації через закладні підслуховуючі пристрої.

counteraction information weapons – протидія інформаційній зброї # сукупність заходів, що включають: захист матеріально-технічних об'єктів, які складають фізичну основу інформаційних ресурсів; забезпечення нормального і безперебійного функціонування баз і банків даних; захист інформації від доступу несанкціонованого, спотворення або знищення; збереження якості інформації (своєчасності, точності, повноти) і необхідної доступності; створення технологій виявлення впливів на інформацію, в тому числі і у відкритих мережах.

counteraction radar observation – протидія радіолокаційному спостереженню # сукупність дій, спрямованих на запобігання одержання радіолокаційного зображення об'єкта. Заходи захисту в даному випадку спрямовані на пониження ЕПР об'єкта в цілому і його характерних ділянок, що містять інформативні демаскуючі ознаки. Можна виділити два основних способи протидія радіолокаційному спостереженню – інформаційне приховування об'єкта радіолокаційного спостереження та приховування енергетичне об'єкта радіолокаційного спостереження спеціальною інформацією) даних, які підлягають шифруванню за допомогою алгоритму RSA.

counteraction radar surveillance – протидія радіолокаційному спостереженню # див. counteraction radar observation.

counteraction security threats – протидія загрозам безпеки # основне завдання захисту системи оброблення інформації, вирішення якої визначає ступінь захищеності системи. Вирішується двома методами: створенням засобів захисту від кожного виду загроз; усуненням причин, що зумовлюють успішну реалізацію загроз.

countercountermeasures – контр протидія # див. anticountermeasures.

counterespionage – контршпіонаж # сукупність заходів контррозвідки, спрямованих на недопущення попадання секретних матеріалів в руки представників іноземних служб розвідувальних.

counterespionage activities – контррозвідка # 1. діяльність спеціальних органів держави з метою боротьби проти розвідок інших держав (попередження замахів, шпіонажу, диверсійної та підривної діяльності) # 2. протидія розвідці агентурній конфронтуючої сторони # 3. назва самих органів.

counterintelligence – контршпіонаж # див. counterespionage.

counterintelligence agency – орган контррозвідки # див. counterespionage activities.

countermeasure – зустрічний захід # контрзахід # дія, обладнання, процедура, метод або інший захід, призначений для мінімізації вразливості.

coverage object – об’єкт прикриття # споруди і конструкції, що створюють ознаки фальшивого об’єкта для дезінформування противника. Фальшиві споруди можуть бути плоскими і об’ємними, функціональними і нефункціональними. Об’ємні і функціональні споруди повинні відтворювати повний набір демаскуючих ознак о. п. протягом усього періоду захисту.

covert channel – прихований канал # канал витоку інформації # канал пересилання, який може застосовуватися для пересилання даних таким чином, що порушує політику безпеки.

covert channels – аналіз прихованих каналів # послуга безпеки, яка забезпечує гарантію того, що канали приховані в системі комп’ютерній відсутні, знаходяться під наглядом або, принаймні, відомі.

covert threat – загроза прихована # неусвідомлювані системою інформаційною в режимі реального часу вхідні дані, що загрожують її безпеці.

CPS – certification practices statement – документальне підтвердження сертифікації.

cracker – крекер # особа, яка порушує систему захисту автоматизованої системи з корисливими інтересами.

craft – літальний апарат # див. airborne vehicle.

crash – аварійна відмова # відмова системи, що вимагає для відновлення її нормального функціонування втручання оператора, а інколи і ремонтних робіт.

credential – повноваження # об'єкт даних, який забезпечує інформацію щодо автентифікації, такі як відкритий ключ разом з іншими полями ідентифікаторів. Об'єкт, який ідентифікується через повноваження, зазвичай володіє секретним або приватним ключем, який може бути використаний, щоб довести свою ідентичність.

credential service provider – постачальник сервісу повноважень # довірена особа, яка приймає рішення і/або керує повноваженнями.

credentials – облікові дані # реєстраційні дані # посвідчення особи # дані, передані для встановлення заявленої ідентичності об'єкта.

credit/blame assignment – присвоювання коефіцієнта «довіра/вина» може недовіра # визначення рішень або операторів, відповідальних за успіх чи невдачу досягнення мети.

crime – злочин # 1. суспільно небезпечна дія, що чинить зло людям; злочинство, злодіяння # 2. неприпустимий, ганебний вчинок.

criminal – злочинець # особа, що здійснила злочин; правопорушник, беззаконник.

crisis – криза # різкий, крутий перелом в будь-чому; важкий перехідний стан; важке положення.

criteria – критерій # мірило для визначення, оцінки предмета, явища; ознака, взята за основу класифікації.

criterion – критерій # див. criteria.

criterion – показник # дані, за якими можна робити висновок про розвиток, хід, стан будь-чого.

criterion of quality and quantity of information obtained – показник якості і кількості добутої інформації # показники, призначені для визначення ефективності органів добування інформації. До них відносяться: повнота добутої інформації; своєчасність добутої інформації; достовірність добутої інформації; точність вимірювання ознак; сумарні витрати на одержання інформації.

CRL – certificate revocation list – список анульованих сертифікатів.

CRM – customer relationship management – керування взаємозв'язками з клієнтами.

crosstalk – перехресні завади # порушення, спричинене в схемі небажаним пересиланням енергії від іншої схеми.

cryptanalysis – криптоаналіз # 1. наука, що займається вивченням і розробкою методів, способів та засобів дешифрування # 2. процес оброблення шифрограми з метою визначення застосованого шифру та відповідного ключа, що необхідні для виділення вихідної інформації (тексту відкритого).

cryptanalyst – криптоаналітик # фахівець, що займається розробленням атак крипто аналітичних на криптосистеми. Опонент кріпи ографові.

cryptanalytical attack – криптоаналітична атака # спроба зламати код або знайти ключ за допомогою аналітичних методів # наприклад статистичний аналіз шаблонів, пошук дефектів алгоритмі шифрування # контраст з методом перебору всіх можливих варіантів.

cryptic code – криптографічний код # див. cryptographic code.

cryptment – засекречування # див. classifying, classification, scrambling, security.

cryptoanalysis – криптографічний аналіз # див. cryptanalysis.

cryptoanalytic attack – криптоаналітична атака # загальна назва методу, яким криптоаналітик намагається зламати криптосистему. У загальному випадку, атака не є алгоритмом злому криптосистеми, а деякою спробою злому, в результаті чого отримують інформацію, що використовують в подальшому для розробки спеціального алгоритму. Криптоаналітична атака за інформацією, якою володіє криптоаналітик, ділять на: атака криптоаналітична лише із криптотекстол атака криптоаналітична з відомим відкритим текстом, атака

криптоаналітична з вибраним відкритим текстом, атака криптоаналітична з вибраним криптотекстом, атака криптоаналітична з вибраним ключем. При всіх криптоаналітичних атаках за припципами Кергхофа вважають, що криптоаналітикові відома повна інформація про алгоритм шифрування, за винятком ключа.

cryptogram – криптограма # 1. шифротекст. підготовлений для відправки каналами зв’язку # 2. тайнопис.

cryptographer – криптограф # фахівець, що займається розробкою криптосистем.

cryptographic binding – криптографічне зв'язування # об'єкт даних, побудований з використанням криптографічних операцій для об'єднання секретних даних з іншими довільними об’єктами даних таким чином, що може бути доведено, що результат був створений тільки юридичною особою, яка має знання цього секрету.

cryptographic checkvalue – криптографічне контрольне значення # інформація, отримана в результаті виконання криптографічного перетворення блоку даних. Контрольне значення може бути отримане шляхом виконання одного або декількох кроків і є результатом математичної функції ключа і блоку даних. Воно, зазвичай, використовується для перевірки цілісності блоку даних # див. cryptography.

cryptographic code – криптографічний код # одна з форм шифру заміни, яка оперує зі смисловими одиницями тексту. При цьому останні замінюються кодовими термінами.

cryptographic key – криптографічний ключ # параметр, який визначає роботу криптографічної функції, такої як: a) перехід від простого тексту до шифрованого тексту і навпаки; b) синхронізована генерація ключових матеріалів; c) обчислення або перевірка цифрового підпису.

cryptographic system – криптографічна система # документація, пристрої, обладнання та пов'язані з ними методи, що застосовуються разом для забезпечення процесу шифрування чи дешифрування.

cryptographic writing – таинопис # умовне таємне письмо; класичний метод забезпечення секретності переписки у розвідці.

cryptographical protection method – криптографічний метод захисту # метод захисту інформаційний, що полягає у перетворенні криптографічному інформації.

cryptographical security – криптографічний захист # вид захисту, що реалізується за допомогою перетворень (перетворень криптографічних) інформації з використанням спеціальних параметрів (ключових даних) з метою приховування (або відновлення) змісту інформації,

підтвердження її справжності, цілісності, авторства тощо.

cryptographical transformation – криптографічне перетворення # 1. метод захисту інформації, що полягає в перетворенні (шифруванні) її складових частин (слів, букв, складів, цифр) за допомогою спеціальних алгоритмів або апаратних засобів і кодів ключів, тобто приведення інформації до неявного виду. Для ознайомлення із шифрованою інформацією застосовується зворотний процес: декодування (дешифрування). Використання криптографічного перетворення є одним із розповсюджених методів, що значно підвищує безпеку передавання даних у мережах ЕОМ, даних, що зберігаються у віддалених пристроях пам'яті, і при обміні інформацією між віддаленими об'єктами (терміналами) # 2. перетворення даних, яке полягає в їхньому шифруванні, виробленні імітовставки або підпису цифрового.

cryptographical transformation – криптоперетворення # 1. криптографічне перетворення # 2. сукупність операцій шифрування даних, а також формування коду автентифікації, імітовставки, хеш-коду та підпису цифрового.

cryptographically protected data – зашифровані дані # мація, до якої застосована операція зашифровування.

cryptography – криптографія # 1. наука, що займається вивченням і розробкою методів створення криптосистем # 2. спосіб тайнопису, заснований на використанні шифру.

cryptography – криптографія # дисципліна, що охоплює принципи, засоби і методи перетворення даних для приховування їхнього інформаційного вмісту, запобігання їх модифікації, яку не можливо виявити, і/або їх несанкціонованого використання. Криптографія встановлює методи, що використовуються при шифруванні і дешифруванні. Будь-яке вторгнення в криптографічні принципи, засоби або методи, є криптоаналізом.

cryptography primitive – криптографічний примітив # елемент (операція або процедура) для вирішення деякої задачі криптографічного захисту інформації. В якості криптографічного примітива можуть виступати генератор псевдовипадкової послідовності, процедура обчислення хеш-функції, алгоритм криптографічного перетворення і т.ін.

cryptography war – криптографічна війна # процес боротьби між криптографом та кріпиоапалігиком.

cryptological hardness – криптостійкість # див. cryptosecurity, resistance to cryptoanalysis, cipher strength.

cryptology – криптологія # наука, складовими якої є криптографія та кріпиоаналіз. За іншим визначенням криптологія охоплює також стеганографію.

cryptonym – криптонім # псевдонім агента або кодове найменування операції (програми), що присвоюється з метою забезпечення безпеки.

cryptoperiod – криптоперіод # період часу впродовж якого ключі на законній основі використовуються в кріпи осіістсмі законними абонентами. Криптоперіод використовується для обмеження обсягу інформації (відносно даного ключа), яка доступна крпп гоаналі гпкоіп: обмеження потенційних збитків від компрометації даного ключа; обмеження використання даного ключа при закінченні його терміну дії; обмеження часу обчислень для проведення атак крипто аналітичних.

cryptosecurity – криптостійкість # характеристика шифру, що показує його стійкість до дешифрування і визначається часом та обчислювальними ресурсами, які необхідні для дешифрування.

cryptosecurity in computational sense – криптостійкість в обчислювальному сенсі # те ж, що криптостійкість практична.

cryptosecurity in information-theoretical sense – криптостійкість у теоретико-інформаційному сенсі # див. perfect cryptosecurity.

cryptosystem – криптосистема # 1. криптографічна система # 2. система для перетворення криптографічного інформації, що містить у собі п’ять компонентів: множину вхідних текстів (відкритих текстів), множину шифртекстів, множину ключів, сім’ю шифруючих (зашифровуючих та розшифровуючих) перетворень.

cryptosystem with a secret key – криптосистема із секретним ключем # криптосистема, у якої один і той же ключ використовується для зашифровування і розшифровування інформації. Такі криптосистеми також називаються одноключовими, симетричними, звичайними, двосторонніми або класичними. В них використовується шифрування блокове і потокове.

cryptotext-only attack – криптоаналітична атака лише із криптотекстом # криптоаналітична атака, при якій крипто аналітику відома певна кількість крипто-текстів, зашифрованих з використанням одного і того ж ключа. Для даного методу атаки широко використовуються методи математичної статистики. Окремим випадком цієї атаки є криптоаналітична атака методом прямого перебору ключів або силова криптоаналітична атака (brute force attack), яку складають з перебору всіх ключів з простору ключів.

CSR – certificate signing request – запит на підпис сертифікату.

CSR – certificate signing request – запит щодо підпису сертифікату.

CTCPEC – canadian trusted computer product evaluation criterion – канадські критерії безпеки комп’ютерних систем.

CUG – closed user group – обмежене коло користувачів.

cumulation – накопичення # див. accumulation.

curator – куратор # 1. особа, що їй доручено загальний нагляд за якоюсь роботою # 2. співробітник розвідки, залучена до співробітництва особа або агент-груповод, який безпосередньо керує роботою одного або декількох агентів.

custom line – лінія абонентська # лінія зв'язку, яка з'єднує пункт абонентський з центром обчислювальним.

customer – клієнт # див. client.

cutover – перехід (до нової системи) # перемикання (на нову систему) # пересилання функцій системи її наступнику в заданий момент.

cyber money – кібер-гроші # е-гроші # див. electronic money, e-money, e-cash.

cybernetic war – кібернетична війна # концепція ведення війни з використанням моделей і імітації. Так як багато об'єктів, проти яких проводяться операції інформаційної війни, не існують фізично, вони можуть бути подані тільки моделями. Розробка таких високоточних моделей є одною з функцій кібернетичної війни. Ці моделі повинні відображати усі аспекти фактичної війни в реальному часі. Близьке до реальної дійсності кібернетичне моделювання бойової обстановки дозволяє не тільки заощадити кошти на навчання і тренування особового складу збройних сил, але і випробувати різноманітні сценарії бойових дій і тактичних прийомів без людських і матеріальних утрат. Операції і засоби інформаційної війни все більше застосовуються для імітаційного моделювання, від індивідуального навчання особового складу до підтримки широкомасштабних навчань і планування воєнних операцій.

cyberspace – кіберспеис # кібернетичний простір. Термін, утворений від слова кібернетика і вживається для позначення сфери діяльності, зв'язаної із застосуванням комп'ютерної техніки і супермагістралей інформаційних.

cycle – цикл # сукупність взаємопов'язаних явищ, процесів, робіт, яка створює закінчене коло дій протягом певного проміжку часу.

cyclic code – циклічний код # лінійний , в якому якщо w є словом коду, то кодовими словами будуть і всі результати циклічного зсуву w.

cylinder lock – циліндрові замки # замки механічні, що діють за принципом сувальдних, але в іншому конструктивному виконанні. Циліндричний механізм в зібраному вигляді являє собою однорядний або дворядний сувальдний пристрій. Сердечник обертається, коли верхні торці вставлених в нього штифтів розташовані урівень з поверхнею цього сердечника, що можливо тільки при наявності в ключовому пазові «свого» ключа. Подібні замки мають малу замкову щілину і легкий плоский ключ.

D

DAA – designated approving authority – орган сертифікації.

daemon – програмний агент # процедура, яка активізується без явного виклику, коли відбувається зміна, додавання, видалення чи інша подія.

data – дані # інформація # *1.* переосмислене подання інформації формалізованим способом, придатним для обміну, інтерпретації чи опрацювання # *2.* сукупність значень, що відносяться до основних і похідних заходів і/або показниками [індикаторами] # дані можуть оброблятися людьми чи автоматичними засобами # див. information.

data administrator – адміністратор даних # особа, що має повну уяву продані, які використовуються в установі (на підприємстві), і відповідає за зберігання, оновлення та організацію їхнього використання.

data authentication – автентифікація даних # процес, що його застосовують для перевірки цілісності даних # наприклад перевірка того, що отримані дані ідентичні відправленим даним, перевірка того, що програма не заражена вірусом.

data availability – доступність даних # властивість даних, що полягає у можливості їхнього читання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів і т. ін.

data breakpoint – точка переривання даних # точка припинення доступу до даних, яка залежить від доступу до певного об'єкта даних.

data check – контроль даних # перевірка вірогідності і цілісності даних. Розрізняють синтаксичний, семантичний і прагматичний контроль.

data circuit – канал пересилання даних # пара пов'язаних каналів пересилання, що забезпечує засоби двостороннього пересилання даних # між комутаторами даних, канал пересилання даних може або не може містити обладнання для пересилання даних (DCE), залежно від типу інтерфейсу, що його застосовують під час обмінювання даними # між станцією пересилання даних та комутатором даних або концентратором даних канал пересилання даних містить DCE в кінцевій станції пересилання даних і може містити обладнання, подібне до DCE у комутаторі даних або місці концентратора даних.

data circuit transparency – прозорість каналу пересилання даних # здатність каналу пересилання даних передавати всі дані без зміни вмісту даних або структури даних.

data circuit-terminating equipment – прикінцеве обладнання каналу пересилання даних # на станції пересилання даних, обладнання, яке забезпечує перетворення сигналу та кодування між термінальним

обладнанням даних (ТОД) та лінією зв’язку # DCE може бути окремим обладнанням, або невід'ємною частиною ПОПД, або проміжним обладнанням # DCE може виконувати інші функції, які зазвичай виконуються в кінцевій мережі на лінії зв’язку.

data coding – кодування даних # див. coding, encoding.

data collection – збирання даних # процес ідентифікації і одержання даних від різних джерел, групування одержаних даних і подання їх у формі, необхідній для введення в ЕОМ.

data compatibility – інформаційна сумісність # використання різних баз даних автоматизованими системами оброблення інформації різних рівнів.

data content standard – стандарт контенту даних # логічна специфікація набору даних, яка досить широко застосовується в різних прикладних системах.

data corruption – пошкодження даних # випадкове чи навмисне порушення цілісності даних.

data definition – визначення даних # визначення, яке встановлює правила, яким мають відповідати один або кілька наборів екземплярів даних

data density – щільність даних # кількість символів даних, що зберігаються на одиницю довжини, області чи об'єму # щільність даних зазвичай виражають в символах на міліметр (cpmm) або символах на радіан (cprad) # на дисках, зазвичай, вказують загальну ємність диска, записана на одній або з обох сторін, а не щільність даних.

data encryption – шифрування даних # процес зашифровування і розшифровування.

data encryption procedure in telecommunication systems – процедура шифрування даних в телекомунікаційних системах # процедура, призначена для закриття всіх даних абонента або декількох полів повідомлення. Може мати два рівні: шифрування в каналі зв’язку (шифрування лінійне) і міжкінцеве (абонентське).

data exception – виняткова ситуація з даними # виняток, що виникає, коли програма намагається неправильно застосувати чи отримувати доступ до даних.

data export – експорт даних # послуга керування даними, яка знаходить у базі даних набір даних та створює копію цих даних, організовану відповідно до формату обміну даними.

data import – імпорт даних # послуга керування даними, яка включає до бази даних набір даних, організований відповідно до формату обміну даними..

data independence – незалежність даних # незалежність процесів від даних, яка полягає в тому, щоб визначення даних можна змінювати без зайвого порушення процесів.

data integrity – цілісність даних # 1. відповідність значень даних бази даних певному набору правил # 2. стан, при якому дані, що

зберігаються в комп’ютері, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважають збереженою, якщо дані не спотворені і не зруйновані (стерті).

data interchange format – формат обміну даними # набір правил структурування даних, який визначає формат даних, придатних для експорту даних з однієї системи керування даними та їх імпорт до іншої системи керування даними.

data interchange standard – стандарт обміну даними # стандарт, який визначає набір даних відповідно до правил структурування даних, такий, що набором даних можуть обмінюватися одна комп'ютерна система з іншою.

data interlock – блокування даних # захист файлу або його частини (блока, запису) шляхом заборони доступу до нього всіх користувачів, за винятком одного.

data key – ключ даних # ключі, які використовуються для операцій криптографічного перетворення над даними користувача. В системі зв’язку це, звичайно, короткострокові або ключі сеансові, однак особисті ключі криптосистем асиметричних, які використовуються для підпису цифрового є, звичайно, довгостроковими ключами.

data management – адміністративне керування даними # керування даними # сукупність функцій забезпечення необхідного представлення даних, їхнього накопичення і зберігання, поновлення, вилучення, пошуку і видачі.

data management environment – середовище керування даними # абстрактна концептуалізація даних та пов’язаних елементів обробки в комп'ютерних системах.

data management service – сервіс керування даними # послуга, яку надає система керування даними.

data management session – сеанс керування даними #період часу, на протязі якого набір послуг керування даними використовується клієнтом процесу керування даними.

data management system – система керування даними # система, що займається організацією та керуванням даними.

data manipulation – маніпулювання даними # в системах керування базами даних – звертання до бази даних і виконання пошуку, читання і модифікації її записів.

data manipulation process – процес маніпулювання даними # процес, семантика якого встановлюється правилами обробки даних в засобах моделювання даних.

data manipulation rule – правило маніпулювання даних # правило, якого або треба дотримуватись, коли процес визначається, або якого автоматично дотримується система керування даними, коли процес виконується.

data medium – носій інформації/даних # матеріальні об'єкти, що забезпечують запис, зберігання і передавання інформації у просторі і часі. Носіями інформації можуть бути: люди; матеріальні тіла (макрочастки); поля (випромінювання); елементарні частки (мікрочастки).

data medium protection device – пристрій захисту носія даних # рухомий або знімний пристрій, що дає змогу лише читання носія даних.

data message – інформаційне повідомлення # вид програми радіомовлення, яка містить оперативну інформацію про найбільш важливу подію, факт або явище, що представляють значний інтерес для більшості цих слухачів противника, на яких ведеться мовлення. Іформаційне повідомлення повинно відповісти на питання: що відбулося, де, коли, хто діяв, як, чому, які наслідки того, що трапилося. Вважають, що тривалість кожного повідомлення не повинна складати більше однієї хвилини. Повідомлення можна передавати в ефір у вигляді тематичної добірки.

data modelling facility – засіб моделювання даних # правила для визначення схем та правила маніпулювання даними, що зберігаються згідно зі схемою.

data origin – джерело даних # див. data source.

data origin authentication – автентифікація відправника даних # підтвердження того, що відправник отриманих даних відповідає заявленому.

data origin authentication – автентифікація джерела даних # функція захисту, в результаті виконання якої з певними гарантіями встановлюють належність даних (повідомлень) джерелу даних повідомлень.

data privacy – даних приватність # статус даних, що полягає в доступності даних тільки власникові або обмеженій групі користувачів; гарантована доступність даних із боку певної особи або групи осіб.

data processing system security – безпека системи оброблення даних # технологічні та адміністративні охоронні заходи, що застосовуються в системі оброблення даних для захисту обладнання, програмного забезпечення та даних від несанкціонованого, навмисного чи випадкового модифікування, розривання або руйнування.

data processing validity – достовірність оброблення інформації # функція ймовірності помилки, тобто події, яка полягає у тому, що інформація в системі не збігається у межах заданої точності з деяким її істинним значенням. Забезпечення необхідного рівня достовірності оброблення інформації є однією з основних умов ефективного функціонування автоматизованої системи. Необхідної достовірності оброблення інформації досягають застосовуванням різноманітних методів, реалізація яких потребує

введення в системи оброблення даних надмірності інформаційної, часової або структурної. Достовірність даних досягається шляхом контролю достовірності та виявлення помилок у вихідних і виведених даних, їхня локалізація і виправлення. Умова підвищення достовірності – пониження долі помилок до допустимого рівня. В конкретних системах необхідна достовірність встановлюється з врахуванням небажаних наслідків, до яких може привести помилка, що виникла, і тих затрат, які необхідні для її попередження.

data procuring – добування даних і відомостей # активні дії сил та засобів органів розвідки, спрямовані на пошук об'єктів (джерел) інформації та її носіїв, виявлення їх, встановлення з ними контакту розвідувального, одержання даних і відомостей.

data protection – захист даних # 1. впровадження відповідних, адміністративних, технічних або фізичних засобів для захисту від несанкціонованого навмисного чи випадкового поширення, модифікації чи знищення даних # 2. здійснення адміністративних, технічних або фізичних заходів для запобігання несанкціонованого доступу до даних.

data protection document – документ системи захисту інформації # документа, що визначають структуру і алгоритм функціонування системи захисту інформації організації. Розрізняють документи системи захисту інформації керівні, нормативні і методичні.

data protection efficiency – ефективність захисту інформації # здатність системи захисту інформації забезпечити достатній рівень її безпеки.

data protection **legislation** – законодавство про захист інформації (даних) # сукупність законів (норм), що регламентують законодавчі заходи, прийняті у державі для захисту інформації (даних), що оброблюються системами автоматизованими (комп'ютерами).

data protection normative document – нормативні документи системи захисту інформації # документи системи захисту інформації, які визначають перелік відомостей, що складають державну, воєнну, комерційну або будь-яку іншу таємницю. Такі документи є основними нормативними документами. Інші нормативні документи визначають максимально допустимі значення рівнів полів з інформацією і концентрації демаскуючих речовин на межах зони контрольованої, які забезпечують необхідний рівень безпеки інформації. Ці норми розроблюються відповідними відомствами, а для комерційних структур, які виконують недержавні замовлення, – фахівцями цих структур.

data protection security – захист даних # 1. оберігання даних від несанкціонованого, навмисного чи випадкового їхнього розкриття

(порушення їхньої конфіденційності), модифікації або знищення. Захист даних передбачає проведення організаційних заходів, застосування програмних та технічних методів і засобів, спрямованих на задоволення обмежень, які встановлені для типів і екземплярів даних в системі оброблення даних # 2. здатність системи керування базою даних контролювати правомочність доступу користувачів до певних порцій даних, що зберігаються, і способи використання цих даних. Механізми захисту даних усувають також можливість одночасного оновлення однієї і тієї ж порції даних декількома користувачами, що паралельно звернулися до бази даних. Для перевірки прав програм користувачів на доступ до даних і (або) їхнє оброблення вводяться так звані замки захисту.

data protection theory – теорія захисту інформації # складова частина теорії інформаційної боротьби. Охоплює загальні положення, що визначають: предмет, завдання і зміст теорії; об'єкти і елементи захисту інформації; основні фактори, що впливають на зміст і ефективність захисту інформації, а також визначає та вивчає загрози інформації і методологічні основи її захисту, систему показників оцінки ефективності захисту інформації, загальну математичну модель захисту інформації, організаційно-технічні і правові основи захисту інформації.

data reconstitution – реконструкція даних # відтворення даних # 1. метод відновлювання даних за допомогою збирання даних з компонентів, доступних в альтернативних джерелах # 2. метод відновлювання даних за допомогою аналізу першоджерел.

data recovery – відновлення даних # процес відтворення даних із носія, що містить захищену копію даних, на носій-оригінал у випадку порушення на ньому цілісності даних.

data restoration – відновлювання даних # акт поновлювання даних, які були втрачені чи забруднені # методи охоплюють копіювання даних з архіву, реконструкції даних з вихідних даних або відтворення даних з альтернативних джерел.

data security – безпека даних # захист даних # *1.* стан даних, що зберігаються, обробляються й передаються, при якому неможливе їхнє випадкове або навмисне одержання, змінювання або знищення # *2.* властивість організації доступу до даних, що забезпечує їхнє оброблення за заздалегідь установленими правилами і тільки за ними. Під такими правилами найчастіше розуміють захист даних від несанкціонованого використання, розкривання, навмисного чи ненавмисного спотворення або руйнування. За рахунок застосування організаційних, етично-правових та

технічних методів захисту досягають безпеку даних.

data structuring rule – правило структурування даних # правило, що описує те, як потрібно структурувати набір даних.

data terminal equipment – термінальне обладнання даних # частина станції пересилання даних, яка слугує джерелом даних, приймачем даних або і тим і іншим # DTE може бути під'єднано безпосередньо до комп'ютера чи може бути його частиною.

data trace – трасування даних # запис імен та значень змінних, доступних або змінюваних під час виконання програми.

data transmission network – мережа передавання даних # сукупність кіл передавання даних та пристроїв комутації, що дозволяють здійснювати взаємне з'єднання кінцевого обладнання даних.

data transmission validity – достовірність передавання інформації # ступінь відповідності прийнятого повідомлення переданому.

data type – тип даних # пойменована формальна специфікація, яка керує загальними статичними та динамічними властивостями екземплярів цих типів даних.

data validation – підтверджування правильності даних # процес, що його застосовують для визначення точності даних, повноти чи відповідності зазначеним критеріям # підтвердження правильності даних може охоплювати перевірку форматів, перевірку повноти, перевірку ключових тестів, перевірку достовірності та обмежувати перевірки.

data validity – достовірність даних # ступінь відповідності даних, що зберігаються у пам'яті ЕОМ або документах, реальному стану відображених ними об'єктів предметної області.

data volatility – мінливість даних; волатильність даних # характеристика даних, що відносяться до швидкості зміни цих даних у часі.

data source – джерело даних # людина або пристрій, які здійснюють формування і введення даних в ЕОМ.

databank – банк даних # БнД # система інформаційна автоматизована для централізованого зберігання і колективного використання даних. До складу БнД входять одна чи декілька баз даних, а також набір прикладних програм, складених на мові даної системи керування базами даних.

database – база даних # набір даних, що зберігається відповідно зі схемою та маніпулюється відповідно до набору правил в засобах моделювання даних.

database administration – адміністрування бази даних # виконання функцій визначення, організації, керування, контролю та захисту всіх даних бази даних # захищені дані також містять метадані та подання інших описів бази даних.

database administrator – адміністратор бази даних # спеціальна посадова особа (група осіб), що володіє службовою інформацією про базу даних(але не обов'язково має доступ до інформації, що зберігають в базі даних) і відповідає за її ведення, використання та розвиток. Функції адміністратора бази даних зводяться до підтримки цілісності бази даних, необхідного рівня захисту даних та її ефективності. Адміністратор бази даних входить до складу адміністрації банку даних.

database analyst – аналітик бази даних # фахівець, котрий здійснює аналітичні функції, потрібні при проектуванні та (чи) для підтримки процесу користування базами даних.

database control – керування базами даних # основна функція СКБД, яка полягає в керуванні створенням і веденням баз даних, доступом програм і користувачів до баз даних, пошуком і видачею інформації за їхніми запитами.

database controller – контролер бази даних # абстрактне подання для набору послуг, які узгоджені з конкретним засобом моделювання даних і реалізуються у ньому

database environment – середовище бази даних # база даних та пов'язані з нею схема бази даних та контролер бази даних.

database integrity – цілісність бази даних # стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несуперечливості. Підтримка цілісності бази даних охоплює перевірку цілісності і відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

database key – ключ бази даних # первинний ключ, присвоєний системою керування базами даних.

database language – мова бази даних # мова з формальним синтаксисом, що використовується для визначення, створення, доступу та підтримки баз даних.

database management – керування базою даних # створення, використання та підтримка баз даних.

database management system – система керування базами даних # набір інтегрованих послуг, які підтримують керування базами даних та керують створенням, використанням та підтримкою баз даних.

database recovery – відновлення баз даних # відтворення вмісту бази даних за резервною копією, що виконують у випадку машинних збоїв або програмних помилок для підтримання цілісності даних. Методи та засоби відновлення: копіювання, рестарт із контрольної точки, ведення журналу системного.

data-flow trace – трасування потоку даних # запис імен та значень

змінних, доступних або змінюваних під час виконання програми.

datagram – дейтаграма # дата грама # самодостатній незалежний блок даних, що містить достатню інформацію для маршрутування від джерела до місця призначення.

data-sensitive fault – чутливий до даних збій # несправність, яка може бути виявлена в результаті опрацювання певного шаблону даних.

data-sink – одержувач даних # логічний об'єкт, який приймає сервісні блоки даних n рівня по (n-1)-з'єднанню.

data-source – відправник даних # логічний об'єкт, що відправляє сервісні блоки даних від нижчого рівня по з'єднанню нижчого рівня.

DBA – database administrator – адміністратор бази даних.

DCE – data circuit-terminating equipment – прикінцеве обладнання каналу пересилання даних.

DCS – defined context set – визначена контекстна множина.

deadlock – взаємоблокування # ситуація, у якій опрацювання даних призупинено, оскільки два чи більше пристроїв або паралельних процесів чекають на ресурси, привласнені іншими чи через інші взаємозалежності # наприклад ситуація, коли програма A, що має ексклюзивне блокування на запис X, запитує блокування на запис Y, який виділяється програмі B. Аналогічно, програма B очікує ексклюзивного контролю над записом X перед тим, як відмовитися від контролю над записом Y.

decamouflage – демаскування # порушення маскування, розкривання, виділення об'єктів, що потребують захисту, перед противником.

deception message – дезінформування # див. disinformation, misinformation.

decipherement – розшифровування # процес перетворення шифртексту у текст відкритий при відомому ключі; процес, зворотний процесу зашифровування . При застосуванні багаторазового зашифровування в процесі розшифровування можна отримати і шифртекст # див. deciphering.

decipherer – дешифратор # декодер # *1.* пристрій, призначений для перетворення шифрограм у вихідні повідомлення. Зворотну функцію виконує шифратор # *2.* комбінаційна схема, яка реалізує систему з 2n булевих функцій, кожна з яких є конституентою одиниці від n змінних. Наприклад, дешифратор адреси [address decoder] реалізує вибір комірки пам'яті за сигналами на адресній шині.

deciphering – дешифрування # *1.* розшифровування (читання) тексту, написаного умовними знаками (шифром), тайнописом # *2.* процес перетворення шифртексту у відкритий текст без знання ключа та, можливо, при невідомому алгоритмі шифрування; процес, зворотний процесу зашифровування.

decipherment – дешифрування # процес отримання із шифрувального тексту, вихідних відповідних даних # шифровавний текст може бути

зашифрований повторно, і в цьому випадку одного дешифрування буде не достатньо для отримання початкового тексту.

decision criteria – критерій прийняття рішення # порогові значення, цільові значення або зразки, які використовують для визначення потреби в дії або подальшому дослідженні, або для опису рівня довіри отриманому результату.

decision criteria – критерій прийняття рішення # порогові, цільові або еталонні значення, використовувані для визначення необхідності дії або подальшого аналізу, або для опису рівня впевненості в даному результаті.

declassification – розсекречення # дія, спрямована на зняття заборони на розголошення будь-чого.

declassification of information and their carriers – розсекречення відомостей і їхніх носіїв # зняття раніше введених у передбаченому законом порядку обмежень на розповсюдження відомостей, що складають державну таємницю, і на доступ до їхніх носіїв. Основою для розсекреченню найчастіше є: узяття на себе державою міждержавних зобов'язань із відкритого обміну відомостями, що складають у даній державі державну таємницю; зміна об'єктивних обставин, внаслідок яких подальший захист відомостей, що складають державну таємницю, є недоцільним.

decode – декодовувати # дешифровувати # перетворення даних за допомогою зміни зворотного ефекту деякого попереднього кодування.

decoder – декодер # дешифратор # *1.* пристрій чи стандартна програма, що перетворює закодовані дані у первинну форму. Це іноді також означає заміну одного коду на інший # *2.* логічний пристрій, який формує один або більше виділених вихідних сигналів, що базуються на комбінації вхідних сигналів, які він одержує # див. decipherer.

decoding – декодування # перетворення кодованих даних у форму, яку вони мали до кодування; операція, обернена кодуванню.

decryption – декодування # розшифровування # дешифрація # процес отримання із шифрувального тексту, вихідних відповідних даних. # див. decipherment.

dedicated mode – спеціальний режим # режим забезпечення безпеки, при якому вся інформація в системі розглядається як інформація одного рівня секретності, рівнодоступна для всіх користувачів системи.

default protection – захист за замовчанням # призначення повноважень доступу користувачів за принципом: «усе, що не дозволено, те заборонено». Тобто всі ресурси, доступ до яких явно не дозволений користувачу, вважаються недоступними.

defense information operation – оборонна інформаційна операція # операція інформаційна, що проводиться в умовах великої переваги інформаційної противника і

має за мету зниження цієї переваги. В такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об'єднань і з'єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

deferred maintenance – відкладене технічне обслуговування # корегувальне технічне обслуговування, яке ініціюється не відразу після виявлення відмови чи виявлення збою, а затримується відповідно до правил технічного обслуговування.

deforming masks – деформуючі маски # маски оптичні штучні, призначені для створення у спостерігача неправильного уявлення про форму об'єкта, що підлягає захисту.

DEL – direct exchange line – пряма лінія обміну інформацією.

delayed – відтермінований # відкладений # стосується стану задачі виконуваного завдання, яке заблоковано за допомогою оператора затримки.

delegation – делегування # засіб, що дає змогу об'єкту призначити іншого об'єкта для обслуговування повідомлення.

demand service – сервіс за вимогою # телекомунікаційна сервіс, який передбачає негайне встановлення з'єднання на вимогу користувача, передану засобами сигналізації «користувач – мережа».

demilitarized zone – демілітаризована зона # сегмент мережі, який розташований між мережею організації та загальнодоступною мережею, звичайно Інтернет. Такі служби загальнодоступних мереж як DNS и Web-сервери звичайно установлюються в DMZ.

demodulation – демодуляція # *1.* виділення низькочастотних коливань із високочастотних модульованих коливань # *2.* Процес, зворотний модуляції. Полягає у відновленні модулюючого сигналу.

demon – демон # процедура, яка активізується без явного виклику, коли відбувається зміна, додавання, видалення чи інша подія.

denial of service – відмова в обслуговуванні # відхилення сервісу # припинення санкціонованого доступу до ресурсів системи або затримка операцій і функцій системи, що призводить до втрати приступності для авторизованих користувачів

derived measure – похідна міра # міра, яку визначають як функцію двох або більше основних заходів

derived measure – похідний показник # показник, який визначають як функцію двох або більше значень базового показника.

DES – data encryption standard – стандарт шифрування даних.

descramble – дескремблювання # відновлювання оригінального цифрового сигналу із зашифрованого цифрового сигналу.

descrambler – дескремблер # пристрій для виділення з прийнятого сигналу скрембльованого вхідного повідомлення # див. scramble, scrambling , scrambler.

description – характеристика # див. characteristic, reference.

descriptive name – описове ім'я # ім'я, що ідентифікує один об'єкт або набір декількох об'єктів за допомогою деяких тверджень щодо властивостей об'єктів цього набору.

design documentation – конструкторська документація # сукупність документів, які розроблюються і використовуються в ході проектування виробу, виготовлення дослідного зразка і при організації серійного виробництва виробу.

design documentation – проектна документація # частина документації технічної, яка містить проектні рішення на створення і експлуатацію системи, що створюється.

designated approving authority – орган сертифікації # організація, якій довірено рішення про допуск засобів захисту для забезпечення безпеки інформації в системі оброблення даних та яка в змозі нести відповідальність за забезпечення атестаційних затверджень.

destabilizing factor – дестабілізуючі фактори # явища та процеси природного і штучного походження, що породжують загрози інформаційні. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації, об’єднання. До найбільш сильних із них відносяться ворожі держави або коаліції – в них для формування інформаційних загроз створюються і функціонують спеціальні органи і служби. Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин. Джерелом дестабілізуючого фактора може бути також природне середовище. Кожному джерелу притаманні певні види дестабілізуючих факторів, які можна представити двома групами: фактори дестабілізуючі міждержавні і фактори дестабілізуючі внутрідержавні. Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

destabilizing factor source – джерело дестабілізуючих факторів # див. destabilizing factor.

destructive impact – деструктивний вплив # дія, що здійснюється для руйнування ким-, чим-небудь кого-, що-небудь.

destructive read – зчитування зі стиранням # читання, яке стирає дані у їх висхідному місцезнаходженні.

detection – виявлення розшукування, знаходження, віднаходження.

detection of unauthorized actions in the exchange network – виявлення несанкціонованих дій в мережі обміну # один з основних аспектів забезпечення переваги над противником в інформаційній війні, що полягає в збиранні та підготовці відомостей про несанкціонований доступ для реалізації заходів протидії інформаційної. Одночасно проводяться заходи, спрямовані на зменшення часу безконтрольної присутності противника в мережі обміну інформацією з вирішенням завдання реагування простого та виявник протидії інтелектуальної.

detector – виявник # пристрій для виявлення чого-небудь, а також узагалі те, за допомогою чого можна що-небудь точно визначити, встановити.

detector – детектор # *1.* пристрій для детектування електричних коливань # *2.* прилад для виявлення різних фізичних явищ, частинок і випромінювання.

deterioration of information – старіння інформації # див. aging of information.

deterministic primality test – детермінований тест на простоту # алгоритм вирішення задачі розпізнавання належності натурального числа до множини чисел простих. Прикладами детермінованих тестів є тести тест пробного ділення (сито Ератосфена), тест просіювання в загальному полі (Number Field Sieve Tets (NFST)) Босми, Ленстри та Коена та тест з використанням теорії еліптичних кривих Аткіна, Гольвассера та Кілліана.

device – пристрій # *1.* конструктивно закінчена технічна система, що має певне функціональне призначення # *2.* будь-яка одиниця, яка має єдине IDevID повноваження.

DevID – initial secure device identifier – первинний ідентифікатор захищеного пристрою.

DevID – Secure Device Identifier – ідентифікатор захищеного пристрою.

DevID Certificate – secure device identifier certificate, сертифікат ідентифікатора захищеного пристрою, сертифікат DevID.

DevID Credential – secure device identifier credential – повноваження ідентифікатора захищеного пристрою, повноваження DevID.

DevID Module – secure device identifier module – модуль ідентифікатора захищеного пристрою, модуль DevID.

DevID Secret – secure device identifier secret – ключ ідентифікатора захищеного пристрою.

devIDs – locally significant secure device identifiers – локально значимий ідентифікатор захищених пристроїв.

DHCP – dynamic host configuration protocol – протокол динамічного конфігурування від сервера.

diagnostic – діагностика # стосується виявлення, аналізу чи опису несправностей, збоїв або помилок.

diagnostic check – діагностичний контроль # перевірка функціонування ЕОМ, яка виконується за допомогою діагностичних програм і дозволяє виявляти і локалізувати несправності в обладнанні.

diagnostic function – діагностична функція # здатність функційного модулю виявляти проблеми та визначати тип помилки.

diagnostic program – програма діагностування # програма, призначена для виявлення, визначення та опису несправностей обладнання чи помилок у програмах.

diagram – діаграма #графічне зображення співвідношень між різними величинами, які порівнюються.

dictionary – словник # 1. впорядкований перелік слів, символічних імен або найменувань з їхніми значеннями або тлумаченнями # 2. в обчислювальній техніці – структура даних, що забезпечує доступ до даних за текстовим іменем.

dictionary attack – словникова атака # спроба визначення пароля або ключа шляхом перебору по ключових словах, що часто використовуються на практиці. Множина цих слів і складає словник, звідки походить назва атаки. Найбільш відомі приклади цієї атаки на схеми парольної автентифікації операційних систем.

dictionary system – словникова система # інформаційна система, що містить інформацію щодо підприємства, його операцій, діяльності та дані, пов'язані з однією або кількома прикладними системами.

differential cryptanalysis – диференційний криптоаналіз # метод криптоаналізу, що складається з аналізу впливу різниць в парах відкритого тексту на різниці в парах відповідних шифртекстів. Під «різницею» розуміється результат операції складання за модулем (0) над парами відкритого або шифртексту. Диференційний криптоаналіз є частковим випадком атаки криптоаналітичної з вибраним відкритим текстом.

differential encoding – диференційне кодування # кодування потоку цифрових даних, в якому кожен елемент окрім першого, представляється як різниця в значенні між цим елементом та попереднім елементом.

differential Manchester encoding – диференційне манчестерське кодування # кодування бінарної фази, в якій часовий інтервал, призначений кожному біту, поділений навпіл переходом та наявність або відсутність іншого переходу на початку цього інтервалу часу, визначає значення біту, відповідно «0» або «1» # перехід може відбуватися між двома станами

фізичної змінної, такими як напруга, магнітна полярність або інтенсивність світла # якщо фізична змінна є електричною, цей тип кодування не залежить від полярності й не містить постійного струму.

differentiated service – обслуговування з диференційованою якістю # схема обслуговування, яка для різних пакетних потоків передбачає до 64 рівнів обслуговування; потрібний рівень задається в заголовках IP-пакетів.

differentiation – розмежування # розділення на основі проведення, визначення і встановлення межі.

differentiation of access to information – розмежування доступу до інформації # 1. сукупність заходів, які здійснюють розділення інформації на частини і організацію доступу до неї посадових осіб у відповідності до їхніх функціональних обов'язків і повноважень # 2. сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі правил розмежування доступу можливості надання доступу.

differentiation user authority – розмежування повноважень користувачів # процедура створення в захищеній ділянці пам'яті системи обчислювальної таблиць повноважень, які містять профілі повноважень кожного користувача, термінала, процедури, процесу і т.ін. Ці профілі встановлюються за допомогою спеціальної привілейованої програми розпізнавання і контролю доступу до інформації обмеженого користування, і, як правило, задаються у вигляді матриці встановлення повноважень.

DiffServ – differentiated service – обслуговування з диференційованою якістю.

digit – цифра # графічний знак, призначений для зображення кількісних величин.

digital camera – цифровий фотографічний апарат # апарат фотографічний з світлоелектричним перетворювачем на основі приладу із зарядовим зв'язком, електричні сигнали з виходу якого перетворюються в цифровий вигляд і запам'ятовуються в напівпровідниковій пам'яті апарата або записуються на його магнітний диск. Маючи можливості класичного електромеханічного фотографічного апарата, цифровий фотографічний апарат дозволяє надати користувачеві додаткові функції, які значно підвищують оперативність фотографування. До таких функцій відносяться: можливість зйомки в безперервному режимі з частотою 5-15 кадрів/с, запис текстових і звукових коментарів, дати з часом фотозйомки, перегляд зображень у процесі і після зйомки на оборотному екрані, відображення поточних параметрів зйомки (кількості знятих кадрів, обсяг вільної пам'яті, потоковий режим компресії) і т.ін. Передбачені різноманітні режими

перегляду кадрів і стирання непотрібних, друк вибраних на спеціальному принтері. Стандартний інтерфейс цифрового фотографічного апарата дозволяє переглядати зображення на екрані телевізора, записувати на відеомагнітофон або друкувати на відеопринтері. Цифровий фотографічний апарат також може з'єднуватися з ПЕОМ для подальшого оброблення зображення: відображення на дисплеї, редагування за допомогою графічних редакторів, виведення на друк, передавання комп'ютерними мережами.

digital coding – цифрове кодування # кодування, при якому кодоване повідомлення записується у вигляді послідовності цифр і чисел.

digital encryption of language information – цифрове шифрування мовної інформації # спосіб прихову-вання інформаційного мовної інформації, заснований на шифруванні мовної інформації, яка представлена у цифровій формі. При аналого-цифровому перетворенні амплітуда сигналу вимірюється через рівні проміжки часу, що називаються кроком дискретизації. Для того, щоб цифровий мовний сигнал мав якість не гіршу телефонного, крок дискретизації не повинен перевищувати 160 мкс, а кількість рівнів квантування амплітуди мовного сигналу – не менше 128. В цьому випадку відлік амплітуди кодується 7 бітами, швидкість передавання перевищує 43 кбіт/с, а ширина спектра дискретного двійкового сигналу дорівнює сумі смуг 14 стандартних телефонних каналів. Для передавання мови в цифровій формі стандартними телефонними каналами різко скорочують смугу мовного сигналу за допомогою пристроїв, які називають вокодерами. Шифрування мовної інформації у цифровій формі здійснюється відомими методами (заміною, перестановками, аналітичними перетвореннями, гамуванням і т. ін.) або за допомогою стандартних алгоритмів криптографічного перетворення. Перевагою цифрового шифрування мовної інформації є висока надійність закриття мовної інформації, так як перехоплений сигнал являє собою випадкову цифрову послідовність. Недоліком – необхідність використання модемів, нестійка робота пристроїв шифрування в каналах з великим загасанням сигналу і з високим рівнем завад.

digital flow – цифровий потік # послідовність сигналів цифрових, що передаються каналом зв'язку.

digital money – цифрові гроші # електронний аналог готівки.

digital signature – цифровий підпис # 1. цифрова послідовність, що додається до повідомлення (даних) для забезпечення цілісності та підтвердження авторства і формується із застосуванням криптосистем асиметричних # 2. дані, одержані в результаті

перетворення криптографічного блоку даних і (або) його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальникові даних впевнитися в цілісності блоку і справжньості джерела даних і забезпечити захист від підробки та підлогу.

digital signature procedure in telecommunication systems – процедура цифрового підпису в телекомунікаційних системах # процедура, яка служить для підтвердження правильності змісту повідомлення. Вона засвідчує факт його відправлення власне тим абонентом, який вказаний в заголовку як джерело даних. Підпис цифровий є функцією від змісту таємного повідомлення, відомого тільки абоненту-джерелу, і загальної інформації, відомої всім абонентам системи.

digital switching – цифрове комутування # комутація в мережі передавання даних, при якій з'єднання встановлюється виконанням операцій над цифровими сигналами без їхнього перетворення в аналогову форму.

digital watermark – цифровий водяний знак # спеціальна позначка, яка за допомогою методів стеганографії комп'ютерної непомітно додається до інформації (зображення, музичного твору і т.ін.) з метою контролю авторських прав цієї інформації.

dipole reflector – дипольні відбивачі # радіовідбивачі, призначені для радіолокаційного маскування повітряних об'єктів. Дипольні відбивачі є смужками металізованого паперу або алюмінієвої фольги, металізовані скляні або нейлонові волокна, що розкидаються в зоні розташування об'єкта, який підлягає захисту. Довжина диполів і їхня товщина вибираються так, щоб забезпечити ефективне розсіювання радіохвиль по можливості у більш широкому діапазоні частот. Дипольні відбивачі упаковують в пачки з десятків і сотень одиниць і при викиданні з літака у повітря створюють хмару відбивачів, що помалу опускають на землю. Відбиті від них сигнали спостерігаються на екрані радіолокаційної станції у вигляді множини яскравих точок, що маскують відбитий від літака сигнал. Якщо послідовно скидати достатньо велику кількість пачок, то на екрані радіолокаційної станції створюють засвітлені смуги, в яких важко виявити повітряні об'єкти.

direct code – прямий код # код двійковий подання чисел, в якому незалежно кодуються знак і значення числа.

direct sign – пряма ознака # ознака, яка належить об'єктові, що розглядається.

directory-function – функція каталогу # функція, що обробляє адреси, символьні імена логічних об'єктів, протокольну адресну інформацію,

виконуючи операції перетворення з цими категоріями інформації.

disaster recovery plan – план аварійного відновлювання # план щодо процедур резервного копіювання, екстреного (аварійного) реагування та післяаварійного відновлювання.

disclosure – розголошення інформації # порушення комп'ютерної безпеки, через що дані стають доступними неавторизованим суб'єктам.

disclosure of other recipients service – сервіс надавання інформації про інших отримувачів # сервіс, який дає змогу користувацькому агенту відправника вимагати від системи пересилання повідомлень у разі пересилання повідомлення багатьом отримувачам одночасно, розкривати усі імена відправника/отримувача кожному користувацькому агенту відправника після доставлення повідомлення.

discovery – виявлення # див. detection.

discretionary access control – виборче керування доступом # принцип керування доступом, який полягає в тому, що звичайним користувачам дозволено керувати (довіряють керування) потоками інформації між іншими користувачами й об’єктами свого домена (наприклад, на підставі права володіння об’єктом) без утручання адміністратора.

discretionary confidentiality – довірча конфіденційність # послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

discretionary integrity – довірча цілісність # послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

discretionary access control – обмежуюче керування доступом # розмежування доступу між пойменованими суб’єктами доступу та пойменованими об’єктами доступу. Суб’єкт з певним правом доступу може передавати це право будь-якому іншому суб’єкту.

discursive – дискурсивний # той, що здійснюється шляхом логічних міркувань, розсудковий, опосередкований. Часто застосовується поняття дискурсу [discurse], що має багато значень: лекція, промова, трактат, розмова, бесіда, висловлювання, надфразна єдність, текст. В комунікативіетиці ідея дискурсивності синомізується з поняттям комунікабельності тексту як тканини, фактури і структури різноманітних мов інформації у їхньому розмовному прояві в різних соціокультурних контекстах.

disincentive protection – запобіжний захист # організаційно-правові заходи захисту від копіювання, що передбачають суворий штраф або загрозу штрафу особі, яка намагається несанкціонованим чином копіювати програму або файл.

disinformation – дезінформування # *1.* метод приховування інформації, який полягає в перетворенні (трансформації) вихідного портрета

інформаційного в новий, такий що відповідає фальшивій інформації семантичній або фальшивій структурі ознаковій, та "нав'язуванні" нового портрета органу розвідки або зловмисникові. Дезінформування відноситься до числа найбільш ефективних способів захисту інформації. Дезінформування надає власникові інформації, що потребує захисту, запас часу, який зумовлений перевіркою розвідкою достовірності одержаної інформації. Наслідки рішень, прийнятих противником на основі фальшивої інформації, можуть бути для нього гіршими у порівнянні з рішеннями, що приймаються при відсутності інформації. Основна проблема дезінформування полягає в забезпеченні достовірності фальшивого інформаційного портрета. Дезінформування здійснюється шляхом підгонки ознак інформаційного портрета об'єкта, що потребує захисту, під ознаки інформаційного портрета фальшивого об'єкта, який відповідає раніше розробленій версії. Розрізняють наступні способи дезінформування: дезінформування заміною реквізитів інформаційного портрета; дезінформування ознаками з різних інформаційних портретів реальних об'єктів; дезінформування сполученням істинних і фальшивих ознак; дезінформування зміною інформаційних вузлів. Як правило, використовуються різноманітні комбінації способів дезінформування # *2.* спосіб впливу психологічного, що полягає в намірі подання противникові такої інформації, яка вводить його в оману відносно справжнього положення справ. Дезінформування охоплює використання явно фальшивих даних і відомостей. В цьому випадку воно стає обманом. Заходи з дезінформування повинні здійснюватися за єдиним замислом; із ретельним погодженням пропорцій правди й брехні (при максимальному використанні правдоподібної інформації); з обов'язковим приховуванням справжніх намірів, мети й завдань, що вирішуються військами. Дезінформування широко застосовується в усіх видах стратегічних операцій.

disinformation by change of information nodes – дезінформування зміною інформаційних вузлів # спосіб дезінформування, що полягає у зміні тільки вузлів інформаційних із збереженням незмінною всієї іншої частини інформаційного портрета.

disinformation by replacing the details of the information portrait – дезінформування заміною реквізитів інформаційного портрета # спосіб дезінформування, який використовується у випадку, коли портрет інформаційний об'єкта захисту схожий на інформаційні портрети інших "відкритих" об'єктів і не має специфічних інформативних ознак. В цьому випадку обмежуються розробленням і

підтримуванням версії про інший об'єкт, видаючи за його ознаки об'єкта, що потребує захисту.

disinformation by signs from various information portraits of real objects – дезінформування ознаками з різних інформаційних портретів реальних об'єктів # спосіб дезінформування, спрямований на підтримування версії з ознаками, що беруться з різних портретів інформаційних реальних об'єктів. Шляхом різноманітних сполучень таких ознак можна нав'язати протилежній стороні фальшиве уявлення про об'єкти, що потребують захисту, без імітації додаткових ознак.

disinformation of the enemy in the information and computing network – дезінформування противника в інформаційно-обчислювальній мережі # санкціоноване розповсюдження в ІОМ інформації про плани, способи дій і наміри керівництва корпорації, яка не відповідає дійсності.

disorganization – дезорганізація # відсутність організованості, порушення порядку, дисципліни, нормальної діяльності, розладнаність, розвал.

disorganization of the enemy in the information-computer network – дезорганізація противника в інформаційно-обчислювальній мережі # дії, спрямовані на дезорієнтацію противника відносно об'єкта атаки, що цікавить його (інформаційного ресурсу, інформаційної системи, елемента ІОМ), а також дії з руйнування технологічно взаємозв'язаних засобів інформаційної війни, що застосовуються противником в ІОМ.

display function – функція відображення # правило, за яким кожному елементу ж деякої множини X поставлено у відповідність деякий елемент $y=f(x)$ деякої множини Y. Кажуть, що задано відображення або функція $f : X \rightarrow Y$ із множини X у множину Y.

distance – відстань вимір простору, який розділяє два пункти, предмети тощо; віддаль, відлеглість, дистанція.

distortion – спотворення # 1. представлення в хибному, неправильному вигляді # 2. неправильність, помилка.

distributed databank – розподілений банк даних # система територіально розподілених банків даних локальних, які функціонують під єдиним керуванням і об'єднуються засобами мережі обчислювальної. Основу такої системи складають розподілені бази даних (РБД) і система керування розподіленими базами даних (СКРБД).

distributed database – розподілена база даних # набір даних, розподілених у двох або більше середовищах баз даних.

distributed information system – розподілена інформаційна система # інформаційна система , дані та пов'язані процеси якої розподілені у двох або більше середовищах баз даних.

distributed network – розподілена мережа # мережа обчислювальна, всі пари вузлів якої з'єднані безпосередньо або через резервні канали зв'язку, що проходять через проміжні вузли.

distribution – **1.** розповсюдження # розширення обсягів дії чого-небудь # **2.** розподіл # дія, спрямована на ділення чогось між ким-, чим-небудь, надання кожному окремої частки.

distribution data – розподілені дані # дані, які визначають місцезнаходження, повернення та фрагментування інформації щодо об'єктів даних в розподіленій системі баз даних.

distribution of information and functions of its processing – розподіл інформації і функцій її оброблення # розподілення інформації і функцій її оброблення за ознаками, що забезпечують звернення до інформації і її оброблення на основі дозволених повноважень. До числа таких ознак відносяться: ступінь важливості; ступінь секретності; виконувані функції користувачем, пристроєм; види документів; види даних; найменування томів, файлів, масивів, записів; ім'я користувача; функції оброблення інформації: читання, запис, виконання; ділянок оперативної і довготривалої пам'яті; години дня. Застосовується в системі розпізнавання і обмеження доступу до інформації.

DMZ – demilitarized zone – демілітаризована зона.

DNS – domain name server – сервер доменних імен.

DNS name space – простір імен DNS # набір або дерево імен доменів і правила створення цих імен. Кожний вузол в імені домену являє деякий об'єкт, наприклад, комп'ютер або псевдонім для електронної пошти. Для будь-якого домену виділений DNS-сервер, з якого здійснюється його адміністрування. Компанії або великі мережі вправі поділяти домен на декілька піддоменів для спрощення адміністрування або інших потреб. В цьому випадку кожний з піддоменів повинен мати свій DNS-сервер, який містить його базу даних. Усі зміни в базі даних здійснюються тільки цим сервером, і він обробляє запити клієнтів і інших DNS-серверів. Сервер, що зберігає базу, називають відповідальним (authoritive) сервером цього домену або піддомену.

document – документ # матеріальний об'єкт із зафіксованою на ньому інформацією у вигляді тексту, звукозапису або зображення, призначений для передавання у часі і просторі з метою збереження і суспільного використання. Документи охоплюють службову інформація, наукові публікації у відкритих і закритих виданнях, статті в газетах і журналах про діяльність організації або її співробітників, конструкторську і технологічну документацію і т.ін. Документи – найбільш інформативні джерела інформації, так як вони містять, як

правило, достовірну інформацію в обробленому і стисненому вигляді, особливо, коли вони підписані або затверджені. Що стосується інформативності різноманітних публікацій, то вони мають достатньо широкий діапазон оцінок: від дуже високої, коли описується відкриття, до навмисної або ненавмисної дезінформації.

document electric communication – документальний електрозв'язок # вид електрозв'язку, за якого здійснюється передавання документальних повідомлень: літеро-цифрового тексту, цифрових даних і графічних зображень.

document identification and authentication – ідентифікування і встановлення автентичності документів # сукупність спеціальних заходів (протоколів) для забезпечення захисту інформації кожною стороною, що приймає участь в обміні документами. Для цього широке застосування знаходять криптографічні методи. При неавтоматизованому обміні інформацією автентичність документа засвідчується позитивним результатом перевірки особистого підпису людини, автора документа. При автоматизованому передаванні документів каналами зв'язку застосовується підпис цифровий.

documentation – документація # сукупність документів, ділових паперів, оформлених за єдиними правилами. Обґрунтування чого-небудь за допомогою документів. Існують різноманітні види документації: державна, цивільного призначення, графічна, інформаційного забезпечення, міжнародна, нормативна, програмна, робоча, секретна, експлуатаційна і т. ін.

documented information – документована інформація # інформація, яку треба контролювати й підтримувати в організації, і носії, які її містять. Документована інформація може бути в будь-якому форматі й на будь-якому носії та від будь-якого джерела. Документовану інформацію можна відносити до: системи керування, зокрема й пов'язаних процесів; інформації, яку створюють для функціювання організації (документації); доказів досягнутих результатів (записи).

documented information – документована інформація # інформація, якою потрібно керувати та підтримувати в робочому стані організацією, а також носій, на якому вона міститься # документована інформація може бути в будь-якому форматі, на будь-якому носії і з будь-якого джерела # документована інформація може стосуватися – системи менеджменту, у тому числі прилеглих до неї процесів; – інформація, створена організацією для забезпечення функціонування (документації); – підтвердження досягнутих результатів (записів).

documents – документація # див. documentation.

documents about organization and instruction – організаційно-розпорядча документація # найбільш загальна категорія керівницьких документів. Система організаційно-розпорядчої документації охоплює організаційну, розпорядчу і довідково-інформаційну документацію. В організаційній документації реалізується такий вид організаційно-розпорядчого впливу, як установлення норм (правил), регулюючих діяльність системи управління. До організаційної документації відносяться положення, статути, правила, посадові інструкції. Організаційні документи встановлюють права органів керування та керівників видавати розпорядчі документи: рішення, постанови, розпорядження, накази, вказівки.

domain – домен # *1.* ділянка # *2.* частина адреси доменної, відділена крапками # наприклад: доменна адреса www.irtc.org.ua, містить три домена: домен верхнього рівня ua (Україна), вкладений домен org (тип підприємства) і вкладений домен irtc (Міжнародний науково-навчальний центр інформаційних технологій та систем НАНУ) та www (WWW-сервер). До інших д. верхнього рівня відносяться: com – комерційні, gov – урядові, edu – навчальні, org – громадські організації, net – телекомунікаційні мережі, і національні домени різних держав: ua – Україна, jp – Японія, fr – Франція і т.ін. Звичайно для підтримки кожного домена (крім найнижчого рівня) використовується окремий сервер DNS. У такий спосіб утворюється ієрархія серверів DNS. На кожному DNS-сервері ведеться база даних про адреси IP (DNS-серверів їхніх вкладених доменів або кінцевих персональний комп'ютерів мережі).

domain name registration – реєстрування доменної адреси # внесення імені і відповідної йому IP-адреси в базу даних DNS-сервера. Реєстрація в доменах верхнього рівня платна. Реєстрація доменів нижнього рівня безкоштовна і виконується провайдером.

domain name server – сервер доменних імен # сервер, який транслює доменні імена користувачів (опорних комп'ютерів), існуючих у домені, в IP-адреси.

domestic destabilizing factor – внутрідержавні дестабілізуючі фактори # правовий вакуум у більшості питань забезпечення безпеки інформаційної; навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки; політичні конфлікти; зловмисні дії злочинних елементів або груп; відмови, збої, технічні помилки систем інформаційних (засобів); природні явища (процеси), що утруднюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

DoS – denial of service – відмова в обслуговуванні.

dossier – досьє # сукупність документів, матеріалів, що стосуються певного питання, справи, особи, а також папка, в якій містяться ці матеріали.

doubling – дублювання # виготовлення будь-чого у двох екземплярах, повторювання; паралельне з будь-ким виконання схожої, однакової роботи.

DPNSS – digital private network signaling system – сигнальна система цифрових приватних мереж.

DSL – digital subscriber line – цифрова абонентська лінія.

DTE – data terminal equipment – термінальне обладнання даних.

duplex-transmission – дуплексне передавання # передавання даних одночасно в двох напрямках.

duplicate – дублювання # копіювання даних з вихідного носія на носій призначення, який має таку ж фізичну форму # наприклад копіювання файлу з магнітної стрічки на іншу магнітну стрічку.

dynamic host configuration protocol – протокол динамічного конфігурування від сервера # протокол з протокольного стеку TCP/IP, який дозволяє персональному комп'ютеру чи робочій станції отримати тимчасову чи постійну IP-адресу з адресного пулу центрального сервера через механізми ручного, автоматичного та динамічного призначення, що забезпечує можливість повторного використання IP-адрес.

dynamic stereotype – динамічний стереотип # відносно стійка система реакцій організму на вплив зовнішнього середовища.

E

EAP – extensible authentication protocol – розширюваний протокол. Автентифікації.

EAP-TLS – eap transport layer security – розширюваний протокол аутентифікації для захисту транспортного рівня.

eavesdropping – перехоплювання інформації # несанкціоноване перехоплення випромінення, що несе інформацію (інформаційне випромінення).

EBCDIC – extended binary-coded decimal interchange code – розширений двійково-десятковий код обмінювання

EC – elliptic curve – еліптичні криві.

e-cash – електронні гроші # е-гроші # див. electronic money, e-money, cyber money.

ECC – elliptic curve cryptography – криптографія на основі еліптичної кривої.

ECDSA – elliptic curve digital signature algorithm – алгоритм цифрового підпису на основі еліптичної кривої.

eclioclieck – лунаконтроль # метод контролю передавання даних, при якому прийняті дані повертаються на передавальний пункт і порівнюються з переданими даними.

economic efficiency – економічна ефективність # показник економії праці в результаті застосування

певних заходів; ступінь віддачі виробництва, машин, апаратів.

economy security – економічна безпека # положення, при якому економіці держави не загрожує небезпека. Характеризують рівнем розвитку виробничих сил та економічних відносин, спрямованих на реалізацію потреб особистості і суспільства, наявністю розвиненої інфраструктури та корисних копалин, кваліфікованої робочої сили і системи її підготовки, а також характером інтеграції у систему світових господарських зв'язків. Створення замкненого самодостатнього господарства в межах окремої країни або групи країн, спрямоване на максимальне обмеження імпорту, стимулювання експорту товарів і капіталу, а також економічна залежність руйнують системи економічної безпеки.

EDGE – enhanced data-rates for GSM evolution – покращення швидкості обробки даних для розвитку GSM-стандарту.

EDI – electronic data interchange – електронний обмін даними.

effect – ефект # *1.* результат, наслідок яких-небудь причин, заходів, дій # *2.* сильне враження, спричинене ким-небудь або чим-небудь # *3.* засіб, що має на меті справити сильне враження, викликати здивування.

effectively unbreakable – практична криптостійкість # див. computationally secure.

effectiveness – ефективність # результативність # ступень реалізації запланованих дій та досягнення запланованих результатів.

Efficiency – ефективність # *1.* результат, наслідок будь яких причин, сил, дій # *2.* ступінь співвідношення результатів з затратами; система показників, що характеризують рівень використання потужностей різноманітних систем. Розрізняють ефективність технічну і економічну. В обчислювальній техніці технічна ефективність – це швидкість обробки одиниці інформації, питомі затрати на обробку одиниці інформації.

efficiency [of technical] protection of information – ефективність [технічного] захисту інформації # ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам.

efficiency of economic intelligence – ефективність економічної розвідки # відношення прибутків від діяльності розвідувальної до витрат на її проведення.

efficiency of information struggle – ефективність інформаційної боротьби # ступінь реалізації мети інформаційної боротьби.

efficiency of obtaining information – ефективність добування інформації # ступінь виконання завдань, поставлених перед органом добування інформації. Для об'єктивного визначення ефективності використовується група загальносистемних показників кількості і якості інформації: повнота інформації, що добувається;

своєчасність добування інформації; достовірність інформації; точність вимірювання розвідувальних ознак; сумарні витрати на добування інформації.

efficiency of psychological impact – ефективність психологічного впливу # ступінь реалізації мети психологічної війни. Залежить від цілого ряду факторів, які поділяються на передумови сприйняття психологічного впливу і передумови засвоєння змісту психологічного впливу.

EGP – exterior gateway protocol – протокол зовнішнього шлюзу.

EGPRS – enhanced general packet radio service – покращений загальний сервіс пакетного радіо передавання.

EIS – enterprise information system – інформаційна система підприємства.

electric communication – електрозв'язок # див. electrical communication.

electrical communication – електрозв'язок # будь-яке передавання сигналів електричних, що відображають знаки, текст, зображення, звуки або знання будь-якої природи за допомогою проводових, радіо, оптоелектронних та інших електромагнітних пристроїв (систем).

electromagnetic emission – електромагнітне випромінювання # процес випромінювання хвиль електромагнітних.

electromagnetic shielding електромагнітне екранування # об'єднання способів екранування високочастотних електричних і магнітних полів. Для виготовлення екранів застосовують наступні матеріали: сталь листова декапована товщиною 0,35-2 мм; сталь тонколистова оцинкована товщиною 0,51-1,5 мм; сітка сталева ткана з номерами 0,4-2,5; сітка сталева плетена з номерами 3-6; сітка з латунного проводу марки Л-80 з номерами 0,25-0,25; металізовані тканини. Матеріал екрана вибирають на основі оцінки необхідного коефіцієнта послаблення побічних електромагнітних випромінювань і наведень екраном, для чого на місці, де передбачається встановлення екрана, вимірюється рівень поля.

electronic attack – електронна атака # елемент війни електронної, що передбачає активний вплив на електронні засоби противника. За видом впливу електронну атаку поділяють на дві компоненти: неруйнівні впливи, які включають електронне придушення і електронну дезінформацію; руйнівні впливи на основі застосування протирадіолокаційних ракет, зброї спрямованої енергії (лазерної, НВЧ) і т. ін.

electronic **blocking** – радіоелектронне блокування # узгоджений вплив засобами придушення радіоелектронного і функціонального ураження на технічні елементи систем розвідки і канали передавання інформації.

electronic document – електронний документ # сукупність даних в

пам’яті ЕОМ, призначених для сприйняття людиною з допомогою відповідних програмних і засобів апаратних. Може включати крім текстової, графічну і звукову інформацію та має нелінійну структуру.

electronic lock – електронний замок # замки кодові з електронними ідентифікаторами у вигляді мікросхем, розташованих в герметичному корпусі з нержавіючої сталі. Кожна мікросхема має незмінюваний 64-розрядний номер (ключ), для визначення якого необхідно перебрати біля 1CF° комбінацій. Механічна стійкість з. е. забезпечується за рахунок подовжених горизонтальних і вертикальних ригелів. Ключ може вводитися зі спеціальної клавіатури, або з ідентифікаційної картки.

electronic money – електронні гроші # серії наборів цифр, що представляють собою банківські купюри і монети. Реалізація електронних грошей може бути як апаратною у вигляді карток, в яких використовується спеціальне програмне забезпечення, нанесене в мікросхему або магнітну смугу. Для захисту і збереження конфіденційності використовуються методи захисту криптографічні. За допомогою г. е. можна купувати товари в режимі прямого доступу, сплачувати перегляд фільмів за вимогою в інтерактивних телевізійних системах. Вони можуть замінити готівку і чеки для щоденних покупок та інших витрат.

electronic signature – електронний підпис # див. digital signature.

electronic war – електронна війна # комплекс заходів із застосуванням засобів випромінювання електромагнітного, спрямованих на пониження ефективності або запобігання застосування противником електромагнітного спектру, а також на забезпечення ефективного використання електромагнітного спектра своїми військами. В. е. є основоположним елементом впливу як на системи управління противника в оперативній і тактичній ланках, так і в цілому на інфраструктуру інформаційну противника. В. е. охоплює три основних елементи: забезпечення електронне, атака електронна і боротьба з електронною протидією або контрпротидія електронна.

electronic warfare operation – операція радіоелектронної боротьби # комплекс заходів і дій з радіоелектронного придушення і захисту своїх військ (сил) і систем зброї від радіоелектронного придушення. Складовими частинами операції радіоелектронної боротьби будуть: радіоелектронні удари з метою придушення всієї системи радіоелектронних засобів противника; радіоелектронна оборона (захист) об’єктів і засобів; заходи забезпечення операції радіоелектронної боротьби.

element – елемент # складова частина будь-чого цілого.

elliptic curve cryptosystem – криптосистема на основі еліптичних рівнянь # криптосистема, побудована на основі еліптичних кривих, які представляють математичний об'єкт, що може бути визначеним над будь-яким полем (скінченним, дійсним, раціональним або комплексним). У криптографії звичайно використовують скінченні поля. Еліптична крива представляє собою множину точок *(x,y)*, що задовольняють наступному рівнянню: *y2 = x3 + ax + 6*, а також нескінченно віддалена точка. Для точок на кривій достатньо легко вводиться операція додавання, яка відіграє ту ж роль, що операція множення в криптосистема RSA та Ель-Гамаля. В реальних криптосистемах використовується рівняння *y2 = x3 + ax + bmodp*, де *p* – просте. Проблема дискретного логарифма на еліптичній кривій полягає у наступному: дана точка G на еліптичній кривій порядку *r* (кількість точок на кривій) та інша точка *Y* на ці й же кривій. Необхідно знайти єдину точку ж таку, що *Y = xG*, тобто *Y* є ж-та степінь G.

embedded message – вбудоване повідомлення # процес стеганографічного перетворення контейнера і секретного повідомлення.

emergence – емерджентність # *1.* особливість систем, яка полягає в тому, що властивості системи не зводяться до сукупності властивостей частин, з яких вона складається, та не виводяться з них # *2.*внутрішня цілісність систем.

emergency protection – захист від аварійних ситуацій # створення засобів попередження, контролю і організаційних заходів для виключення несанкціонованого доступу на комплексі засобів автоматизації в умовах відмов його функціонування, відмов системи захисту інформації, систем життєзабезпечення людей на об'єкті розташування і при виникненні стихійного лиха.

emission – випромінювання # виділення променями теплової, електромагнітної та іншої енергії.

emitter – випромінювач # див. radiator.

e-money – електронні гроші # е-гроші # див. electronic money, e-cash, cyber money.

emptiness detector – виявник пустот # засоби пошуку невипромінюючих закладних пристроїв, що дозволяють виявляти можливі місця встановлення закладних пристроїв в пустотах стін або інших дерев'яних та цегляних конструкціях. Виявляти пустоти можуть різноманітні ультразвукові прилади, в тому числі медичного призначення, і спеціальні в. п. Спеціальні технічні засоби для виявлення пустот використовують: відмінності в значеннях діелектричної проникності середовища і пустоти; різницю в значеннях теплопровідності повітря і суцільного середовища. Ефективним

засобом виявлення пустот у стінах, нагрітих на декілька градусів вище температури повітря в приміщенні, є тепловізори.

empty container – порожній контейнер # контейнер без вбудованого прихованого повідомлення.

encapsulation – інкапсуляція # [у телекомунікаційних системах] механізм, використовуваний протоколами, у якому певний рівень додає інформацію вищого рівня до свого протокольного блока даних.

enciphered data – зашифровані дані # див. black data, cryptographically protected data.

encipherement – зашифровування # див. encryption.

encipherer– комерційний шифратор # шифратор # пристрій, призначений для автоматичного шифрування. Функцію з дешифрування виконує дешифратор.

encipherment – шифрування # криптографічне перетворення даних для одержання зашифрованого тексту # зворотний процес називається дешифруванням # див. cryptography.

encode – кодувати # перетворення даних за допомогою коду таким чином, що можливе зворотне перетворення до вихідної форми.

encoded information type – закодований тип інформації # частина конверта, що визначає тип закодованої інформації окремих частин вмісту # наприклад MIME (multipurpose Internet mail extender – багатофункційний розширювач електронної пошти Internet) та ASN.1.

encoding – кодування # див. coding.

encryption – **1.** зашифровування # шифрування # 1. процес зашифровування або розшифровування # 2. процес перетворення криптографічного даних, за допомогою якого текст відкритий перетворюється в шифртекст з метою захисту від несанкціонованого доступу # **2.** криптографічний захист # шифрація # криптографічне перетворення даних # результат шифрування – це зашифрований текст # зворотний процес називається дешифруванням.

encryption algorithm – криптографічний # алгоритм шифрування # алгоритм, згідно якого здійснюють криптографічне перетворення інформації.

encryption control – керування шифруванням # процес періодичної зміни коду ключа, що забезпечує кожний раз оригінальне представлення інформації при використанні одного і того ж алгоритму шифрування або пристрою.

encryption for end user – шифрування для кінцевого користувача /ш. для конечного пользователя/ – те ж, що шифрування абонент-

encrypter – шифратор # див. encipherer.

end user – кінцевий користувач # параметричний користувач # користувач обчислювальної системи, який звертається до системи обчислювальної для одержання

інформації або вирішення прикладних задач.

endec – кодек # блок апаратури цифрового передавання мовних сигналів по телефонних каналах (кодер-декодер).

end-to-end encripherment – міжкінцеве шифрування # шифрування даних усередині або на стороні відправника кінцевої системи з відповідним дешифруванням, яке виконується лише всередині або на стороні одержувача кінцевої системи # див. link-by-link encipherment.

end-to-end encryption – абонентське шифрування # шифрування даних, яке передбачається у складі або на виході джерела інформації з відповідним розшифровуванням тільки у складі або на вході кінцевого користувача інформації.

enemy – ворог # противник # див. opponent, adversary.

energy condition of reconnaissance contact – енергетична умова розвідувального контакту # умова, що передбачає забезпечення на вході розвідника приймача відношення сигнал/завада, достатнього для одержання на його виході інформації з необхідною якістю.

engineering protection subsystem – підсистема інженерного захисту # частина системи охорони об’єктів, призначена для механічного запобігання проникненню зловмисника до об’єктів захисту. Вона охоплює інженерні конструкції, що створюють механічні перепони на шляху зловмисника, і засоби (комплекси) керування доступом людей і транспорту на територію, що охороняється.

enlistment – вербування # див. recruiting.

ensembles – ансамбль # *1.* узгодженість, струнке ціле # *2.* послідовність випадкових величин Z_n $(n \epsilon N)$, які набувають значення у множині двійкових слів (в $0,1^n$).

enterprise network – корпоративна мережа # мережа обчислювальна локальна, що функціонує в масштабі великого підприємства, закладу; інтермережа відособленого використання.

entity – **1.** логічний об'єкт # активний елемент в підсистемі, що поєднує набір можливостей визначений для певного рівня і який відповідає окремому типові логічного об'єкта певного рівня, без використання будь-яких додаткових можливостей # **2.** об'єкт # сутність # дещо, що має окреме і індивідуальне існування та може бути ідентифікованим у контексті.

entity authentication – автентифікація логікового об'єкта.

entity authentication assurance – гарантування автентифікації об'єкта # ступінь довіри, досягнутої у процесі автентифікації, що об'єкт є тим, чим він є, або тим, що від нього очікується # впевненість ґрунтується на ступені довіри до зв’язку між об'єктом і представленої ним ідентичності.

entity invocation – виклик логічного об'єкта # специфічне використання

частини або всіх можливостей даного логічного об'єкта, без використання будь-яких додаткових можливостей.

entity-title – символьне ім'я логічного об'єкта # ім'я, що використовується для однозначної ідентифікації логічного об'єкта.

entity-type – тип логічного об'єкта # опис класу логічних об'єктів в термінах набору можливостей визначених для n-рівня ВВС.

environment – середовище # 1. носій інформації, тобто матеріал, на який записуються дані і на якому вони зберігаються # 2. оточення в якому функціонує об’єкт. Середовище виконання програми прикладної є ЕОМ, операційна система, запам’ятовуючі пристрої, набори даних.

environment of users automated system – середовище автоматизованої системи користувачів # сукупність користувачів, які можуть одержати доступ до середовища автоматизованої системи інформаційно. Множина $K = \{k_i, k_2,.., k_n\}$, елементами якої є показники, що характеризують користувачів, вважають оцінкою середовище користувачів. Користувачів автоматизованої системи можна характеризувати за службовим станом (керівник, користувач, допоміжний персонал, користувач, що не входить до штату автоматизованої системи), допуском до інформації, рівнем компетентності і т. ін.

episodic sign – епізодична ознака # ознака, що проявляється при певних умовах.

equal-length code – рівномірний код # див. constant-length code.

equivalent key – еквівалентні ключі # ключі, відмінні один від одного, для яких даний криптоалгоритм для будь-якої (або майже будь-якої) пари однакових вхідних текстів породжує однакові криптограми. У симетричних критпоалгоритмах це може трапитися, наприклад, в тому випадку, коли в процесі розширення ключа або утворення ключів циклових із різних ключів отримуються однакові значення. При побудові криптоалгоритму намагаються уникнути або зменшити кількість еквівалентних ключів, оскільки вони зменшують простір ключовий шифру.

equivalent term – еквівалентний термін # термін, який визначається на одній природній мові і за обсягом поняття відповідає терміну на іншій природній мові.

error – **1.** помилка # похибка # невідповідність між обчислюваним, спостережуваним або вимірюваним значенням або станом та дійсним, конкретним або теоретично правильним значенням або станом # **2.** помилка [користувача] # дії людини чи бездіяльність, що може призвести до непередбачуваного результату.

error condition – помилковий стан # умова, яка виникає, коли оператор намагається змусити обчислювач

виконувати функцію, яку він не може виконати.

error control – керування помилками # частина протоколу, що дає змогу виявлення помилок та, можливо, виправлення помилок.

error control software – програмні засоби керування помилками # програмне забезпечення, яке керує системою опрацювання даних для виявлення, запису та, можливо, виправлення помилок.

error correction – корекція помилок # метод, що його застосовують для виправлення помилкових даних, створених під час пересилання, перенесення чи зберігання даних.

error detection – виявлення помилок # метод визначення чи дані передавалися чи були передані неправильно.

error indication – **1.** індикація помилки # візуальна індикація того, що оператор намагався виконати функцію, яку калькулятор не може виконати # **2.** прогнозування помилок # кількісне твердження про очікувану кількість чи природу помилок у системі чи компоненті.

error log – журнал помилок # файл, в який система записує інформацію про збої.

error range – діапазон помилок # *1.* набір значень, які може прийняти помилка # *2.* # різниця між найвищими і найнижчими значеннями помилок.

error rate – коефіцієнт помилок # співвідношення загальної кількості виявлених помилок до загальної кількості переданих або перенесених даних.

error recovery – відновлювання працездатності системи після помилки # процес виправлення чи обходу ефекту збоїв або помилок для продовження виконання потрібної функції функційним модулем.

error seeding – підсівання помилок # процес навмисного додавання відомих несправностей у програму з метою моніторингу швидкості виявлення, видалення та оцінювання кількості невідомих несправностей, що залишилися в програмі.

error span – діапазон виявлення помилок # різниця між найвищими і найнижчими значеннями помилок.

error-checking code – код з виявленням помилок # див. binary error-detecting code, error-detecting code, self-checking code.

error-correcting code – код з виправленням помилок # див. binary error-correction code.

error-detecting code – код з виявленням помилок # див. binary error-detecting code, error-correcting code, self-checking code.

espionage – шпіонаж # передача, викрадення або збирання з метою передавання іноземній державі або її агентурі відомостей, що складають державну або воєнну таємницю, або відомостей, що складають службову або комерційну таємницю підприємств (шпіонаж промисловий, шпіонаж технологічний).

essence – сутність # див. entity.

estimate – оцінка # див. evaluation, estimation, assessment.

estimation – оцінка # див. evaluation, estimate, assessment.

ethernet technology – технологія ethernet # технологія побудови пакетних мереж, що використовує множинний доступ до мережі з опитуванням носія і виявленням конфліктів, а також транспортна технологія.

etymology – етимологія # *1.* розділ мовознавства, що вивчає походження слів # *2.* пояснення походження якогось слова зіставленням його з спорідненими словами тієї або іншої мови.

Euler phi function – функція Ейлера # для цілих чисел, більших або рівних 1, функцією Ейлера $\varphi(n)$ є кількість чисел, менших за и та взаємно простих з n, тобто таких, які не мають з n спільних дільників, відмінних від *1*. Ф. Е. відіграє значну роль в теорії криптосистем асиметричних. Так від складності її обчислення для досить великих чисел залежить стійкість кріпиоспе геми RSA.

evaluation – оцінка # 1. думка (висновок) про цінність, рівень або значення кого-чого-небудь # 2. наближене значення певної величини.

evaluation analysis – кваліфікаційний аналіз # аналіз системи обчислювальної з метою визначення рівня її захищеності і відповідності вимогам безпеки на основі критеріїв стандарту інформаційної безпеки. Інша назва кваліфікування рівня безпеки, оцінка безпеки інформації. Згідно «загальних критеріїв» кваліфікаційний аналіз може здійснюватися як паралельно з розробкою продукту інформаційних технологій, так і після її завершення. Для проведення кваліфікаційний аналіз розробник продукту повинен надати наступні матеріали: профіль захисту; проект захисту; різноманітні обґрунтування і підтвердження властивостей та можливостей ІТ-продукту, одержані розробником; сам ІТ-продукт; додаткові відомості, одержані шляхом проведення різноманітних незалежних експертиз. Процес кваліфікаційного аналізу охоплює три стадії: аналіз профілю захисту на предмет його повноти, несуперечності, реалізованості й можливості використання у вигляді набору вимог для продукту, який аналізують; аналіз проекту захисту на предмет його відповідності вимогам профілю захисту, а також повноти, несуперечності, реалізованості й можливості використання у вигляді еталона при аналізі ІТ-продукту; аналіз ІТ-продукту на предмет відповідності проекту захисту. Результатом кваліфікаційного аналізу є висновок про те, що підданий аналізу ІТ-продукт відповідає представленому проекту захисту.

evaluation deliverable – поставка компоненту для оцінки # будь-який ресурс, який оцінювач або орган оцінювання вимагає від замовника

або розробника для виконання одного або декількох видів діяльності з проведення оцінювання або з нагляду за оцінюванням.

evaluation evidence – свідчення оцінки # фактична поставка компоненту для оцінки.

evaluation technical report – технічний звіт про оцінку # звіт, про те що документ містить загальний вердикт і його логічне обґрунтування, виконаний оцінювачем і представлений в орган оцінки.

event – подія # виникнення або зміна певного набору обставин. Подія може бути одиничним або багаторазовим і може мати кілька причин. Подія може полягати в тому, що чогось не сталося. Подія може іноді позначатися як «інцидент» або «подія».

event journal – контрольний журнал # див. audit journal.

event log – журнал реєстрації подій # контрольний журнал # див. event journal, audit journal.

examine – досліджувати # винесення вердикт на основі аналізу з використанням спеціальних знань і досвіду оцінювача # твердження, в якому використовується це дієслово, вказує на те, що конкретно та які саме властивості повинні бути піддані аналізу.

exception – виняток # стан, що може виникнути під час виконання програми, що може спричинити відхилення від звичайної послідовності виконання, і для якого існують засоби визначення, підвищення, розпізнавання, ігнорування чи опрацювання # наприклад Стан "(ON ERROR)" в PL/1; переповнення; похибка діапазону.

exception handler – оброблювач виняткових ситуацій # частина програми, що виконується у відповідь на певний вид винятку.

exchange authentication information – інформація обміну автентифікації.

exclusive access – монопольний доступ # доступ програми (запиту) доданих в режимі, при якому всі інші програми (запити) в цей момент не мають доступу до цих же даних і знаходяться в режимі очікування.

executive management – виконавча дирекція # особа чи група осіб, яким керівний орган делегував повноваження стосовно впровадження стратегій і політик для досягнення цілей організації. Виконавчу дирекцію іноді називають вищим керівництвом і вона може включати виконавчого директора, фінансового директора, директорів з інформації та інші ролі.

executive management – вища виконавча керівництво # особа або група осіб, кому делеговано керівним органом керування відповідальність за реалізацію стратегії і політик для досягнення цілей організації # вище виконавче керівництво іноді називається вищим керівництвом і може охоплювати вищих посадових осіб, керівників фінансового спрямування, керівників IT -

напрямку та інших подібного роду керівників.

exhaustive attack – атака методом добору ключа # спроба порушити комп'ютерну безпеку, намагаючись отримати можливі значення паролів або ключів методом підбору # відмінна від аналітичної атаки.

experiment method – метод експерименту # специфічний метод вивчення об’єктів психологічної війни, який передбачає активне втручання фахівців психологічної війни у діяльність об’єкта, що вивчається, з метою одержання інформації. Для цього об’єкт ставиться у відповідні умови, а потім здійснюється спостереження за його діями. Загальна логіка експерименту полягає у тому, щоб поставити об’єкт вивчення у незвичайну для нього ситуацію. Розрізняють штучний і натурний експеримент. Недоліком штучного експерименту є те, що він здійснюється при обмежених можливостях (фактично його можна проводити тільки на військовополонених, або разом з бойовими частинами в ході спеціальних операцій). До того ж об’єкти майже завжди здогадуються, що їх вивчають. Натурний експеримент здійснюється в умовах, коли об’єкти вивчення знаходяться у своїх звичайних умовах, і не підозрюють про те, що за ними пильно спостерігають.

expert – експерт # фахівець, який здійснює експертизу.

expert evaluation – експертні оцінки # дані, які одержує висококваліфікований фахівець в даній галузі — експерт при аналізі об’єкта і прогнозуванні його подальшого розвитку.

expert examination – експертиза # *1.* розгляд, дослідження експертом певних справ, питань, що потребують спеціальних знань # *2.* процес опитування експертів, збирання і первинний аналіз експертної інформації.

expert on qualifications – експерт з кваліфікації # фахівець, що займається аналізом кваліфікаційним.

expert system – експертна система # клас систем інформаційних автоматизованих, що мають бази даних і бази знань, здатні здійснювати аналіз і корекцію даних незалежно від санкцій користувача, аналізувати і приймати рішення як на основі запиту, так і незалежно від запиту користувача і виконувати ряд аналітично-класифікаційних задач. Можна виділити ЕС діагностики, планування та про- гнозування. ЕС діагностики призначені для знаходження причин аномальності явищ, що спостерігаються. Основою для аналізу служать набори даних, за допомогою яких виявляються відхилення від еталонної поведінки і в результаті чого ставиться діагноз. ЕС планування призначені для вироблення програми дій, необхідних для досягнення певних цілей. ЕС прогнозування призначені

для побудови сценарію майбутнього. Засновуючись на подіях минулого і сучасного, вони здатні виводити ймовірні наслідки із заданих ситуацій. Для цього в прогнозуючих ЕС використовуються динамічні параметричні моделі.

explosion – вибух # *1.* миттєве руйнування чого-небудь, що супроводжують утворенням дуже нагрітих (високотемпературних), із високим тиском газів; звук, що супроводжує таке руйнування # *2.* переносно – раптовий сильний, гучний прояв чого-небудь.

exponentiation algorithm – експоненціальний алгоритм # алгоритм, який на нескінченній с послідовності входів робить більше як 2_n кроків, де n – довжина входу, а $c>0$ – деяка константа. Експоненціальний алгоритм в теорії складності відповідають повільним, неефективним на практиці алгоритмам.

exposure – незахищеність даних # можливість того, що певна атака буде застосовувати конкретну вразливість системи опрацювання даних.

extended binary-coded decimal interchange code – розширений двійково-десятковий код обмінювання # міжнародний восьмибітовий код, що використовується для подання двійково-десяткових даних при вводі-виводі інформації.

exterior gateway protocol – протокол зовнішнього шлюзу # протокол передавання інформації досяжності мережі та мережної політики між автономними системами.

external context – зовнішні обставині # зовнішнє середовище, де організація намагається досягти своїх цілій. Зовнішні обставині можуть охоплювати: культурне, соціальне, політичне, законодавче, фінансове, технологічне, природне та конкуруюче середовище інтернаціонального чи національного, чи регіонального або локального характеру; ключові рушійні чинники й тенденції, які впливають на цілі організації; взаємовідносини із зовнішніми акціонерами, а також їх розуміння та значимість.

external context – зовнішній контекст # зовнішнє середовище, в якій організація прагнути досягти своїх цілей # зовнішній контекст може включати: – культурну, соціальну, політичну, юридичну, технологічну, економічну, природну і конкурентне середовище, на міжнародному, національному, регіональному або місцевому рівні; – ключові рушійні фактори і тенденції, що впливають на цілі організації; і – взаємини із зовнішніми зацікавленими сторонами, їх думки і цінності.

external information relations – зовнішні # відносини інформаційні системи інформаційної з іншими системами та із середовищем їхнього існування.

external operational system – зовнішня операційна система # окрема

операційна система, яка взаємодіє з оцінюваною операційною системою.

external storage – зовнішня пам’ять # backing storage.

extra sector – захисний сектор # сектор, який записаний на доріжці, що перевищує стандартну кількість секторів, як частина методу захисту від копіювання.

extra track – захисна доріжка # доріжка, записана на диск, що перевищує стандартну кількість доріжок, як частина методу захисту від копіювання.

extraction – добування # див. procuring, getting.

extranet – екстранет # розширення мережі Інтранет організації, особливо через інфраструктуру загальнодоступної мережі, що робить можливим спільне використання ресурсів організацією, іншими організаціями й особами, з якими вона має справу, з наданням обмеженого доступу до своєї мережі Інтранет # наприклад, клієнтам організації може надаватися доступ до деяких частин її мережі. Інтранет за допомогою створення Екстранет, але клієнтів не можна вважати «довіреними» з точки зору безпеки

EIT – encoded information type – закодований тип інформації.

F

facility for technical protection of information – засіб технічного захисту інформації # пристрій та/або програмний засіб, в яких функція захисту інформації є основною.

facility with protection – **1.** [технічний] засіб із захистом # **2.** захищений [технічний] засіб # **3.** захищена техніка # технічний засіб, в якому функція захисту інформації від загроз є додатковою до основної.

fact – факт # 1. дійсна подія, вище # 2. реальність, дійсність.

factor – фактор # умова, рушійна сила, причина будь-якого процесу.

failsafe – відмово захищений # надійний # стосується запобігання компромісам у випадках відмов.

failsafe operation – операція убезпечення від несправностей # така робота комп'ютерної системи, що в разі відмови компоненти, зменшуються ймовірності відмови обладнання, пошкодження обладнання та негативного впливу на персонал.

failsoft – відмово тривкий # надійний # стосується функційного блока, який продовжує функціонувати режимі з мінімальними повноваженнями, незважаючи на несправності чи ручні операції із-за меж системи # збереження працездатності системи – це засіб для виконання операцій відмовостійкості.

failure – відмова # втрата функційним блоком здатності виконувати необхідну функцію.

failure access – доступ через відмову # неавторизований і зазвичай ненавмисний доступ до даних у системі опрацювання даних, що виникає внаслідок несправності апаратного чи програмного забезпечення.

failure recovery – відновлення після відмови # процедура поновлення роботи обчислювальної системи після відмови, що виключає вироблення системою неправильних результатів.

fake sector – фальшивий сектор # сектор, що складено із заголовка, але без даних, який застосовують часто на диску, щоб змусити неавторизовану програму копіювання не вдаватися до копіювання диску.

false attack object – хибний об'єкт атаки # об'єкт або елемент мережі інформаційно- обчислювальної, що підставляється противникові та імітує процес або результат роботи об'єкта атаки, вибраного противником. Хибний об'єкт атаки призначений для використання в процесі протидії інтелектуальної і сприяє досягненню мети інформаційної боротьби в інформаційно-обчислювальній мережі. У відповідності до принципів побудови хибного об'єкта атаки в загальному випадкові хибні об'єкти атаки складається з наступних модулів: модуля взаємодії з противником; основного модуля, який відповідає за перетворення даних і композицію усіх інших модулів хибних об'єктів атак; модуля взаємодії із суб'єктом інформаційної боротьби; модуля взаємодії з центром безпеки інформаційно-обчислювальної мережі. Хибний об'єкт атаки повинен функціювати, на основі коректно побудованого алгоритму інтелектуальної протидії, залучаючи, коли це необхідно суб'єкта інформаційної боротьби для вирішення нетривіальних ситуацій взаємодії з противником.

falsification – підробка # фальшива річ, імітація.

fatal error – критична помилка # помилка, яка впливає на подальше виконання програми, якщо така є, вона призводить до безглуздих результатів.

fault – відмова # див. failure.

fault – **1.** збій # самоусувна відмова або одноразова відмова, яку незначним втручанням усуває оператор # **2.** несправність # ненормальний стан, який може спричинити зменшення чи втрату здатності функційного блока виконувати необхідну функцію # нестравність стан, що характеризується неможливістю виконувати необхідну функцію, за винятком неможливості під час профілактики чи інших запланованих дій або через відсутність зовнішніх ресурсів.

fault seeding – підсівання збоїв # процес навмисного додавання відомих несправностей у програму з метою моніторингу швидкості виявлення, видалення та оцінювання кількості невідомих несправностей, що залишилися в програмі.

fault stability – стійкість до відмов # послуга, що забезпечує здатність комп'ютерної системи продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

fault tolerance – збереження працездатності системи # здатність функційного блока продовжувати виконувати необхідну функцію за наявності несправностей або помилок.

fault trace – відстежування несправностей # запис внутрішньої операції функційного блока, отриманий через відстеження послідовності його станів безпосередньо перед виявленням несправності.

FCITS – federal criterion for information technology security – федеральні критерії безпеки інформаційних технологій.

features – особливості # характерна риса, ознака, властивість кого-, чого-небудь.

federal criterion for information technology security – федеральні критерії безпеки інформаційних технологій # стандарт інформаційної безпеки, розроблений Національним інститутом стандартів і технологій США (NIST) і Агентством національної безпеки США (NSA) в 90-х роках для використання в Американському федеральному стандарті з оброблення інформації (Federal Information Processing Standard), який повинен був замінити «помаранчеву книгу». «Федеральні критерії» охоплюють практично весь спектр проблем, зв'язаних із захистом та забезпеченням безпеки, так як включають усі аспекти конфіденційності, цілісності і працездатності. Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій і системи оброблення інформації. Ключовим поняттям концепції інформаційної безпеки "Федеральних критеріїв" є поняття профілю захисту. Відповідно до «федеральних критеріїв» процес розробки систем оброблення інформації здійснюється у вигляді послідовності наступних основних етапів: розробка і аналіз профілю захисту; розробка і аналіз кваліфікаційний IT-продуктів; компонування й сертифікація системи оброблення інформації. «Федеральні критерії» регламентують тільки перший етап цієї схеми – розробку й аналіз профілю захисту. Процес створення IT-продуктів і компонування систем оброблення інформації залишаються за межами цього стандарту.

feedback attack – атака із зворотним зв'язком # атака на віддалену мережу обміну інформацією, яку характеризують тим, що на деякі запити, передані на об'єкт атаки, суб'єктові атаки потрібно одержати відповідь, тобто, між об'єктом атаки й суб'єктом атаки існує зв'язок зворотний, який дозволяє суб'єктові атаки адекватно реагувати на усі зміни, що відбуваються на об'єкті атаки. Дана атака може здійснюватися наступним чином: установлення суб'єктом атаки контролю над об'єктом атаки (спостереження за об'єктом атаки); очікування суб'єктом атаки

встановленого запиту від системи інформаційного впливу, що функціонує на об'єкті атаки; видача суб'єктом атаки команди на виконання певних операцій; виконання заданих операції; повідомлення суб'єктові атаки про виконання операції. Дальше слід перейти до другого (або третього) пункту послідовності дій. Таким чином, при наявності зворотного зв'язку суб'єкт атаки має можливість керувати віддаленою атакою (в ідеальному випадку – в реальному масштабі часу). Переривання зворотного зв'язку може привести до втрати керування атакою, а, отже, і до припинення атаки.

ferma pseudoprime number – слабке псевдопросте число # число складене, яке не визначається тестом Ферма.

fiber optic cable – волоконно-оптичний кабель # сукупність волокон оптичних, покритих захисною оболонкою. За умовами експлуатації кабелі розподіляються на монтажні, станційні, зонові і магістральні. Кабелі перших двох типів використовуються всередині будівель і споруд. Зонові і магістральні кабелі прокладаються в колодязях кабельних комунікацій, у ґрунтах, на опорах, під водою.

field detector – виявник поля # засоби радіоконтролю приміщень, призначені для виявлення радіовипромінювання пристроїв закладних в безпосередній близькості від джерела випромінювання. Найпростіші з них індикатори поля, які світловим або звуковим сигналом інформують оператора про наявність в місці розташування електромагнітного поля з напруженістю, вищою за фонову. Більш складні виявники поля – частотоміри – забезпечують, крім того, вимірювання частоти коливань поля.

field indicator – індикатор поля # виявник поля, що являє собою широкосмуговий приймач прямого підсилення (у найпростішому випадку – детекторний) з телескопічною штировою антеною. Наведений радіозакладкою в антені сигнал детектується і підсилюється до значень, що перевищують поріг спрацьовування звукової і світлової сигналізації. Нові варіанти індикатори поля доповнюють пристроєм акустичного зворотного зв'язку (акустичної "зав'язки" між гучномовцем індикатора поля і мікрофоном закладки), який дозволяє виділити випромінювання закладки на фоні інших радіосигналів. Подальшим удосконалення і. п. є інтерсептори.

file access – доступ до файла # перегляд, модифікування, заміна або вилучення файла, а також перегляд і маніпулювання його атрибутами.

file code – код захисту файла # в операційній системі UNIX – ціле число, біти якого описують клас файла і право доступу користувача до нього.

file protect ring – кільце захисту файлів # знімне пластикове чи металеве кільце, наявність або відсутність якого на магнітній стрічці котушки заважає писати на магнітній стрічці і тим самим запобігає випадкове стирання файлу.

file protection – захист файлів # впровадження відповідних адміністративних, технічних чи фізичних засобів для захисту від несанкціонованого доступу, модифікації чи видалення файлу.

file protection security – захист файла # див. data protection security.

file transfer protocol – протокол перенесення файлів # застосовний протокол транспортування файлів даних між мережними вузлами, який використовує послуги протоколу TCP керування передаванням. Спрощений варіант протоколу TFTP (Trivial FTP) застосовується, коли не потрібні автентифікація і перегляд каталогів.

file updating – оновлювання файлу # дія пов'язана з внесенням, видалення чи модифікацією даних у файлі.

file virus –# комп'ютерний вірус , призначений для зараження ЕОМ із запущеної на ній програми, яка вже містить вірус. В цьому випадку можливе зараження інших виконавчих файлів, в тому числі COM, EXE, SYS, BAT-файли і деякі інші. Файловы віруси можуть бути резидентними та нере- зидентними.

filter delay band – с муга затримування фільтра # смуга частот, в якій загасання передавання фільтра дорівнює або більше заданого значення.

filter pass band – смуга пропускання фільтра # смуга частот, в якій загасання передавання фільтра дорівнює або менше заданого значення.

filter transmission band –пропускання фільтра # див. filter pass band.

filtering – фільтрація # процес прийому або відхилення потоків даних у мережі відповідно до специфікованих критеріїв

filtration – фільтрування # процес зміни (спотворення) новин (інформації) при проходженні їх через різні стадії журналістської (інформаційної діяльності), коли «інформація з перших рук» (first-hand) попадає у другі руки (second-hand), а потім і в треті і мимоволі в результаті перетворюється в тому чи іншому плані. Визнання неминучості ф., фактично ставиться під сумнів повну об'єктивність новин.

find – пошук # функція чи режим, які дозволяють користувачеві знаходити у тексті подібні речі, як певні рядки символів, вбудовані команди чи символи з певним атрибутом.

finding – виявлення # див. detection.

FiOS – fiber optic service – сервіс із застосуванням волоконної оптики.

FIPS – federal information processing standard – федеральний стандарт оброблення інформації.

firewall – **1.** брандмауер # файєрвол # апаратно-програмний засіб захисту даних, який фільтрує вхідні й вихідні дані за заданими критеріями і

обмежує та контролює використання комп'ютерів чи локальної комп'ютерної мережі # **2.** міжмережний екран # вид бар'єру безпеки, розміщеного між різними мережними середовищами, що складається зі спеціалізованого пристрою або сукупності декількох компонентів і методів, через які повинний проходити весь трафик з одного мережного середовища в інше (і навпаки), при цьому пропускається тільки авторизований трафик, що відповідає локальній політиці безпеки.

firewall – файервол # системний компонент, який виконує роль шлюзу для фільтрації пакетів у мережі, тим самим реалізує принцип брандмауера. На жаргоні системних адміністраторів ф. називається стіною.

fitness-for-use test – тест придатності до використання # перевірка, яка здійснюється для визначення того, чи виконує реалізована система функційні цілі, встановлені її користувачами.

fixation–1. фіксація # запис, реєстрація, встановлення чого-небудь; зосередження уваги на чомусь # 2. фіксування #закріплення чого-небудь у певному положенні.

fixed drive – накопичувач на фіксованому диску # нагромаджувач на диску, що має носій інформації, який не знімається.

fixed-length code – код постійної довжини # код рівномірний, код з постійною довжиною комбінації кодової.

fixing – фіксація # фіксування # fixation.

flash memory – флеш-пам'ять # вид пристрою запам'ятовуючого постійного з еле- ктричним перезаписом.

flaw – функційний дефект # помилка в користуванні, пропущенні чи недогляді, який дає змогу обійти чи вимкнути механізми захисту.

flier – літальний апарат # див. airborne vehicle.

floppy-disk drive – накопичувач на гнучких магнітних дисках # нагромаджувач, в якому носіями інформації є змінні диски магнітні гнучкі.

flow – потік # сукупність чого-небудь, що рухається.

flow control – керування потоками # сукупність функцій і процедур, які забезпечують неможливість передавання інформації каналами прихованими, тобто в обхід комплексу засобів захисту. В більш вузькому значенні часто розуміється сукупність процедур, які забезпечують неможливість передавання інформації від об'єкта системи комп'ютерної з більш високим рівнем доступу до об'єкта комп'ютерної системи з більш низьким рівнем доступу.

flow of documentary information – документальний інформаційний потік # сукупність документів, що утворюють документальний масив. При отриманні документальний інформаційний потік виконує

наступні види аналізу: кількісний (статистичний або наукометричний), аналіз структури документального потоку, інформаційних зв'язків, якісний (змістовний) аналіз публікацій в документальному інформаційному потоці.

foreign key – зовнішній ключ # у відношенні, один або група атрибутів, що відповідають первинному ключу в іншому відношенні.

form – анкета # див. questionnaire.

foundation – основи # див. base, basic, ground, principle, fundament, law.

fragmentation – фрагментування # декомпозиція у середовищі більш ніж однієї бази даних значень екземплярів одного типу даних в розподіленій базі даних.

frame – кадр # [у телекомунікаційних системах] пакет канального рівня, який містить заголовок та кінцевик, що вимагаються фізичним середовищем.

frame relay – ретранслювання кадрів # служба телекомунікації!, створена для з'єднання локальних мереж, їх називають кінцевими точками в мережі ретрансляції кадрів. Служба ретрансляції кадрів упаковує дані в кадри змінної довжини (фрейми) і пересилає їх на зв'язану кінцеву точку. Усе виправлення помилок здійснюється в кінцевій точці, що збільшує швидкість передавання даних.

frame relay technology – **1.** технологія транслювання кадрів # **2.** технологія frame relay # технологія перенесення даних у вигляді послідовності суміжних бітів, обмеженої відкриваючим і кінцевим прапорами.

fraud – шахрайство # обман, шахрайські дії з корисною метою.

fraudulent computer virus – шкідливий комп'ютерний вірус # шахрайський комп'ютерний вірус # див. malicious computer virus.

frequence band receiving-set – діапазон частот радіоприймача # інтервали радіочастот, в яких радіоприймач здійснює прийом радіосигналів. Діапазон частот радіоприймача забезпечують шириною смуги пропускання селективних елементів вхідних фільтрів та інтервалом частот гетеродина. Настройка приймача на необхідний діапазон або піддіапазон частот здійснюється шляхом переключення елементів вхідних контурів і контуру гетеродина, а настройка на частоту всередині діапазону (піддіапазону) – шляхом змінювання частоти гетеродина. В сучасних приймачах як гетеродин використовується пристрій – синтезатор частот, який створює множину (сітку) гармонічних коливань на стабілізованих фіксованих частотах з інтервалом, відповідно до кроку настройки приймача.

frequency – несуча # див. carrier.

frequency – частота # величина, що характеризує кількість коливань хвиль (періодичних сигналів) за секунду. Частота вимірюється в герцах (Гц) – 1 Гц дорівнює одному повному коливанню за секунду.

Частота також вимірюється в кілогерцах (кГц, 1000 Гц), мегагерцах (МГц, 1000 кГц), гігагерцах (ГГц, 1000 МГц) та терагерцах (ТГц, 1000 ГГц).

frequency band – діапазон радіочастот # означений безперервний інтервал радіочастот, в якому коливання та хвилі мають порівняні властивості і умовну назву. За частотою радіохвиль виділяють такі діапазони радіочастот: вельминизьких (3-30 Гц), наднизьких (30-300 Гц), інфранизьких (0,3-3 кГц), дуже низьких (3-30 кГц), низьких (30-300 кГц), середніх (0,3-3 МГц), високих (3-30 МГц),дуже високих (30-300 МГц), ультрависоких (0,3-3 ГГц), надвисоких (3-30 ГГц), вельмивисоких (30-300 ГГц) та гіпервисоких (0,3-3 ТГц) радіочастот.

frequency band – смуга частот # ділянка частот, обмежена нижнім і верхнім краями.

frequency distortion – частотні спотворення # спотворення сигналу, що викликаються придушенням або зміною складових спектра вхідного сигналу радіоприймача. Через частотні спотворення сигнал на вході демодулятора може набувати форми, відмінної від вхідної.

frequency range receiving-set – діапазон частот радіоприймача # див. frequence band receiving-set.

FTP – file transfer protocol – протокол передавання файлів.

FTTH – fiber to the home – мережа з доведеним до користувача оптичним кабелем.

function – функція # 1. діяльність, обов'язок, робота; призначення # 2. змінна величина, значення якої залежить від значень іншої величини (величин).

functional check – функційний контроль # метод забезпечення контролю функціонування системи автоматизованої з метою своєчасного виявлення відмов, помилок і збоїв апаратури, програмного забезпечення і помилок людини, виключення їхнього впливу на подальший процес оброблення інформації та встановлення місця розташування елемента, блока програми, робочого місця, що відмовили, з метою наступного швидкого відновлення системи. Існуючі методи к. ф. обчислювальних систем можуть бути розділені на програмні, апаратні і комбіновані (поєднання програмного з апаратним).

functional class – клас функційних вимог безпеки # в «загальних критеріях» – верхній рівень формальної структури вимог безпеки функціональних. Містить наступні елементи: назву класу; опис класу; розділи функційних вимог безпеки. Функціональні вимоги розподілені на 11 класів функційних вимог безпеки: аудит; причетність до приймання/передавання; криптографія; захист інформації; ідентифікація і автентифікація; керування безпекою; конфіденційність роботи в системі; надійність засобів захисту; контроль

за використанням ресурсів; контроль доступу до системи; пряма взаємодія). Зміст класів функціональних вимог відрізняється своєю всеохоплюючою повнотою і багаторівневим підходом до забезпечення безпеки. Окремі класи вимог спрямовані на забезпечення безпеки самих засобів захисту, контролю за експлуатацією системи, забезпечення конфіденційності сеансів доступу до системи й організації обміну інформацією.

functional criterion – функційні критерій # група критеріїв для визначення функційної потужності засобів захисту, які в «європейських критеріях» розглядаються на трьох рівнях деталізації. На першому рівні розглядаються цілі забезпечення безпеки, другий рівень містить інформацію про специфікації функцій захисту, у третій – механізми, що реалізують їх. Специфікації функцій захисту розглядаються з точки зору наступних вимог: ідентифікація і автентифікація; керування доступом; підзвітність; аудит; повторне використання об'єктів; цілісність інформації; надійність обслуговування; безпека обміну даними. Більшість вимог співпадають з вимогами «помаранчевої книги». Вимоги безпеки обміну даними регламентують роботу засобів, що забезпечують безпеку даних, які передаються каналами зв'язку, і включають наступні розділи; автентифікація; керування доступом; конфіденційність даних; цілісність даних; неможливість відмови від здійснених дій. Набір функцій безпеки специфікується з використанням посилань на класи-шаблони, що визначені раніше. В «європейських критеріях» їх десять. П'ять з них (F-Cl, F-C2, F-Bl, F-B2, F-B3) відповідають класам «помаранчевої книги» з аналогічним позначенням. Інші п'ять класів відображають точку зору розробників стандарту на проблему безпеки: клас F-IN призначений для систем з великими проблемами при забезпеченні цілісності, що є типовим для систем керування базами даних; клас F-AV характеризується підвищеними вимогами до забезпечення працездатності; клас F-DI розрахований на розподілені системи оброблення інформації; клас F-DC приділяє особливу увагу вимогам до конфіденційності інформації, що передається; клас F-DX пред'являє підвищені вимоги і до цілісності і до конфіденційності інформації (в ньому об'єднані вимоги класів F-DI і F-DC з додатковими можливостями шифрування і захисту від аналізу трафіка.

functional families – розділи функційних вимог безпеки.

functional standard – функціональний стандарт # стандарт, що складається зі зібрання інших стандартів, узгоджених між собою.

fundament – основи # див. base, basic, ground, foundation, principle, law.

G

game – гра # ряд дій, спрямованих до певної мети; інтрига, таємний задум.

gamma – гама # випадкові або псевдовипадкові послідовності чисел.

garbage collection – збирання сміття # загроза, що полягає в захопленні й аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться.

gatekeeper – **1.** контролер зони # **2.** гейткіпер # елемент мережі передачі даних, який забезпечує транслювання адрес і керує доступом до мережі для мультимедійних терміналів та шлюзів.

gateway – шлюз # апаратно-програмний засіб, що забезпечує з'єднання двох мереж з різними протоколами або середовищами передавання інформації. Шлюз працює на мережному або більш високих рівнях. Так звані прикладні шлюзи при пересиланні даних з однієї мережі в іншу виконують трансляцію протоколів. Наприклад поштовий ш. конвертує два різних протоколи пошти електронної. Іноді цей термін застосовують у ситуації, коли не потрібна трансляція протоколів, а дані просто пересилаються з однієї мережі в іншу. Шлюз характеризують наявністю декількох адрес мережного рівня, наприклад, декількох IP-адрес. У IP-мережах роль шлюзу виконує маршрутизатор, що комутує канал мережі, до якого підключений персональний комп'ютер.

general fundamentals of information plantation theory – загальні основи теорії інформаційної боротьби # найважливіші спільні вихідні положення теорії інформаційної боротьби. В загальних основах визначаються: апарат понять інформаційної боротьби; напрямки і методи досліджень інформаційної боротьби; тенденції розвитку інформатизації і її роль в різноманітних галузях життя суспільства; роль і місце інформаційної боротьби у мирний і воєнний час; об'єкт, предмет, цілі, завдання і структура теорії інформаційної боротьби. Найважливішими логічними елементами змісту загальних основ теорії інформаційної боротьби є категорії, закони, закономірності і принципи інформаційної боротьби.

general IT-product specification – загальна специфікація IT-продукту # специфікація, що відображає реалізацію продуктом інформаційних технологій вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту, що реалізують вимоги безпеки функціональні і вимоги гарантій безпеки «загальних критеріїв».

general multi protocol label switching – узагальнена багатопротокольна комутація за мітками # багатопротокольна комутація за мітками, яка підтримує різні транспортні технології – оптичне мультиплексування, асинхронний режим переносу ATM, комутацію кадрів Frame Relay.

general resistance – загальна опірність # опірність навіюванню, яка зумовлена критичністю людей до спроб будь-що навіяти їм. В цілому, вона широка за спектром дії, але слабка за силою (хоча є суттєві відмінності між людьми за цими параметрами).

generation – генерування # відтворення, вироблення.

generator – ***1.*** генератор #пристрій, апарат чи машина, які виробляють якийсь продукт, електричну енергію або перетворюють один вид енергії на інший # ***2.*** давач # див. measuring transducer.

generic name – загальне ім'я # ім'я набору об'єктів. Загальне символьне ім'я є конкретною формою загального імені.

getting – добування # див. procuring, extraction.

getting information without physical penetration into the controlled area – добування інформації без фізичного проникнення в контрольовану зону # одержання інформації з носіїв, що розповсюджуються за межі контрольованої зони. Для забезпечення добування інформації дистанційного органи добування застосовують найбільш чутливу апаратуру для приймання носія і добування з нього інформації, яка за своїми параметрами перевищує параметри кращих зразків апаратури побутового і навіть військового призначення.

getting information without violating the state border – добування інформації без порушення державного кордону # одержання інформації з носіїв, що розповсюджуються за межі зони контрольованої держави – державного кордону. В цьому випадку добувається тільки та інформація, носії якої можуть легально або нелегально перетинати кордон. У випадку носіїв випромінювання з інформацією, добування інформації можливе наземними засобами добування інформації, розташованими за межами державного кордону (наприклад засоби радіо- і радіотехнічної розвідки, що перехоплюють радіосигнали з семантичною і ознаковою інформацією), засобами добування інформації зверху, розташованими на космічних апаратах або штучних супутниках Землі (засоби фото, телевізійного, радіолокаційного спостереження, радіо- і радіотехнічної розвідки), а також засобами добування інформації, розташованих на літальних апаратах (літаках-розвідниках, безпілотних літальних апаратах) і кораблях, що

літають та плавають вздовж повітряних і морських кордонів.

GII – global information infrastructure – глобальна інформаційна інфраструктура.

global address administration – глобальне адміністрування адрес # адміністрування адрес, під час якому всі індивідуальні адреси локальної мережі унікальні в одній або іншій локальній мережі.

global attack – глобальна атака # широкомасштабна атака # атака на мережу обміну інформацією віддалена, спрямована на декілька сегментів мережі обміну інформацією.

global information infrastructure – глобальна інформаційна інфраструктура # сукупність мереж, кінцевого обладнання користувачів, інформаційних та людських ресурсів, яка може бути використана у глобальному масштабі для доступу до інформації, спілкування, роботи, навчання, розваг – у будь-який час, у будь-якому місці, і за прийнятною ціною.

global positioning system – глобальна система позиціювання # спеціалізована супутникова система, що надає користувачам дані для автоматичного визначення їх географічного місцезнаходження.

glossary – глосарій # словник # див. dictionary.

GMPLS – general multi protocol label switching – узагальнена багатопротокольна комутація за мітками.

governance of information security – керування інформаційною безпекою # система, за допомогою якої спрямовують і контролюють дії організації в сфері інформаційної безпеки.

governance of information security – корпоративне керування інформаційною безпекою # система, яка забезпечує спрямованість і контрольованість дій з інформаційної безпеки організації.

governing body – **1.** адміністративний орган керування # **2.** керівний орган # особа або група осіб, які несуть відповідальність за показники діяльності і внутрішню узгодженість організації. Керівний орган у деяких юрисдикціях може бути радою директорів.

government bodies – орган влади # державні і суспільні заклади і організації, що функціонують в даній системі влади. Розрізняють органи державного управління, органи місцевого самоуправління, вищі органи влади, органи законодавчої, виконавчої, судової влади, органи політичного, воєнного, господарського керівництва і т. ін.

government management – державне керування # одна з форм діяльності держави, яка виражається в практичній реалізації законів, в організації суспільних відносин з метою забезпечення державних інтересів і політики, що проводиться державою.

GPRS – general packet radio service – загальний сервіс пакетної радіопередачі.

GPRS tunneling protocol – протокол тунелювання служби GPRS # протокол реалізовано в інтерфейсі Gn для тунелювання даних користувача між різними вузлами GSN (GPRS Support Node) підтримки загальних послуг пакетного радіопередавання GPRS. Нульова версія протоколу може використовуватися з данограмним протоколом користувача UDP та протоколом керування передаванням TCP, перша версія – тільки з протоколом UDP.

GPS – global positioning system – глобальна система позиціювання.

grade of service – категорія обслуговування # сукупність видів обслуговування, які можуть бути надані користувачу.

graph – граф # системи зв'язків між об'єктами довільної природи. Задавання г. зводиться до вказування непустої множини вершин графа, множини ребер і так званого інцидентора, що встановлює відповідність між ребрами та парами вершин.

Gray code – код Грея #двійковий код рефлексивний, кодові комбінації якого одержують за наступними правилами: кодова комбінація коду двійкового натурального складається з такою ж комбінацією зсунутою вправо на один розряд, при цьому молодший розряд зсунутої комбінації відкидається.

ground – основи # див. base, basic, principle, foundation, fundament, law.

group – група # сукупність людей, об'єднаних спільністю інтересів, професії, діяльності, а також сукупність предметів, об'єднаних спільністю ознак.

group key – груповий # ключ, спільний для групи абонентів системи.

group resistance – групова опірність # опірність навіюванню з боку групи як цілого. Цей різновид опірності навіюванню залежить від якісного складу групи: ступеню її згуртованості, єдності мети й мотивів діяльності та інших факторів. Чим менше розвинені міжгрупові зв'язки й відносини, тим слабкіша групова опірність. Встановлено також, що загальна опірність групи завжди нижча опірності окремих, найбільш стійких її членів.

group signature – груповий підпис # схема підпису цифрового, яка дозволяє будь-якому членові групи підписати повідомлення таким чином, щоб при перевірці можна було встановити, що повідомлення підписане одним із членів групи, без конкретизації його особи.

grouping isolation – групувальна ізоляція # електричне розділення між групами електричних кіл # група має електричне з'єднання, наприклад, з джерелом живлення.

GSM – global system for mobile communications – глобальна система мобільного обміну даними.

GTP – GPRS tunneling protocol – протокол тунелювання служби GPRS.

guarantee – гарантія # *1.* порука, забезпечення # *2.* в системі захисту інформації – оцінка міри довіри в тому, що система захисту відповідає конкретній системі автоматизованій та забезпечує виконання певної політики безпеки. Гарантії даються органом сертифікації при акредитації системи оброблення даних на підставі її сертифікації # *3.* сукупність вимог (шкала оцінки) для визначення міри упевненості, що система комп'ютерна коректно реалізує політику безпеки.

guarantee criterion – критерій гарантій # група критеріїв для визначення рівня гарантій реалізації засобів захисту, які в «європейських критеріях» складаються з двох компонентів: критеріїв ефективності й критеріїв коректності. До складу критеріїв ефективності входять: відповідність набору засобів захисту проголошеним цілям захисту; взаємна узгодженість різних засобів і механізмів захисту; здатність засобів захисту протистояти атакам; можливість практичного використання недоліків архітектури засобів захисту; простота використання засобів захисту; можливість практичного використання функціональних недоліків засобів захисту. До складу критеріїв коректності входять: на стадії процесу розробки – специфікації вимог безпеки, розробка архітектури, створення робочого проекту, реалізація; середовище розробки – засоби керування конфігурацією, мови програмування й компілятори, безпека середовища розробки; експлуатаційна документація – настанова користувача, настанова адміністратора; середовище експлуатації – доставка й установка, запуск і експлуатація.

guaranteed service – обслуговування з гарантованою якістю # обслуговування, відповідне до підписаної якості обслуговування.

guard – **1.** захист # 1. умовний вираз, який застосовується для визначення відкритого чи закритого характеру альтернативи в операторові вибіркового очікування # 2. функційний блок, який забезпечує захисний фільтр між двома системами опрацювання даних, що працюють на різних рівнях безпеки чи між терміналом користувача та базою даних, для відфільтровування даних до яких користувач не має права доступу # **2.** охорона # 1. група (людей, кораблів, машин), що охороняють кого-що-небудь # 2. термін, що означає слідкування за збереженням кого-, чого-небудь.

guarding – охорона # див. guard, protection.

guidance data protection document – настановчий документ системи захисту інформації # документи системи захисту інформації, що визначають порядок забезпечення захисту інформації і обов'язки

посадових осіб по захисту інформації. Типовими керівними документами є: інструкція по захисту інформації в організації; положення про підрозділ організації, на який покладаються завдання забезпечення безпеки інформації; інструкції по роботі з грифованими документами; інструкції по захисту інформації про конкретні вироби.

H

hacker – хакер # 1. особа, яка порушує систему захисту системи автоматизованої з метою висвітлення її недосконалості та отримання доступу (без корисних інтересів) # 2. програміст-фанатик, який займається досконалим вивченням систем обчислювальних з метою розширення їхніх можливостей та створенням більш-менш корисних допоміжних програм, які здебільшого погано документовані та інколи спричиняють небажані побічні результати.

hacker – хакер # 1. технічно ерудований комп'ютерний ентузіаст # 2. технічно ерудований комп'ютерний ентузіаст, який застосовує свої знання та засоби для отримання несанкціонованого доступу до захищених ресурсів.

hacking – хакінг # неавторизоване використання або спроба обходу чи зламу механізмів захисту інформаційної обчислювальної системи або мережі.

hacking fraud – хакерське шахрайство # проникнення хакерів в комп’ютерну систему захисту для видалення механізмів захисту або переконфігурування системи для своїх цілей.

half-duplex-transmission – напівдуплексне передавання # передавання даних в одному з двох напрямків по черзі. Вибір напрямку здійснюють (n+1)- логічним об’єктом.

Hamming code – код Хеммінга # код з мінімальною надмірністю, що забезпечує виправлення поодиноких помилок.

handover in the NGN – хендовер # естафетне перемикання # перемикання з’єднання у процесі руху абонента з однієї робочої зони на іншу.

handshake – обмін сигналами керування # процедура обміну сигналами керування при передаванні данних у режимі з встановленням з'єднанн, яка передбачає обмін сигналами керування між предавачем та отримувачем перед потатком передавання даних. Ця процедура складається з трьох фаз: встановлення з'єднання, передавання даних, роз'єднання з'єднання. Таким чином, з'єднання має певний визначений час життя.

hard error – систематична помилка # постійна помилка, яка завжди повторюється під час послідовних спробах читання даних.

hardware check – апаратний контроль # див. automatic check.

hardware check authenticity – апаратний контроль достовірності # метод контролю достовірності оброблення інформації із застосуванням апаратних засобів, що виконують практично ті ж функції, що засоби контролю достовірності програмного. Проте вони працюють швидше і дозволяють виявляти помилки ближче до місця їхнього виникнення, а також помилки, які недоступні для програмних методів.

hardware documentation – технічна документація # документація технічного забезпечення # система текстових і графічних документів, що містять інформацію про технічні вироби (деталі, зразки, комплекси), технічні і технологічні процеси, затверджені встановленим порядком. Основні види технічної документації: конструкторська, нормативно-технічна, технологічна.

hardware documents – документація технічного забезпечення # див. hardware documentation.

hardware environment – апаратне середовище # засоби технічні, що використовуються при виконанні програми.

hardware security – апаратний # використання апаратних засобів (наприклад, регістрів границь, замків і ключів або апаратури шифрування) для захисту даних в ЕОМ.

hardware-based security – апаратний захист # див. hardware security.

hash addressing – геш-адресування # метод перетворення пошукового ключа на адресу з метою зберігання та отримання даних # метод часто розробляється для мінімізації часу пошуку.

hash clash – геш-колізія # виникнення того самого значення геш-функції для двох або більше різних ключів.

hashing – гешування # метод перетворення пошукового ключа на адресу з метою зберігання та отримання даних.

heterogeneity – гетерогенність # властивість системи інформаційного обслуговування, що виявляється у взаємному сполученні різнорідних, різноманітних за властивостями і складом форм забезпечення (наприклад, інформаційне та бібліотечно-бібліографічне) і засобів забезпечення (наприклад, реферування та синтезування), що діють на засадах взаємодоповнюваності.

heterogeneous network – гетерогенна мережа # мережа, що функціонує за багатьма мережними протоколами.

hiding – приховування # *1.* утаювання будь-чого для того, щоб воно не виявлялося явно # *2.* спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому перешкоджанні несанкціонованого доступу до інформації.

hiding of information – приховування інформації # спосіб технічного захисту інформації, що полягає у виключенні або суттєвому утрудненні несанкціонованого одержання інформації.

hiding-place operation – тайникова операція # дії, спрямовані на закладення матеріалу в таємне місце (тайник) із тим, щоб його міг вилучити агент шпигунської організації. Зв'язок через тайник є однією з форм безособового зв'язку.

HIDS – host based intrusion detection system – система виявлення вторгнень на базі хостів.

hierarchical check – контроль ієрархічний # метод контролю повноважень, при якому повноваження кожного об'єкта контролюються об'єктом з більш високими повноваженнями, в результаті чого створюється ієрархія повноважень.

high-frequency compromising source emission – випромінювач небезпечних високочастотних сигналів # див. high-frequency tell-tale source emission.

high-frequency tell-tale source emission – випромінювач небезпечних високочастотних сигналів # джерела побічних високочастотних коливань, до яких відносяться: високочастотні генератори, що входять до складу багатьох радіотехнічних засобів; підсилювальні каскади, в яких при певних умовах виникають паразитні високочастотні коливання; нелінійні елементи, на які подаються гармонічні високочастотні коливання і електричні сигнали з мовною інформацією. У результаті акустоелектричних перетворень або інших інформаційних впливів на джерела побічних коливань (модуляції) модульовані коливання стають небезпечними сигналами, що можуть бути прийняті за межами зони контрольованої. Високочастотні коливання створюються не тільки функціональними або паразитними генераторами радіоелектронних засобів, але можуть бути підведені до них зловмисниками від зовнішнього генератора. Численні небезпечні високочастотні сигнали створюють працюючі ПЕОМ, особливо ті, що розташовані в пластмасових неметалізованих корпусах. їхнє випромінювання має широкий діапазон: від одиниць до сотень МГц. Найбільш потужними інформативними джерелами електромагнітного випромінювання є відеопідсилювач і електронно-променева трубка монітора.

home network – мережа прописки # мережний домен, у якому зберігаються специфічні для абонента службові дані, потрібні протягом встановлення з'єднань.

homogeneous network – гомогенна мережа # мережа, що функціонує за одним мережним протоколом.

horizontal fragmentation – горизонтальне фрагментування # фрагментування, де розподілення формуються з усіх значень даних для підмножини екземплярів.

host – хост # хост-комп'ютер # мережний комп'ютер # комп'ютер, на якому працює мережний протокол, наприклад, TCP/IP. Х. має деяке прикладне програмне забезпечення, призначене для

передавання і приймання пакетів. Він обміню дані з іншими хост-комп'ютерами і значна частина діяльності в Інтернеті зумовлена керуванням інформаційними потоками між хост-комп'ютерами. Типовими прикладами х. можуть бути: маршрутизатори, комп'ютери персональні, сервери, проксі-сервери, шлюзи і т. ін.

host computer – головний комп'ютер # провідний комп'ютер # у комп'ютерній мережі комп'ютер, який надаючи користувачам такі сервіси, як обчислення, доступ до бази даних, може виконувати функції керування мережею.

host machine – хост-машина # 1. комп'ютер, що його застосовують для розробляння програмного забезпечення, призначеного для іншого комп'ютера # 2. комп'ютер, що його застосовують для емуляції іншого комп'ютера # 3. комп'ютер, на якому інстальована програма чи файл.

hot site – резервний вузол # повністю обладнаний комп'ютерний центр, який забезпечує негайну альтернативу можливості опрацювання даних.

hot standby – сервіс негайної заміни # «гарячий» резерв # конфігурація, у якій надлишковий функційний блок може бути негайно уведений в експлуатацію, якщо основний функційний блок несправний.

hotspot – [бездротова] точка доступу # «гаряча» точка # X, Y позиції, які відповідають координатам, вказаним для покажчика # наприклад позиція кінчика стрілки маніпулятора.

HTTP – hypertext transfer protocol – протокол передавання гіпертексту.

hub – концентратор # мережний пристрій, що функціонує на першому рівні еталонної моделі взаємодії відкритих систем OSI # мережні концентратори не є інтелектуальними пристроями, вони забезпечують тільки точки фізичного з'єднання для мережних систем або ресурсів

Huffman code – код Хаффмена # префіксннй код, в якому довжина комбінації кодової обернено пропорційна частоті появи елемента, що кодується (чим частіше зустрічається елемент, тим коротша кодова комбінація).

human error – помилка [користувача] # дії людини чи бездіяльність, що може призвести до непередбачуваного результату.

human intelligence – агентурна розвідка # добування інформації шляхом проникнення агента-розвідника до джерела інформації на відстань доступності його органів чуття або технічних засобів, що використовуються агентом, з метою копіювання інформації і передавання її споживачеві інформації.

HUMINT – human intelligence – агентурна розвідка.

hydroacoustic intelligence – гідроакустична розвідка # добування відомостей про противника гідроакустичними засобами шляхом приймання, реєстрації та аналізу

акустичних (звукових) коливань, що випромінюються або відбиваються кораблем, торпедою і т. ін.

hypertext environment – гипертекстове середовище # комплекс прийомів створення комп'ютерним шляхом багатошарових гіпертекстів, що дозволяють користувачам без утрати змісту початкового запиту встановлювати різноманітні зв'язки з додатковими даними і тим самим створювати враження розширення інформаційного простору цих даних.

hypertext transport protocol – протокол перенесення гіпертексту # протокол перенесення файлів і даних різноманітних форматів через мережу Інтернет між клієнтом, користувачем Internet (web-browser), і Internet-сервером (web-server).

hypothesis primality test – гіпотетичний тест на простоту # тест на простоту, який відноситься до детермінованих тестів на простоту, якщо деяка (покладена в його основу) гіпотеза справедлива, і до тестів на простоту ймовірнісних в противному випадку. Прикладом тесту на простоту гіпотетичного є тест Міллера.

I

I AN A – Internet Assigned Numbers Authority – організація з розподілу адрес в Інтернеті.

IAB – Internet Architecture Board – консультативно-технічна Інтернет група.

ICMP – Internet control message protocol – протокол керівних повідомлень Інтернет.

idea – поняття # див. concept, notion.

identification – ідентифікування # *1.* ототожнення, прирівнювання, уподібнення # *2.* надання суб'єктам і об'єктам доступу ідентифікатора і (або) порівняння пред'явленого ідентифікатора з переліком наданих ідентифікаторів # *3.* операція розпізнавання обчислювальною системою суб'єктів та об'єктів доступу за унікальною ознакою ідентифікатором, яка необхідна для управління доступом; після і., як правило, проводиться перевірка повноважень # *4.* процедура присвоєння ідентифікатора об'єктові комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором.

identification user – ідентифікування користувача # упізнання користувача (за прізвищем та паролем) для визначення його повноважень.

identifier – ідентифікатор # 1. один або кілька символів, які застосовують для ідентифікації чи іменування елементів даних, а також для позначення деяких властивостей цього елемента даних # 2. лексичний токен, який іменує мовну конструкцію # наприклад імена змінних, масивів, записів, міток, процедур тощо # ідентифікатор зазвичай складено з літер, за якими, за потрібності, слідують літери, цифри чи інші символи # 3. лексична одиниця, що використовується як ім'я для елементів мови; ім'я, що присвоюється даним і являє собою

послідовність латинських літер і цифр, яка починається з літери.

identity – ідентичність # набір атрибутів, пов'язаних з об'єктом # у конкретному контексті ідентичність може мати один або кілька ідентифікаторів, які дозволяють однозначно розпізнавати об'єкт в цьому контексті.

identity authentication – автентифікація персональних даних # виконання тестів, що дають змогу системі опрацювання даних розпізнавати об'єкти # наприклад перевірка паролю чи токену ідентифікаційних даних.

identity information verification – перевірка інформації ідентичності # процес перевірки ідентифікаційної інформації та повноважень щодо емітентів, джерел даних, або інших внутрішніх або зовнішніх ресурсів по відношенню до автентичності, достовірності, коректності та зв’язків об'єкта.

identity proofing – доказ ідентичності # процес, за допомогою якого орган реєстрації (Registration Authority – RA) здобуває і перевіряє інформацію, достатню для ідентифікації об'єкту на зазначеному або зрозумілому рівні гарантування.

identity token – маркер ідентичності # пристрій, що його застосовують для справжності автентифікації персональних даних # наприклад смарт-карта, металевий ключ.

identity validation – перевірка особистих даних # виконання тестів, що дають змогу системі опрацювання даних розпізнавати об'єкти # наприклад перевірка паролю чи токену ідентифікаційних даних.

identity-based security policy – ідентифікаційна стратегія захисту # стратегія захисту інформації, заснована на ідентифікаторах і/або атрибутах користувачів, групи користувачів або логічних об'єктів, що діють від імені користувачів і доступних їм ресурсів/логічних об'єктів.

IDS – intrusion detection system – система виявлення вторгнень.

IDS – intrusion detection system – система виявлення вторгнень.

IESG – Internet Engineering Steering Group – інженерна керуюча група Інтернету

IETF – Internet Engineering Task Force – робоча група інженерів Інтернету.

IGP – interior gateway protocol – протокол внутрішнього шлюзу.

illegal access – несанкціонований доступ # навмисне звернення користувача до даних, доступ до яких йому не дозволений, з метою їхнього читання, оновлення або руйнування.

illegal access to hardware – несанкціонований до апаратури # дії порушника, спрямовані на здійснення доступу до внутрішнього монтажу, ліній зв’язку, технологічних органів управління з метою: зміни та руйнування принципової схеми обчислювальної системи і апаратури; приєднання стороннього пристрою; зміни

алгоритму роботи обчислювальної системи шляхом використання технологічних пультів і органів управління; завантаження сторонніх програм і внесення комп'ютерних вірусів у систему; використання терміналів системи і т. ін.

illegal extraction of information – нелегальне добування інформації # одержання даних і відомостей в результаті проведення таємних заходів спеціальними службами і органами розвідки. Нелегальне добування інформації застосовують для одержання найбільш цінних даних і відомостей.

image – зображення # відображення інформації, візуальне подання даних.

imagery intelligence – видова розвідка # повітряна і космічна розвідка з використанням оптико- електронних засобів. У видовій розвідці найновіші досягнення в галузі електроніки, оптики, техніки обчислювальної, зв'язку, дистанційного зондування і технологій інформаційних. Об'єднання видової розвідки і картографування дає можливість одержання точної видової і геокосмічної інформації.

IMAP – Internet message access protocol – протокол доступу до повідомлень Інтернет.

IMINT – imagery intelligence – видова розвідка.

immunity– захищеність # див. protectability, proofness.

impact – вплив # дія, здійснювана ким-, чим-небудь на кого-, що-небудь.

impact on enemy resources – впливи на ресурси противника # вид протидії інтелектуальної в мережах інформаційно-обчислювальних(ІОМ), що припускає поглинання ресурсів мережі і неефективне їхнє використання противником. До таких ресурсів відносять: час, що затрачається противником для досягнення мети нападу інформаційного; ресурси обчислювальних засобів, що затрачаються противником в ході атаки інформаційної і в процесі верифікації інформації, одержаної від об'єкта, що атакується; людські ресурси, що затрачаються в ході боротьби інформаційної; морально-психологікова стійкість осіб, що беруть участь в інформаційній боротьбі на стороні противника; ресурси інформаційні противника, що формуються в результаті інформаційних атак на ІОМ; зброя інформаційна противника й способи її застосування; матеріальні й фінансові витрати противника на ведення війни інформаційної.

IMS – IP multimedia subsystem – мультимедійна підсистема IP-мережі.

IN – intelligent network - інтелектуальна мережа.

incident – інсцедент # група атак, які згруповані за ознакою типу, техніки проведення, часом та типом елементів операційних систем.

inclined masks – похилі маски # штучні оптичні маски, які використовують для приховування тіней об'ємних

об’єктів, за довжиною яких з врахуванням положення сонця можна визначити висоту об’єктів при спостереженні зверху (з літаків і космічних апаратів).

indication object – ознака об’єкта # ознаки, властиві конкретному об’єктові, які дозволяють виявляти цей об’єкт серед інших схожих об’єктів та розпізнавати його належність, призначення, функції, властивості, особливості й характеристики. Ознаки об’єкта складають частину його ознак, а їхні значення відрізняються від значень відповідних ознак інших об’єктів. Ознаки об’єкта описують його різноманітні стани, характеристики й властивості. У найбільш загальному випадку ознаки об’єкта поділяють на розпізнавальні ознаки і ознаки діяльності об’єктів. Ознаки об’єкта поділяють на видові, ознаки сигналів та ознаки речовин. За інформативністю ознаки поділяються на іменні, прямі та непрямі. За часом прояву ознаки поділяються на постійні, періодичні та епізодичні.

indication– ознака # див. sign.

indicator – індикатор # показник # міра, яка надає оцінку або значення визначеного атрибута, отриманого з аналітичної моделі відносно визначених інформаційних потреб.

indigenous error – локальні помилки # помилка в програмі, яка не була навмисно вставлена як частину процесу виявлення помилок.

indigenous fault – локальні помилки # помилка в програмі, яка не була навмисно вставлена як частину процесу виявлення помилок.

indirect sign – непряма ознака # ознака, що не належить безпосередньо об’єктові, але відображає властивості і стан об’єкта. Такі ознаки є результатом взаємодії об’єкта з навколишнім середовищем.

indistinguishable ensembles – нерозрізнені ансамблі # ансамблі, які не можна відрізнити один від одного за допомогою будь-якого алгоритму ймовірнісного поліноміального. Більш точно – це такі ансамблі $/X_n/_{n\in N}$ та $/Y_n/_{n\in N}$, для яких для будь-якого ймовірнісного поліноміального алгоритму A: $|P[A(X_n) = 1] - P[A(Y_n) = 1]| < 1/n^c$ для довільної константи c при досить великих n. Тут $P[A(X_n) = 1]$ – ймовірність того, що алгоритм A розпізнає ансамбль X^n.

individual – індивід # окрема людина, особа.

individual resistance – індивідуальна опірність # протидія навіюванню зі сторони однієї людини. Встановлена залежність цього різновиду опірності навіюванню від індивідуальних і вікових особливостей психіки (стійкості поглядів і переконань, багатства життєвого досвіду, загальної критичності, співвідношення між раціональними й емоційними сторонами психіки і т. ін.).

individual-personality features – індивідуально-особистістні особливості # характеристики різних категорій людей, специфіку яких необхідно враховувати, для

досягнення максимального ефекту впливу психологічного. Існує ряд класифікацій, що дозволяють відрізняти одні категорії людей від інших. Так за класифікацією Кречмера-Шелдона, що заснована на взаємозв'язку між статурою й характером, розглядають три основних групи людей: пікніки (ендоморфи), атлетіки (мезоморфи), астеніки (ектоморфи). За темпераментом люди поділяються на сангвініків, флегматиків, холериків, меланхоліків. За акцентуацією характеру (гіпертрофією окремих рис характеру порівняно з іншими рисами) налічується декілька десятків різновидів типів людей: демонстративний (істероїдальний) тип; застряваючий (параноїдальний) тип; збудливий тип; боязливий (сензитивний) тип; екзальтований тип; епілептоїдний тип і т.ін. Акцентуйовані особистості особливо уразливі по відношенню до одних впливів, що травмують психіку, в цей же час мають дуже високу стійкість до інших впливів.

industrial espionage – промисловий шпіонаж # сукупність операцій таємних, які здійснюються корпораціями або державами у відношенні інших корпорацій або держав; наприклад, збирання інформації про конкурентів, викрадення патентної інформації і навіть акти саботажу у формі викривлення даних або послуг.

industry – індустрія # 1. промисловість # 2. виробництво.

inference – умовиводи # розумова діяльність на основі властивих індивідуальній свідомості норм висновків, які співпадають багато в дечому з правилами і законами логіки.

inference access control – керування доступом за аналізом відкритої інформації # керування доступом до інформації про окремий атрибут, яка отримується шляхом аналізу інформації про сукупність атрибутів (отримується інформаційно-аналітичним шляхом).

infiltration – інфільтрація # 1. просочування, проникнення # 2. процес проникнення агента на територію ворожої держави або у ворожу організацію. В першому випадку впровадження може бути як відкритим (коли агент має легальне прикриття і на законних засадах приїжджає в країну), так і таємним (коли він нелегально перетинає кордон сушею, повітрям або водою).

infopolicy – інформаційна політика # головні напрямки і предмет діяльності держави в галузі інформації. Основною метою інформаційної політики є створення умов для ефективного і якісного інформаційного забезпечення стратегічних і оперативних завдань соціального і економічного розвитку держави. Основними напрямками такої політики є: забезпечення умов для розвитку і захисту всіх форм власності на ресурси інформаційні; формування і захист державних інформаційних ресурсів; створення і

розвиток центральних і регіональних мереж інформаційних і систем інформаційних, забезпечення їхньої сумісності і взаємодії в єдиному просторі інформаційному держави; створення умов для якісного і ефективного інформаційного забезпечення громадян, установ державної влади, органів місцевого самоуправління, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення безпеки національної в сфері інформатизації, а також забезпечення прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення і удосконалення системи інвестування і механізму стимулювання розробки і реалізації проектів інформатизації; розвиток законодавства у сфері процесів інформаційних, інформатизації і захисту інформації.

informatics – інформатика # див. computer science.

information – інформація # 1. відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиюсь діяльність, що їх сприймають людина і живі організми, керуючі машини та інші системи. За змістом будь-яка і. може бути віднесена до семантичної (цією, що містить смисл) або до інформації про ознаки матеріального об'єкта – ознакової # 2. зміст повідомлення, сигналу, пам'яті, а також відомості, що містяться в повідомленні, сигналі або пам'яті # 3. змістовно-суттєва частина знань (відомостей, даних) про склад, структури і алгоритми предметної частини, яка є потенційно доступною для кількісних оцінок. Неформально за кількісну міру і. можна вважати різницю між кількістю інформаційних невизначеностей апріорної і апостеріорної. Від'ємне значення цієї різниці часто називають дезінформацією # 4. в техніці обчислювальній — сукупність всіх даних і програм, які використовуються в системі автоматизованій незалежно від способу їхнього фізичного та логічного подання.

information access method – метод доступу до інформації # способи, прийоми забезпечення доступу до інформації. Можна поділити на три групи: проникнення розвідника до джерела інформації фізичне; залучення до співробітництва з органами розвідки осіб, які мають легальний або нелегальний доступ до інформації, що цікавить розвідку; дистанційне знімання інформації з носія.

information accumulation – накопичення інформації # один з

основних видів роботи інформаційної. Розрізняють нагромадження інформації активне і нагромадження інформації пасивне. Розвиток інформатики постійно пересуває межу можливостей добування знань при накопиченні інформації із застосуванням ЕОМ. Одне з первинних завдань накопичення інформації – перетворення нагромаджуваної інформації з форми у вигляді фізичних сигналів у символьну форму, а також стиснення інформації, тобто зменшення надмірності в її поданні. При цьому часто доводиться вирішувати задачу розпізнавання образів, наприклад, розпізнавання мови, оброблення зображень.

information action – інформаційні дії # сукупність узгоджених за метою, завданнями, місцем і часом заходів, що проводяться силами і засобами, залученими для ведення боротьби інформаційної, протягом певного часу в певному районі (напрямку). Під час виконання інформаційні дії можуть здійснюватися удари інформаційні. Інформаційні дії можна класифікувати за видами (наступальні і оборонні), масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні і тактичні) і об'єктами впливу (інформаційні системи, морально-психологічний стан особового складу та їхня комбінація). До наступальних інформаційних дій відносять вплив інформаційний (акція інформаційна) та блокада інформаційна, до оборонних – дії (акції) з інформаційного захисту.

information activity – діяльність інформаційна # сукупність процесів збирання, накопичення, аналізу, перетворення, зберігання, пошуку і розповсюдження інформації (а також інших допоміжних процесів, що забезпечують ці основні процеси), що систематично здійснюються будь-якою організацією (установою, підрозділом, групою осіб і т. ін.).

information **advantage** – інформаційна перевага # ситуація, при якій є можливість змінити уявлення противника про дійсну обстановку і позбавити його здатності прогнозувати подальші події та впливати на них. Основою здобуття інформаційної переваги є більш швидке одержання і використання оперативної інформації, ніж це може зробити противник.

information agency – інформаційне агенство # агентство новин.

information agency – інформаційний # установа або підрозділ, який постійно здійснює роботу інформаційну.

information aggressiveness measure – міра інформаційної агресивності #обсяг інформації, що цілеспрямовано передається від однієї системи інформаційної до іншої.

information analysis – аналіз інформації # систематичне дослідження інформації та її потоку в реальній або запланованій системі.

information and computing center – інформаційно-обчислювальний центр # центр обчислювальний, що має інформаційну систему автоматизовану і забезпечує як інформаційне обслуговування користувачів, так і вирішення широкого кола обчислювальних задач.

information attack – інформаційна атака # атака на мережу обміну інформацією віддалена, яка полягає у раптовому застосування зброї інформаційної для здійснення впливів на мережу противника. Ефективність н. і. досягається у тому випадку, якщо забезпечені його широкомасштабність, довгостороковість та скритність.

information attack – інформаційна атака # сукупність активних впливів інформаційних сил і засобів окремих підрозділів на елемент або групу елементів систем інформаційних противника з метою

information bank – банк даних # БнД # див. databank.

information base – інформаційна база # в системах автоматизованих – сукупність даних, розташованих на зовнішніх носіях і призначених для використання програмами та користувачами. Наприклад, в банках даних інформаційна база – це частина інформаційного фонду, що охоплює бази даних і їхні описи метаданих.

information battle center – інформаційний центр бойових дій # військова частина (підрозділ), призначений для створення засобів ведення війни інформаційної на підтримку операцій; планування компаній, придбання і випробовування обладнання, захисту штабів від інформаційного нападу. З цією метою центр навчає, споряджає і розгортає групи реагування, розробляє і підтримує бази даних і програми прикладні, проводить аналіз уразливості електронних систем своїх військ (сил).

information blockade – інформаційна блокада # узгоджене за завданнями, місцем і часом застосування сил і засобів із метою найбільш повного зниження можливостей противника з одержання і використання інформації, необхідної для ефективного ведення операцій (бойових дій). Одним з основних способів досягнення мети інформаційної блокади є блокування радіоелектронне.

information carrier – носій інформації # матеріальний об’єкт, що містить інформацію, яка підлягає захисту від загроз.

information carrier across state border – носій інформації через державний кордон # носії інформації, які можуть легально або нелегально перетинати державний кордон. Основними носіями такого виду є: люди, що зберігають інформацію у своїй пам’яті; матеріальні тіла з інформацією, які перевозяться або переносяться людьми; електромагнітні випромінювання у

світловому (оптичному) та радіодіапазонах.

information carrier of constituting state secre – носій відомостей, що складають державну таємницю # матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що складають таємницю державну, знаходять своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів.

information center – інформаційний центр # постійний чи тимчасово діючий орган, який здійснює обслуговування інформаційне по колу заздалегідь визначених питань. Зазвичай під інформаційним центром розуміють спеціалізована установа, що організує і координує роботу прямо чи побічно підпорядкованих йому інформаційних підрозділів.

information classification – класифікація інформації # процес віднесення відселектованої інформації до конкретної відомості кадастру інформаційного.

information classification mark determining criterion – критерій для визначення грифа конфіденційності інформації # результати прогнозу наслідків попадання інформації до конкурента або зловмисника, в тому числі: величина економічних і моральних збитків, що можуть бути нанесені організації; реальність створення передумов для катастрофічних наслідків в діяльності організації, наприклад, банкрутства тощо.

information coding – кодування інформації # перетворення інформації у вигляді умовних сигналів з метою автоматизації її зберігання, оброблення, передавання і вводу-виводу.

information completeness – повнота інформації # характеристика, яка визначає кількість інформації, необхідної для прийняття рішення.

information computer network – інформаційно-обчислювальна мережа # сукупність зв'язаних лініями зв'язку інформаційно-обчислювальних центрів, призначених для оброблення інформації.

information confidentiality – конфіденційність інформації # властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

information confrontation – інформаційне протиборство # процес реалізації впливів інформаційних, спрямованих на досягнення мети державної політики в мирний і воєнний часи. Має місце у відносинах між державами незалежно від розвитку співробітництва між ними.

information co-operation – інформаційна кооперації # форма забезпечення інформаційної безпеки між рівноправними суб'єктами

процесу інформаційного (фізичними, юридичними, міжнародними), що охоплює сукупність їхніх взаємоузгодженпх дій, спрямованих на одержання відомостей про фактори дестабілізуючі і загрози інформаційні та захист від них доступними законними способами і засобами.

information counteraction – інформаційна протидія # сукупність заходів боротьби інформаційної, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. Інформаційна протидія охоплює блокування добування, оброблення і обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання інформаційної протидії вирішують шляхом маскування, контррозвідки, придушення радіоелектронного і руйнування систем інформаційних противника.

information crisis – інформаційна криза # перехідний, нестійкий стан будь-якої системи, пов'язаний із серйозними порушеннями в організації потоків інформаційних та здійсненні процесів інформаційних.

information density – інформативність # інтенсивність потоку інформації.

information department – інформаційний орган # див. information agency.

information distribution industry – індустрія розповсюдження інформації # галузь індустрії інформаційної, пов'язана із створенням і керуванням телекомунікаціями й мережами розповсюдження інформації. Вона охоплює телекомунікаційні компанії, мережі кабельного телебачення, системи сунуті пікового мовлення, радіо- і телевізійні станції, компанії стільникового зв'язку і т. ін.

information element – інформації елемент # інформація на носії з достатньо чіткими межами, що задовольняє наступним вимогам: належить конкретному джерелу (документу, людині, зразка продукції і т. ін.); міститься на окремому носії; має конкретну ціну.

information encryption – шифрування інформації # перетворення криптографічне інформації з метою її захисту від доступу несанкціонованого.

information environment – інформаційна сфера # сфера діяльності суб'єктів, зв'язана із створенням, перетворенням і споживанням інформації. Інформаційна сфера умовно поділяється на три основні предметні частини: створення і розповсюдження інформації вихідної та похідної; формування ресурсів інформаційних, підготовки продуктів інформаційних, надання послуг інформаційних; споживання інформації та дві забезпечувальні предметні частини: створення і застосування систем інформаційних, технологій інформаційних і засобів їхнього забезпечення; створення і

застосування засобів і механізмів інформаційної безпеки.

information environment – інформаційне середовище # сфера діяльності суб'єктів, зв'язана із створенням, перетворенням і споживанням інформації.

information evaluation – інформаційна оцінка # документ, в якому аналізується існуюче на даний момент положення, або робиться прогноз про розвиток подій на майбутнє; будь-яке передбачення, яке міститься в інформаційному документі.

information exchange network – мережа обміну інформацією # теж, що інформаційна мережа; складова частина мережі інформаційно-обчислювальної.

information explosion – інформаційний вибух # стрімке зростання загального обсягу інформації, що створюють в межах будь-якої галузі діяльності або суспільства у цілому на певному етапі їхнього розвитку.

information extraction agency – орган добування інформації # спеціалізовані органи, призначені для добування інформації. Найчастіше є складовою частиною органів розвідки.

information falsification – підробка інформації # навмисні дії, що призводять до зміни інформації, яка повинна оброблятися або зберігатися в системі обчислювальній.

information flow – інформаційний потік # інформація, що знаходиться в упорядкованому русі по заданих напрямках із фіксованими початковими, проміжними та кінцевими точками.

information flow – потік інформації # передавання інформації від одного до іншого об'єкта комп'ютерної системи.

information hiding – інформаційне приховування # приховування інформації, яке досягається зміною портрета інформаційного або створенням неправдивого (хибного) інформаційного портрета семантичного повідомлення, фізичного об'єкта або сигналу. Для зміни інформаційного портрета семантичного повідомлення може застосовуватися, наприклад, перетворення криптографічне інформації. Для створення хибного інформаційного портрета семантичного повідомлення можуть використовуватися методи стеганографії.

information impact – інформаційний вплив # *1.* організоване застосування сил і засобів боротьби інформаційної для вирішення завдань завоювання (підтримки) переваги інформаційної над противником # *2.* вплив, який здійснюється із застосуванням засобів зброї інформаційної, які дозволяють здійснювати з інформацією, що передається, оброблюється, створюється, знищується і сприймається, задумані дії. Інформаційний вплив буде допустимим, якщо він грубо не порушує прийняті у більшості систем інформаційних в даному

інформаційному просторі норми і правила поведінки (вихідні результати).

information industry – інформаційна індустрія # галузь економіки, зв'язана з виробництвом, обробленням, передаванням, збереженням всіх видів інформації, створенням необхідних для цього технологічних пристроїв. До неї входять приватні й державні організації, які створюють інформацію різноманітних видів, власність інтелектуальну, забезпечують функціонування пристроїв для розповсюдження інформації споживачам, виробляють обладнання і програмне забезпечення, призначене для оброблення інформації. Інформаційна індустрія можна представити у вигляді трьох її галузей, які створюють зміст (індустрія змісту), його розповсюджують (індустрія розповсюдження інформації) і оброблюють (індустрія оброблення інформації). Вона є найбільш динамічним сектором світової економіки, породжує продукти й послуги, які суттєво змінюють характер ведення бізнесу в традиційних галузях, безпосередньо не зв'язаних із створенням і розповсюдженням інформації Використання інформаційно-телекомунікаційних технологій у багатьох сферах послуг і промисловості стало цілком необхідним елементом конкурентної боротьби і стратегічного розвитку.

information integrity – цілісність інформації # властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

information integrity violation – порушення цілісності інформації # спотворення інформації, її руйнування або знищення.

information interlock – блокування інформації # дії, наслідком яких є припинення доступу до інформації користувачів інформаційної системи.

information law – інформаційне право # система соціальних норм і відносин, що виникають у сфері інформаційній і охороняються силою держави. Відносини, що виникають при здійсненні процесів інформаційних (відносини інформаційні), є основними об'єктами правового регулювання. Нормативну базу інформаційного права складає законодавство інформаційне. Інформаційне право є правовим фундаментом інформаційногосуспільства.

information leakage – витік інформації # *1.* несанкціонований процес перенесення інформації від джерела до зловмисника. Витік інформації є можливим шляхом її розголошення людьми, втрати ними носіїв з інформацією, перенесення

інформації за допомогою випромінювання, потоків елементарних часток, речовин в газоподібному, рідкому або твердому стані. Витік інформації у порівнянні з утратою (викраденням) матеріальних об'єктів має ряд особливостей, які необхідно враховувати при організації захисту інформації: витік інформації може здійснюватися тільки при попаданні її до зацікавленого в ній несанкціонованого одержувача (зловмисника); при витоку інформації здійснюють її тиражування, яке не змінює характеристики носія інформації; ціну інформації при її витоку зменшують за рахунок тиражування; факт витоку інформації, як правило, виявляють через деякий час, за наслідками витоку, коли заходи забезпечення її безпеки можуть виявитися неефективними. Витік інформації здійснюють каналами витоку # *2.* просочування в засоби масової інформації відомостей із закритих або малодоступних джерел. Ці відомості можуть або слугувати на благо суспільним інтересам, або стати засобом маніпулювання суспільною думкою.

information leakage – витік інформації # неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

information leakage channel comprehensive model – комплексна модель каналу витоку інформації # модель, що об'єднує і ув'язує між собою статичні і динамічні моделі каналу витоку інформації. В ній вказуються інтегральні параметри каналу витоку інформації: джерело інформації і його вигляд, середовище розповсюдження і його протяжність, місце розташування приймача сигналу, інформативність каналу і показники загрози безпеці інформації.

information leakage channel functional model – функційна модель каналу витоку інформації # модель, що характеризує режими функціювання каналу витоку інформації, інтервали часу, протягом якого можливий витік інформації.

information leakage channel information model – інформаційна модель каналу витоку інформації # модель, що містить характеристики інформації, витік яких можливий каналом витоку інформації: кількість і цінність інформації, пропускна здатність каналу, прогнозована якість інформації, що приймається зловмисником.

information leakage channel spatial model – просторова модель каналу витоку інформації # модель, що містить опис положення каналу витоку інформації у просторі: місця розташування джерела і приймача сигналів, їхня відстань від меж території організації, орієнтація вектора розповсюдження носія інформації в каналі витоку інформації і його протяжність. Таку модель доцільно подавати у вигляді графа на плані приміщення, будівлі,

території організації, прилеглих зовнішніх ділянок середовища.

information leakage channel structural model – структурна модель каналу витоку інформації # модель, що описує структуру (склад і зв'язки) каналу витоку інформації. Таку модель доцільно подавати в табличній формі.

information legislation – інформаційне законодавство # сукупність правових актів нормативних і окремих норм права, спрямованих на регулювання суспільних відносин у сфері інформаційній. Інформаційне законодавство є нормативною базою права інформаційного і являє собою комплексну галузь, що охоплює як деякі галузі законодавства і спеціальні нормативні акти, повністю присвячені проблемам інформації, так і окремі норми інформаційно-правові в актах інших галузей законодавства.

information lifecycle – життєвий цикл інформації # період існування інформації, починаючи з її створення до споживання.

information loss – втрата інформації # *1.* дія, внаслідок якої інформація в системі інформаційній перестає існувати для користувачів # *2.* неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

information **management** – адміністративне керування інформацією # 1. назва галузі досліджень, спрямованих на виявлення конкретних форм і засобів регулювання процесів вибору і розповсюдження інформації каналами зв'язку (засобами масової інформації) # 2. керуюча діяльність щодо процесів інформаційних, яка охоплює збирання (добування), оброблення та розповсюдження (доведення) інформації. Важливу роль в керуванні інформацією відіграють зворотні зв'язки з рівня споживання інформації на рівні оброблення та добування.

information message – інформаційне повідомлення # див. data message.

information method of protection – інформаційний метод захисту # метод захисту, що полягає у спеціальному перетворенні інформації, що обробляється в обчислювальній системі.

information metrology – інформаційна метрологія # стандартизація, нормативне закріплення понять і термінів в галузі інформації.

information model – інформаційна модель # 1. формалізований опис інформаційних структур і операцій над ними # 2. параметричне подання процесу циркуляції інформації, яке підлягає автоматизованій обробці в системі керування.

information need – інформаційна потреба # розуміння, необхідне для керування цілями, задачами, ризиками й проблемами.

information network – інформаційна мережа # сукупність систем інформаційних автоматизованих, об'єднаних в єдину мережу за допомогою засобів передавання

даних. Користувач має доступ до інформації будь-якої автоматизованої інформаційної системи, що входить до мережі.

information network security – безпека інформаційної мережі # стан мережі інформаційної, при якому забезпечують безпеку даних, які знаходяться в ній.

information node – інформаційний вузол # сукупність елементів і зв'язків найбільш інформативної частини інформаційного портрета. До інформаційного вузла відносять принципово нові технічні, технологічні і образотворчі рішення та інші досягнення, які складають ноу-хау.

information noises – інформаційні шуми # в комунікативістиці – різного роду трансляції та тексти (від зведень новин до рекламних кліпів), що здійснюють негативний вплив на вдачу та культуру суспільства. З інформаційними шумами також пов'язують процеси наростання перевантажень комунікаційних # див. noises.

information object – інформаційний об'єкт # набір даних, які представляють інформацію про об'єкт # наприклад повідомлення, контакти, звіт.

information onstituting a state secret – відомості, що складають державну таємницю # відомості, розповсюдження яких може заподіяти шкоду державі. До таких відомостей можуть бути віднесені відомості: в воєнній галузі; в галузі економіки, науки і техніки; в галузі зовнішньої політики і економіки; в галузі розвідувальної, контррозвідувальної і оперативно-розшукової діяльності

information operation – інформаційна операція # сукупність узгоджених за метою, завданнями, місцем і часом дій (акцій), ударів, і битв, що проводяться за єдиним замислом і планом для вирішення завдань боротьби інформаційної (завоювання і утримання переваги інформаційної над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямах. Інформаційні операції можуть бути наступальними і оборонними. Мета о. і. досягається вирішенням наступних завдань: інформаційним впливом на противника, захистом інформаційним і ефективним використанням ресурсів інформаційних власного угруповання військ (сил). Інформаційні операції проводять в межах відповідної загальновійськової, самостійної, спільної або спеціальної операції. Інформаційну операцію можна класифікувати за масштабами як стратегічні, оперативно-стратегічні, оперативні і оперативно-тактичні і характеризувати наступними основними показниками: просторовим розмахом, тривалістю, а також кількісним і якісним складом сил і засобів.

information overload – інформаційне перевантаження # надлишкова,

кумулятивно зростаюча інформація, що поступає різними каналами засобів масової інформації і здатна чинити негативний вплив на стан здоров'я, психіки і менталітету людей.

information owner – власник інформації # *1.* суб'єкт, що здійснює володіння і використання інформації та реалізує повноваження на розпорядження інформацією у межах прав, встановлених законом або особою, яка володіє інформацією # *2.* суб'єкт відносин інформаційних, який має право на володіння, розпорядження й користування ресурсом інформаційним за угодою з установою (особою), що володіє інформацією.

information portrait – інформаційний портрет # сукупність елементів і зв'язків між ними, що відображають суть повідомлення (мовного або даних), ознаки об'єкта або сигналу. Елементами дискретного семантичного повідомлення, наприклад, є букви, цифри або інші знаки, а зв'язки між ними визначають їхню послідовність. Інформаційний портрет об'єктів спостереження, сигналів або речовин є їхні структури ознакові еталонні.

information portrait changing method – метод зміни інформаційного портрета # метод приховування інформації, яке досягається наступними способами: видалення частини елементів і зв'язків, що створюють вузол інформаційний (найбільш інформаційну частину) портрета; зміни частини елементів інформаційного портрета при збереженні незмінності зв'язків між елементами, що залишилися; видалення або зміна зв'язків між елементами інформаційного портрета при збереженні їхньої кількості. Зміни інформаційного портрета об'єкта викликають зміни зображення його зовнішнього вигляду (видових демаскуючих ознак), характеристик випромінюваних ними полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на приближения ознакових структур об'єкта до оточуючого його фону, в результаті чого понижується контрастність зображення об'єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання. Проте при зміні інформаційного портрета інформація може не сприйматися не тільки зловмисником, але і її санкціонованим одержувачем. Для санкціонованого одержувача інформаційний портрет повинен бути відновлений шляхом додаткового передавання йому видалених елементів і зв'язків або алгоритму (ключа) цих змін.

information power – інформаційна влада # здатність, право і можливість розпоряджатися будь-ким, будь-чим, здійснювати вирішальний вплив на будь-кого на основі зростання значення інформації і сили її впливу на політичні процеси, на процедури

вироблення і прийняття важливих рішень, їхньої пропаганди і реалізації. Лідирує той, хто володіє повною і своєчасною інформацією. Цілеспрямована інформація важлива також для створення іміджу владі, політиці і політикам, вона здатна керувати поведінкою великих груп людей. Зростання ролі такої інформації привело до появи маркетингу політичного.

information process – інформаційні процеси # процеси створення, збирання, оброблення, накопичення, зберігання, пошуку, розповсюдження і споживання інформації в державі і суспільстві, а також процеси створення і застосування систем інформаційних, технологій інформаційних і засобів їхнього забезпечення, засобів і механізмів безпеки інформаційної.

information processing facilities – засоби оброблення інформації # будь-яка система оброблення інформації, служба чи інфраструктура, чи місце, де їх фізично розміщено.

information procuring – добування інформації # сукупність заходів і дій, спрямованих на забезпечення контакту розвідувального з джерелом інформації та одержання від нього даних і відомостей. В найбільш загальному випадку д. і. являє собою процес, який починається з моменту поставлення завдання її споживачами до моменту подання даних і відомостей в органи збирання і оброблення інформації або безпосередньо користувачу. Добування інформації здійснюється постійно легальними способами на основі принципів добування інформації, а при недостатності одержаної цими способами інформації – шляхом проведення таємних операці .

information products – інформаційна продукція # інформація документована, підготовлена у відповідності до вимог користувачів і призначена або застосовується для задоволення потреб користувачів. До інформаційної продукції відносять: документи, дані; відбірки документів, даних; довідки, аналітичні довідки; бази даних, банки даних; інші види інформаційних продуктів.

information protection actions – дії з інформаційного захисту # оборонні дії інформаційні, узгоджені за завданнями, місцем і часом застосування залучених до ведення боротьби інформаційної сил і засобів з метою забезпечення стійкості функціонування системи управління військами (силами) в умовах впливу інформаційного противника.

information protection in automated system – захист інформації в автоматизованій системі # діяльність, яка спрямована на забезпечення безпеки інформації, що оброблюється в системі автоматизованій, та автоматизованої системи в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити

величину потенційних збитків унаслідок реалізації загроз.

information protection method – метод захисту інформації # сукупність способів, прийомів або системи прийомів, що запобігають несанкціонованому доступу до інформації. При наявності простих засобів зберігання і передавання інформації можуть бути використані традиційні методи її захисту від зловмисного доступу: обмеження доступу; розмежування доступу; розділення доступу (привілеїв); криптографічне перетворення інформації; контроль і облік доступу; законодавчі заходи. При автоматизованому обробленні інформації у зв'язку із збільшенням обсягів, зосередженням інформації, збільшенням кількості користувачів та іншими причинами, що зумовлюються ускладненням технічних засобів оброблення та різноманітними видами носіїв інформації, одержали розвиток як традиційні, так і нові методи захисту: функційний контроль, що забезпечує виявлення і діагностику відмов, збоїв апаратури і програмних помилок та помилок людини; підвищення вірогідності (достовірності) інформації; захист інформації від аварійних ситуацій; контроль доступу до внутрішнього монтажу апаратури, ліній зв'язку і технологічних органів керування; розмежування і контроль доступу до інформації; ідентифікація і автентифікація користувачів, технічних засобів, носіїв інформації і документів; захист від побічних електромагнітних випромінювань і наведень.

information protection method by technical means – метод захисту інформації технічними засобами # сукупність способів забезпечення захисту інформації для певних варіантів співвідношень між джерелами, носіями інформації та зловмисниками: джерело і носій інформації локалізовані в межах розташування об'єкта захисту і забезпечена механічна перепона від контакту з ними зловмисника або дистанційного впливу на них полів його технічних засобів добування інформації; такі співвідношення енергії носія і завад на виході приймача каналу витоку такі, що зловмиснику не вдається зняти інформацію з носія з необхідною для її використання якістю; замість істинної інформації зловмисник одержує неправдиву, яку він приймає за істинну. Ці варіанти реалізуються наступними способами захисту: перешкоджання безпосередньому проникненню зловмисника до джерела інформації за допомогою інженерних конструкцій і технічних засобів охорони; приховування достовірної інформації; «підсовування» зловмиснику неправдивої (хибної) інформації. У зв'язку з цим розрізняють два основних методи захисту інформації технічними засобами: метод охорони

джерел інформації і метод приховування інформації.

information protection object – об'єкт захисту інформації # система оброблення даних, що містить інформацію, яку належить захищати.

information protection system – система захисту інформації # сукупність взаємозв'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації. Такими елементами є люди (керівництво і співробітники організації, насамперед, служби безпеки інформації), інженерні конструкції та технічні засоби, що забезпечують захист інформації. Метою створення системи є забезпечення необхідних рівнів безпеки інформації на об'єкті захисту. Завдання системи захисту інформації конкретизуються стосовно до видів і категорій інформації, що підлягає захисту, а також елементів об'єкта захисту. Входами системи є дії з реалізації загроз, які в процесі реалізації заходів захисту інформації, вибраних на основі критерію ефективності системи захисту інформації, визначають варіант системи захисту (вихід системи захисту інформації). Обмеженнями системи є людські, матеріальні, фінансові ресурси, що виділяються на захист інформації, а також обмеження у вигляді вимог до системи, що передбачають прийняття таких заходів захисту інформації, які не знижують ефективність функціонування об'єкта, що підлягає захисту.

information relations – інформаційні відносини # *1.* відносини, що виникають при здійсненні процесів інформаційних. Основним предметом, із приводу якого або у зв'язку з яким виникають інформаційні відносини, є інформація в усіх її видах і формах. Інформаційні відносини людино-машинних об'єктів і систем в інформаційних середовищах пропонують розглядати як загальнотеоретичні (внутрішні і зовнішні) або прикладні. Серед прикладних виділяються два основні напрямки відносин – відносини інформаційної ізоляції і відносини інформаційної взаємодії # *2.* відносини (взаємодія) між діячами інформаційними. З інформатики відомо сім рівнів такої взаємодії в системах інформаційних: фізичний, канальний, мережііпіі. транспортний, сеансовий, представницький, прикладний. Інформаційні відносини бувають внутрішніми і зовнішніми. За характером інформаційного носія і. в. можуть бути розділені на три типи: об'єкт-об'єкт, суб'єкт-суб'єкт, суб'єкт-об'єкт. За метою функціонування діячів в умовах коаліцій або конфліктів в. і. розділяють на відносини інформаційні співробітництва і суперництва, дезорієнтування, дезінформування і дезорганізації з можливістю перетворення суб'єкта в об'єкт і навпаки. Сукупність

конфліктних відносин суперництва, що організуються стороною-суб'єктом із метою зробити іншу сторону об'єктом бажаного управління у своїх інтересах, означає боротьбу інформаційну.

information relations of cooperation – інформаційні відносини співробітництва # відносини інформаційні в працездатних системах інформаційних, для яких апостеріорну інформаційну невизначеність стану в процесі функціонування зменшують.

information relations of interaction – інформаційні відносини взаємодії # відносини інформаційні, спрямовані на забезпечення інформаційного суперництва та співробітництва інформаційного реальних систем інформаційних.

information relations of isolation – інформаційні відносини ізоляції # відносини інформаційні, спрямовані на забезпечення інформаційного відокремлення і захисту інформаційного реальних систем інформаційних.

information relations of rivalry – інформаційні відносини суперництва # антагоністичні відносини інформаційні, що відповідають безвихідним відносинам у непрацездатних системах, коли дії сторін збільшують невизначеність.

information resources – інформаційні ресурси # 1. результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі). Вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших носіях (мікрофішах, магнітних стрічках, відеодисках і т.ін.)., що зберігаються у довідково-інформаційних фондах інформаційних органів та бібліотек # 2. окремі документи і окремі масиви документів, документи і масиви документів в системах інформаційних (бібліотеках, архівах, фондах, банках, банках даних і т. ін.), що містять інформацію з усіх напрямків життєдіяльності суспільства. Інформаційні ресурси можна класифікувати: за видом інформації; за режимом доступу; за видом носія; за способом формування і розповсюдження; за способом організації зберігання і використання; за формою власності # 3. сукупність даних, що являє собою цінність для установи (підприємства) і виступає як матеріальні ресурси. До інформаційних ресурсів відносять основні та допоміжні масиви, що зберігаються у зовнішній пам'яті комп'ютерних систем, та вхідні документи.

information resources by form of ownership – інформаційні ресурси за формою власності # ресурси інформаційні, що можуть складати: загальнодержавне національне надбання; державну власність; муніципальну власність; приватну власність; колективну власність.

information resources by type of access regime – інформаційні ресурси за режимом доступу # ресурси інформаційні, що містять інформацію відкриту (без обмежень) або інформацію обмеженого доступу (державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну) таємницю).

information resources by type of carrier – інформаційні ресурси за видом носія # ресурси інформаційні, інформація в яких може бути записана на папері, на машиночитаних носіях, у вигляді зображення на екрані ЕОМ, в пам'яті ЕОМ, в каналах зв'язку, на інших видах носіїв.

information resources by type of information – інформаційні ресурси за видом інформації # ресурси інформаційні, що можуть містити інформацію наступних видів: правову інформацію; науково-технічну інформацію; політичну інформацію; економічну (фінансово-економічну) інформацію; статистичну інформацію; інформацію про стандарти і регламенти, метрологічну інформацію; соціальну інформацію; інформацію про охорону здоров'я; інформацію про надзвичайні ситуації; особисту інформацію (персональні дані);кадастри (земельний, містобудівний, лісовий, майновий і т. ін.); інформацію іншого виду.

information resources by way of formation and distribution – інформаційні ресурси за способом формування і розповсюдження # ресурси інформаційні, що знаходяться у стаціонарному або рухомому (мобільному) стані.

information resources by way of organization of storage and use – інформаційні ресурси за способом організації зберігання і використання # ресурси інформаційні, для зберігання і використання інформації в яких можуть використовуватися традиційні форми (масиви документів, фонди документів, архіви) або автоматизовані форми (банки даних, системи інформаційні автоматизовані, бази знань).

information resources owner – власник інформаційних ресурсів # суб'єкт, який у повному обсязі реалізує повноваження володіння, користування, розпорядження ресурсами інформаційними, системами інформаційними, технологіями інформаційними і засобами забезпечення інформаційних технологій.

information resources registration – реєстрування інформаційних ресурсів # процес, який разом з обліком інформаційних ресурсів забезпечує реалізацію функцій контролю за станом ресурсів інформаційних та компонентів системи захисту інформації в системі обчислювальній.

information safety system – система захисту інформації # див. information protection system.

information secrecy – секретність інформації # обмеження, що накладаються автором на доступ до його інформації інших осіб. Оформлюється присвоєнням інформації певного грифа секретності і досягається закриттям її паролем, шифруванням та іншими методами захисту інформації.

information security – інформаційна безпека # *1.* Стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечують їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз інформаційних. В залежності від виду загроз інформаційній безпеці можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації і інформаційних ресурсів від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини і громадянина # *2.* стан захищеності середовища інформаційного суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави # *3.* у праві інформаційному – одна із сторін розгляду відносин інформаційних у межах законодавства інформаційного з позицій захисту інтересів життєво важливих особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

information security – інформаційна безпека # збереження конфіденційності, цілісності і доступності інформації. Додатково можна враховувати інші властивості, такі як автентичність, відстежуваність, неспростовність та надійність.

information security continuity – безперервність інформаційної безпеки # процеси і процедури для забезпечення безперервних дій з інформаційної безпеки**.**

information security evaluation – оцінювання безпеки інформації # процес, метою кого є визначення відповідності стану безпеки інформації в системі комп'ютерній встановленим вимогам.

information security event – подія інформаційної безпеки # ідентифікований стан системи, служби чи мережі, який вказує на можливе порушення політики інформаційної безпеки чи відмови засобів безпеки, або раніше невідому ситуацію, яка може мати відношення до безпеки

information security in automated system – захист інформації в автоматизованій системі # див. information protection in automated system.

information security incident – інцидент інформаційної безпеки # одна або кілька небажаних або

несподіваних подій інформаційної безпеки, що мають значну ймовірність компрометації функціювання бізнесу та загрози інформаційній безпеці.

information security incident management – керування інцидентами інформаційної безпеки # процеси для виявлення, реєстрації, оцінювання, реагування, оброблення й дослідження інцидентів інформаційної безпеки.

information security legislation – законодавство про інформаційну безпеку # сукупність законів (норм інформаційно-правових), що регламентують відносини з приводу прав, обов'язків і відповідальності суб'єктів у зв'язку із створенням і застосуванням засобів і механізмів інформаційної безпеки у державі. Складовою частиною законодавства є сукупність актів нормативних, а також законів у галузі захисту державної таємниці. У зв'язку з введенням у практику мереж інформаційних транскордонних виникає необхідність правового регулювання відносин у галузі усіх видів і способів захисту інформації в цих мережах, насамперед засобами підпису цифрового електронного, засобами криптографічними.

information security mechanism – механізм інформаційної безпеки # сукупність заходів та процесів захисту інтересів життєво важливих особистості, суспільства, держави в сфері інформаційній, що здійснюються в межах законодавства. Вони повинні розроблюватися і впроваджуватися в кожній з предметних частин інформаційної сфери. У предметній частині створення інформації захисту в першу чергу належить: громадянин, суспільство, держава від впливу недостовірної, хибної інформації; інформація як інтелектуальна власність; документована інформація як інтелектуальна і речова власність; честь і достоїнство громадянина у зв'язку із створенням і розповсюдженням недостовірної інформації або несанкціонованим розповсюдженням інформації про нього. У предметній частині формування інформаційних ресурсів, підготовки і надання користувачам інформаційних продуктів, інформаційних послуг необхідно захищати від несанкціонованого доступу: інформаційні ресурси на всіх видах носіїв, в тому числі, що містять інформацію обмеженого доступу; інформаційні системи і мережі; інформаційні технології і засоби їхнього забезпечення. У предметній частині пошуку одержання і споживання інформації насамперед повинні бути захищені: право на одержання і використання інформації. В предметній частині створення і застосування інформаційних систем, технологій і засобів їхнього забезпечення повинні розроблюватися, виходячи з вимог, що виникають в інших предметних частинах, і насамперед в галузі

інформаційної безпеки, всі засоби технічного, організаційного, правового і програмного захисту. При цьому повинні захищатися: машинні носії з інформацією; бази даних (знань) в складі автоматизованих інформаційних мереж і їхніх мереж; програмні засоби в складі ЕОМ, їхніх мереж.

information security monitoring – моніторинг інформаційної безпеки # безперервне і послідовне слідкування за станом загроз, зв'язаних з можливим розв'язанням війни інформаційної, з постійною і тверезою оцінкою можливості протидії, нейтралізації і запобіганню цих загроз. Моніторинг інформаційної безпеки повинен охоплювати: динаміку зовнішньополітичної ситуації, глобальні і локальні протиріччя і конфлікти; науково-технічний прогрес в галузі розробки засобів і методів проникнення в ресурси інформаційні і впливи на інфраструктуру інформаційну, а також в галузі захисту інформації; стан внутрішнього і міжнародного законодавчо-правового забезпечення безпеки інформаційної; стан і ефективність систем забезпечення інформаційної безпеки.

information security object – об'єкт інформаційної безпеки # свідомість, психіка людей; системи інформаційні різного масштабу і різного призначення.

information security policy – політика безпеки інформації # сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації і спрямовані на захист інформації від певних загроз. В автоматизованих системах політика безпеки інформації є частиною загальної політики безпеки організації і може включати, зокрема, положення державної політики у галузі захисту інформації. Для кожної автоматизованої системи політика безпеки інформації може бути індивідуальною і може залежати від технології оброблення інформації, що реалізується, особливостей системи обчислювальної, середовища фізичного і від багатьох інших факторів. Політика безпеки інформації повинна визначати ресурси автоматизованої системи, що потребують захисту, зокрема встановлювати категорії інформації, що оброблюється в системі. Мають бути сформульовані основні загрози для обчислювальної системи, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Складовими частинами загальної політики безпеки інформації в автоматизованій системі мають бути політики забезпечення конфіденційності, цілісності і доступності інформації, що оброблюється. Відповідальність персоналу за виконання положень політики безпеки інформації має бути персоніфікована. Частина політики безпеки інформації, яка

регламентує правила доступу користувачів і процесів системи комп'ютерної, складає правила розмежування доступу.

information security principle – принцип захисту інформації # принцип технічного захисту інформації, що визначає загальні вимоги до способів і засобів захисту інформації щодо прогнозування дій зловмисника, розроблення і реалізації випереджаючих заходів захисту.

information security providing method – метод забезпечення інформаційної безпеки # сукупність форм і способів, що утворюють інструмент, за допомогою якого спеціальні органи забезпечення безпеки інформаційної вирішують весь комплекс завдань з захисту життєво важливих інтересів особистості, суспільства і держави. Вони повинні мати чітке юридичне оформлення при розробці нормативних актів, що регулюють діяльність органів інформаційної безпеки. Застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. В першому випадку забезпечення інформаційної безпеки, як правило, здійснюється у формі патронату інформаційного та кооперації інформаційної, а в другому – в формі боротьби інформаційної.

information security subject – суб'єкт інформаційної безпеки # держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню безпеки інформаційної у відповідності до законодавства.

information security system effectiveness criterion – критерій ефективності системи захисту інформації # кількісна міра для порівняння варіантів системи захисту інформації. Критерій може бути у вигляді одного показника, який враховує основні характеристики системи, або являти собою сукупність часткових показників. Єдиний загальний критерій ефективності називають глобальним коефіцієнтом ефективності системи захисту інформації.

information security system effectiveness global criterion – глобальний критерій ефективності системи захисту інформації # кількісна міра у вигляді одного показника для вибору раціонального варіанта системи захисту інформації, що забезпечує досягнення поставлених цілей, вирішує поставлені задачі при повному наборі вхідних впливів із врахуванням обмежень. Найчастіше застосовують критерій у вигляді відношення ефективність/вартість. Під ефективністю розуміють ступінь виконання системою завдань, під вартістю – витрати на захист.

information security system protection criterion – показник ефективності

системи захисту інформації # див. information security system effectiveness criterion.

information security theory – теорія забезпечення безпеки інформації # наукова дисципліна, яка з єдиних системних позицій вивчає методи попередження випадкового або навмисного розкриття, спотворення інформації, що зберігається, обробляється або передається в системах керування, що функціонують із застосуванням засобів техніки обчислювальної або мереж обміну інформацією. Вона об'єднує основні положення теорії алгоритмів, теорії інформації, теорії кодування, криптології і т.ін. .

information security threat – загроза інформаційній безпеці # сукупність умов і факторів, що створюють небезпеку інтересам життєво важливим особистості, суспільства і держави в інформаційній сфері. Основні загрозі інформаційній безпеці можна розділити на три групи: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання); загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.).

information security threat criterion – показник загрози безпеці інформації # показник, що характеризує розмір шкоди в результаті проникнення зловмисника до джерела інформації, що підлягає захисту, або її витоку по технічному каналу і визначається для кожного шляху і каналу витоку у вигляді добутку ймовірності реалізації даного шляху або каналу на ціну відповідного елемента інформації.

information sharing community – спільнота користування інформацією # група організацій, які домовилися про спільне користування інформацією. Організацією може бути індивідуальна особа.

information signal – інформативний сигнал # фізичні поля та/або хімічні речовини, що містять інформацію з обмеженим доступом.

information society sign – ознака інформаційного суспільства # найбільш характерні ознаки, за якими будь-яке суспільство можна визначити як інформаційне: комп'ютер персональний, приєднаний до мереж інформаційних транскордонних, стає засобом повсякденного використання; виникають нові форми і види діяльності в інформаційних мережах: робота і торгівля в мережах,

відпочинок в мережах, творчість і розваги в мережах, виховання і освіта в мережах, медицина в мережах і т. ін.; кожний член суспільства має можливість своєчасно і оперативно одержувати за допомогою транскордонних інформаційних мереж повну і достовірну інформацію будь-якого виду і призначення з будь-якої держави, знаходячись при цьому практично в будь-якій точці географічного простору; надається унікальна можливість оперативної, практично миттєвої, комунікації кожного члена суспільства як з кожним (і кожного із усіма разом), так і певних груп населення з державними і суспільними структурами поза залежністю від місця проживання на Земній кулі; трансформується діяльність засобів масової інформації за формами створення і розповсюдження інформації, розвивається та інтегрується з інформаційними мережами цифрове телебачення; формується нове середовище – мультимедіа, в якому поряд із "комп'ютерною" розповсюджується також інформація з традиційних ЗМІ; зникають географічні і геополітичні кордони держави в межах інформаційних мереж.

information society theory – теорія інформаційного суспільства # наукова дисципліна, що вивчає об'єктивні основи і загальні закономірності становлення суспільства інформаційного, вплив технологій інформаційних і телекомунікаційних на різноманітні сфери життєдіяльності суспільства та роль державної політики в процесі переходу до інформаційного суспільства. Завданнями теорії інформаційного суспільства є: формулювання базових понять, що характеризують інформаційне суспільство; виявлення основних положень концепції інформаційного суспільства як типу суспільства, що виникло еволюційним шляхом з постіндустріальних суспільств; вивчення загальних закономірностей становлення інформаційного суспільства; визначення економічних, правових, соціально-культурних, технологічних основ інформаційного суспільства й піддавання їх філософсько-методологічному аналізові; виявлення методологічних принципів державної політики з формування інформаційного суспільства в державі та світі.

information source – джерело інформації # суб'єкти і об'єкти, від яких інформація (дані і відомості) може поступати до несанкціонованого одержувача (зловмисника). Цінність такої інформації визначають інформативністю джерела інформації. Основними джерелом інформації є наступні: люди; документи; продукція; вимірювальні датчики; інтелектуальні засоби оброблення інформації; чернетки і

відходи виробництва; матеріали і технологічне обладнання.

information strategy – інформаційна стратегія # сукупність принципів і методів, які використовуються державою при управлінні ресурсами інформаційними.

information structuring – структурування інформації # класифікація інформації у відповідності до структури, функцій і завдань організації з прив'язкою елементів інформації до її джерел. Деталізацію інформації доцільно проводити до рівня, на якому елементові інформації відповідає одне джерело. Вихідними даними для структурування інформації, що потребує захисту, є перелік відомостей, що складають державну, відомчу або комерційну таємницю, та перелік джерел інформації в організації. Результати структурування інформації оформляють у вигляді схеми класифікації інформації та таблиці, розробленої на основі схеми класифікації інформації.

information struggle – інформаційна боротьба *#1.* боротьба з використанням спеціальних способів і засобів для впливу на сферу інформаційну (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в інтересах досягнення поставленої мети. Інформаційна боротьба може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно, як в мирний, так і у воєнний час. Масштаби інформаційної боротьби настільки великі, що її підготовка і ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби # *2.* форма забезпечення інформаційної безпеки від загроз інформаційних навмисних. Ведеться державними органами інформаційної безпеки з формуваннями, що мають різноманітний (суспільний) стан (фізичні особи, юридичні особи, суб'єкти міжнародного права) і зловмисно створюють інформаційні загрози життєво важливим інтересам особистості, суспільства і держави. Інформаційна боротьба охоплює комплекс заходів забезпечення інформаційного, захисту інформаційного і протидії інформаційної, що здійснюються за єдиним замислом і планом з метою захоплення і утримання переваги інформаційної.

information struggle category – категорія інформаційної боротьби # категорії, що відображають найбільш загальні, суттєві предмети, процеси і властивості інформаційної боротьби. Розрізняють загальні і часткові категорії. Загальні мають відношення до всіх галузей теорії інформаційної боротьби. Головні з них «інформація» і «боротьба інформаційна». Часткові формують у складових частинах теорії. Так,

теорія захисту інформації має свої категорії, наприклад, «захист інформації» і «безпека інформаційна», теорія ураження інформації — свої, наприклад, «ураження інформації».

information struggle effectiveness criterion – критерій ефективності інформаційної боротьби # кількісна міра відображення ступеня переваги інформаційної однієї з протиборчих сторін. Визначають співвідношенням інформованості протиборчих сторін. Числове значення критерія ефективності інформаційної боротьби визначають за формулою: *F = K1/K2*. В чисельникові формули – показник інформованості першої, а в знаменникові – другої конфронтуючої сторони. Перевага першої сторони над другою досягають у випадку, якщо *F > 1*.

information struggle effectiveness evaluating – оцінювання ефективності інформаційної боротьби # визначення ступеня відповідності результатів боротьби інформаційної її меті (цілі). Стосовно до збройної боротьби можна виділити два рівні оцінювання ефективності інформаційної боротьби – оцінювання ефективності інформаційної боротьби у війнах і збройних конфліктах в цілому і оцінювання ефективності інформаційної боротьби в операціях (бойових діях) та розділити її (на кожному рівні) на дві частини: загальну оцінку ефективності власне інформаційної боротьби (як самостійного виду боротьби) і спеціальну оцінку дій, в інтересах яких ведеться інформаційна боротьба. Методологія оцінки ефективності інформаційної боротьби відіграє важливу роль в розвитку теорії інформаційної боротьби.

information struggle effectiveness evaluating methodology – методологія оцінювання ефективності інформаційної боротьби # одна з ключових проблем розвитку теорії інформаційної боротьби, вирішення якої надає теорії необхідну фундаментальність і відносну завершеність. Стосовно до боротьби збройної в методології оцінювання ефективності інформаційної боротьби можна виділити два основних рівні. Перший (вищий) рівень охоплює методологію оцінювання ефективності інформаційної боротьби у війнах і збройних конфліктах в цілому, другий – окремі методології оцінювання ефективності інформаційної боротьби в операціях (бойових діях). Крім того, методологія (на кожному з рівнів) має загальну і спеціальну частини. Загальний рівень призначений для оцінки ефективності власне інформаційної боротьби (як самостійного виду боротьби), спеціальний – для оцінки ефективності дій, в інтересах яких ведеться інформаційна боротьба. До загальної частини методології повинні входити метод і методика

оцінки ефективності інформаційної боротьби, а також показники і критерії її ефективності. На основі використання загальної частини методології можна вирішити ряд взаємозв'язаних завдань оцінки ефективності інформаційної боротьби, зокрема, таких як: оцінка ступеня інформованості органу керування за заданою сукупністю відомостей про обстановку і даних поточної інформації про значення ознак, що розкривають ці відомості; обґрунтування вимог до джерел первинної інформації (ознакової) в інтересах подальшого підвищення якості інформованості органу керування про задану сукупність відомостей; обґрунтування вимог до ступеня блокування і модифікації поточної ознакової інформації при розробці заходів протидії інформаційної; відбір найбільш інформативних ознак для розкривання відомостей кадастру інформаційного; оптимізація часового циклу оновлення поточної інформації і т. ін.

information struggle effectiveness evaluating methods – методика оцінювання ефективності інформаційної боротьби # методика, яка охоплює ряд взаємозв'язаних етапів оцінки ефективності інформаційної боротьби: формування кадастру інформаційного органів керування протиборчих сторін; оцінку характеристик інформації про обстановку, що поступає в органи керування, її селекцію і класифікацію; порівняльну оцінку величини показника інформованості органів керування своїми силами і засобами і силами і засобами противника.

information struggle object – мета інформаційної боротьби # забезпечення необхідного ступеня власної безпеки інформаційної і максимальне пониження рівня інформаційної безпеки конфронтуючої сторони. Досягнення мети інформаційної боротьби здійснюють шляхом вирішення ряду завдань, основними з яких є ураження об'єктів сфери інформаційної конфронтуючої сторони і захист власної інформації. Мета і завдання інформаційної боротьби визначають її зміст, а також і структуру теорії інформаційної боротьби. При цьому на зміст інформаційної боротьби великий вплив здійснює ряд факторів, серед яких виділяють політичний, економічний, духовний, власне воєнний і інформаційний фактори.

information struggle theory – теорія інформаційної боротьби # система знань про характер, закони, закономірності, принципи, форми, способи підготовки і ведення боротьби інформаційної. Структуру теорії інформаційної боротьби визначають мета і завдання інформаційної боротьби, згідно яких вона може включати основи теорії інформаційної боротьби загальні, теорію ураження інформації і теорію захисту інформації.

information support documentation – документація інформаційного забезпечення # частина документації проектної, яка містить рішення з інформаційної бази, системи класифікації і кодування та технологічного процесу оброблення інформації.

information system – інформаційна система # прикладна система, сервіси, засоби інформаційних технологій або інші компоненти для оброблення інформації.

information system security – безпека інформаційної системи # стан системи інформаційної, при якому забезпечують безпеку даних, які знаходяться в ній.

information task – завдання інформаційне # завдання, яке зв'язане із створенням, пошуком, вибіркою даних і внесенням в них змін.

information technology security evaluation criterion – європейські критерії безпеки інформаційних технологій # стандарт інформаційної безпеки, розроблений в країнах Європи (Франція, Німеччина, Нідерланди і Великобританія) у 1991 році. «європейські критерії» розглядають наступні задачі засобів інформаційної безпеки: захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні. Для вирішення проблеми визнання засобів захисту ефективними в критеріях уведене поняття гарантій засобів захисту. Гарантії включають в себе два аспекти: ефективність, що відображає відповідність засобів безпеки завданням, що вирішуються, і коректність, що характеризує процес їхнього розроблення і функціонування. Загальна оцінка рівня безпеки системи охоплює функційну потужність засобів захисту і рівень гарантій реалізації # див. guarantee criterion.

information that constitutes state secrets – розвідувальні відомості # результати спостереження за джерелами (об'єктами) розвідки. В. р. добуваються розвідниками або розвідувальними підрозділами. Збирання розвідувальних відомостей повинно задовольняти наступним основним вимогам: оперативність та цілеспрямованість подання розвідувальних відомостей у відповідності з поставленими розвідувальними завданнями; достовірність та відсутність спотворення розвідувальних відомостей; дублювання збирання найбільш важливих розвідувальних відомостей; можливість надходження розвідувальних відомостей у вигляді оригіналу; оброблення розвідувальних відомостей може бути як складовою частиною процесу добування, так і самостійним процесом перетворення,

узагальнення розвідувальних відомостей, який завершує виконання розвідувальних завдань.

information that is no subject of confidential – відомості, які не підлягають засекречуванню # відомості, засекречення яких здатне спричинити шкоду суспільству, державі і громадянам. До них можуть бути віднесені наступні відомості: про надзвичайні події і катастрофи, що загрожують безпеці і здоров'ю громадян, і їхні наслідки, а також про стихійні лиха, їхні офіційні прогнози і наслідки; про стан екології, охорони здоров'я, санітарії, демографії, освіти, культури, сільського господарства, а також про стан злочинності; про привілеї, компенсації і пільги, що надаються державою громадянам, посадовим особам, підприємствам, закладам і організаціям; про факти порушення прав і свобод людини і громадянина; про розміри золотого запасу і державних валютних резервів держави; про стан здоров'я вищих посадових осіб держави; про факти порушення законності органами державної влади і їхнім посадовими особами.

information theory – інформаційна теорія # математична дисципліна, що вивчає методи аналізу процесів інформаційних, насамперед при вивченні засобів масової інформації. Інформація розглядається як повідомлення, що передається від відправника до одержувача і долає при цьому шуми і завади. Задача зводиться до «зменшення невизначеності», і її рішення пов'язується з точністю й об'єктивністю статистичних методів дослідження, що доводять вимірюваність кількості і якості інформації, незважаючи на форми її виразу – від словесного до образного. В інформаційній теорії застосовуються наступні параметри – щільність, ширина, глибина даних і читабельність, що залежить від надлишку інформації, відкритості чи закритості текстів, їх різноманітності, пов'язаної з мірою невизначеності результатів – ентропією і заданим обсягом потоку інформаційного. Можна, наприклад, вивчати обсяг цього потоку шляхом порівняння швидкості проходження словесних, музичних або візуальних образів в задані відрізки часу по різних каналах зв'язку і в різних країнах.

information threat – інформаційна загроза # 1. вплив з боку дестабілізуючих факторів на стан інформованості, що піддає небезпеці інтереси життєво важливі особистості, суспільства і держави. В результаті впливу інформаційної загрози знижується інформованість особистості, у неї з'являється спотворене уявлення про навколишні явища і процеси. Це у свою чергу відбивається на її поведінці, розвитку, освіченості, вихованні, психіці, здоров'ї, тобто порушує основи існування особистості. Вплив інформаційної загрози на

інформаційне поле суспільної свідомості приводить до пониження загальної культури населення, розвитку бездуховності, розпусти, розповсюдженню am туманних ідей, аморального способу життя і т. ін. В матеріальній сфері інформаційні загрози створюють підстави для шантажу, розкрадання, корупції, монополізму і т.ін. У внутріполітичному житті за їхньою допомогою нескладно інспірувати заворушення, страйки, міжнаціональну ворожнечу і т.ін. В різноманітних сферах державної діяльності вплив з. і. може проявлятися по-своєму. Проте очевидно, що неадекватне сприйняття дійсності особами, що приймають рішення на державному рівні, може призвести до найсерйозніших наслідків # *2.* вхідні дані, призначені для активізації в системі інформаційній алгоритмів, відповідальних за порушення звичного режиму функціонування. Інформаційні загрози можуть бути явними і прихованими.

information threat object – мета інформаційної загрози # активізація алгоритмів, відповідальних за порушення звичного режиму функціонування, тобто за виведення системи інформаційної за межі допустимого стану.

information traffic – інформаційний трафік # 1. див. traffic # 2. в комунікативістиці – термін, що одержав активне застосування в дослідженнях проблем керування і контролю, які виникають в різноманітних інформаційних системах і мережах, а особливо складними стають в супермагістралях інформаційних (наприклад, керування трафіком, контроль трафіка тощо).

information value – цінність інформації # властивість інформації, що визначається її придатністю до практичного використання в різних галузях цілеспрямованої діяльності людини. Розповсюдження інформації та її використання приводить до зміни її цінності і ціни. З часом цінність більшості видів інформації, що циркулює у суспільстві, меншає – інформація старіє.

information war – інформаційна війна # *1.* комплекс заходів і операцій, спрямованих на забезпечення переваги інформаційної по відношенню до потенційного або реального противника. Інформаційну війну можна розглядати в двох аспектах: в широкому розумінні – як форму геополітичного суперництва сторін (протиборство інформаційне) і в більш вузькому значенні – стосовно галузі боротьби збройної (боротьба інформаційна). Інформаційна війна ведеться не тільки в фізичному просторі, де знаходяться фізичні системи інформаційні і засоби, але і в деякій віртуальній зоні (віртуальному або кібернетичному просторі). Інформаційна війна розширює простір ведення війн, який раніше обмежувався великими висотами в атмосфері (стратосфері) і великими

глибинами у Світовому океані. До особливостей в. і. відноситься те, що вона ведеться як під час фактичних бойових дій, так і в мирний час, і в кризових ситуаціях без офіційного оголошення. Початок і. в. неможливо визначити однозначно. В інформаційній війні відсутня лінія фронту; проведення противником операцій в. і. практично неможливо виявити, а якщо факти проведення таких операцій виявляються, вони залишаються анонімними. Які-небудь міжнародні юридичні і моральні норми ведення інформаційної війни відсутні. Та чи інша країна може стати об'єктом інформаційної дії, не знаючи про це. Невисока вартість технічних засобів, які можуть бути використані в інформаційній війні, суттєво розширюють коло можливих її учасників. Ними можуть бути окремі країни та їхні органи розвідки, злочинні, терористичні і наркобізнесові угруповання, комерційні фірми і навіть особи, що діють без злочинних намірів. Усі форми інформаційної війни зводяться до впливу на інфраструктуру інформаційну противника, його системи інформаційні і ресурси інформаційні з проведенням будь-яких дій, що мають за мету спотворення інформації, що одержується ним , позбавлення його можливостей одержання нової інформації або фізичне знищення його інформаційних засобів, а також до захисту інформації власних збройних сил від аналогічних дій противника. Як правило виділяють наступні форми інформаційної війни: боротьба радіоелектронна; війна психологічна; війна з використанням засобів розвідки; війна кібернетична; війна з хакерами # *2.* відкриті та приховані цілеспрямовані впливи інформаційні систем інформаційних одна на одну з метою одержання певного виграшу в матеріальній сфері.

information war operation – операція інформаційної війни # операції, що проводяться спеціально для впливу на потоки інформаційні противника і досягнення переваги інформаційної над противником. Результат бойових операцій залежить від операції інформаційної війни. Війна інформаційна впливає на бойове планування, розгортання збройних сил, припинення бойових дій і перегрупування військових частин. Деякі операції інформаційної війни можуть виходити за межі безпосередніх бойових дій. Це відноситься, наприклад, до формування гром а д- ської думки. У проведенні операцій інформаційної війни важливу роль відіграє розвідка. Вона не обмежується тільки науковими і технічними аспектами при добуванні і аналізі даних розвідувальних. В багатьох випадках такі дані повинні включати відомості біографічного характеру про державних керівників і командування противника,

соціологічні, культурні і економічні фактори, особливо коли війська входять в безпосередній контакт з місцевим населенням в районах їхнього знаходження.

information war strategy – стратегія інформаційної війни # теорія і практика підготовки до війни інформаційної, її планування і ведення. Стратегія інформаційної війни найбільш необхідна збройним силам, коли їм доводиться проводити операції воєнні у середовищі, що відрізняється від звичайного середовища ведення бойових дій. Стратегію інформаційної війни визначають воєнні, політичні і економічні інтереси держави.

information war using intelligence tools – інформаційна війна з використанням засобів розвідки # застосування різноманітних систем і датчиків для спостереження і контролю обстановки на полі бою. Сучасні армії розробляють схеми використання інформації від датчиків у реальному або близькому до реального часі для управління бойовими діями і наведення зброї на цілі. Інформація від датчиків, встановлених безпосередньо в зоні бойових дій, зіставляється і суміщається з відеозображеннями, що отримуються від безпілотних розвідувальних літальних апаратів і літаків та даними розвідки агентурної для формування повної картини бойової обстановки.

information warfare agency – орган інформаційної війни # органи керування інформаційною війною і люди (фахівці, офіцери, підрозділи) для її ведення. До органу інформаційної війни можуть відноситись: органи планування і координації з питань інформаційної війни, які здійснюють розроблення системи планування діяльності з усіх питань, що зв’язані з інформаційною війною; органи стратегічного рівня з відслідковування ознак початку інформаційної війни, які займаються збиранням і аналізом інформації розвідувальної, визначенням ознак початку атак інформаційних; органи проведення операцій із захисту від зброї інформаційної, що здійснюють попередження про інформаційні атаки тактичного рівня і займаються ліквідацією наслідків нападу інформаційного; підрозділи розроблення конструкцій і архітектури автоматизованих систем керування, що здійснюють розроблення єдиної архітектури і технічних стандартів в галузі засобів і систем захисту від інформаційної зброї; групи незалежних експертів, що здійснюють аналіз уразливості автоматизованих систем керування, у тому числі, через здійснення експериментальних атак на автоматизовані системи керування та їхні окремі елементи.

information warfare concept – концепція інформаційної війни # система поглядів на війну інформаційну та шляхи її ведення. За останніми оцінками концепція інформаційної війни повинна

передбачати: заглушення (у воєнний час) елементів інфраструктури державного і воєнного управління (ураження центрів командування і управління); електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (боротьба радіоелектронна); одержання розвідувальної інформації шляхом перехоплення і декодування (дешифрування) інформаційних потоків, що передаються каналами зв'язку, а також побічним випромінюванням і за рахунок спеціально впроваджених в приміщення і технічні засоби електронних пристроїв перехоплення інформації (розвідка радіоелектронна); здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) з наступним їхнім спотворенням, знищенням або викраденням чи порушенням нормального функціонування цих систем (так звана "хакерна війна"); формування і масове розповсюдження інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри і орієнтацію населення і осіб, що приймають рішення (війна психологічна); одержання необхідної інформації шляхом перехоплення і оброблення відкритої інформації, що передається незахищеними каналами зв'язку, циркулюючої в інформаційних системах, а також опублікованої в засобах масової інформації.

information warfare efficiency – ефективність інформаційної війни # ефективність інформаційної боротьби # див. efficiency of information struggle.

information warfare law – закон інформаційної боротьби # закони, що характеризують впорядкованість будови і функціонування, тенденції зміни і розвитку тих чи інших явищ боротьби інформаційної. Закон інформаційної боротьби являють собою більш менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, які існують і діють у інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ведення інформаційної боротьби. Так як сфера інформаційна є частиною соціальної діяльності суспільства, то в ній проявляють себе: загальні закони діалектики; загальні і специфічні закономірності соціального розвитку; власні закони, закономірності війни, інформаційної боротьби (наприклад, закон визначальної ролі політичних цілей війни; закони залежності ходу і кінця війни (інформаційної боротьби) від економічних, соціально-політичних, науково-технічних і воєнних можливостей протиборчих сторін).

Особливістю законів (закономірностей) війни, а також інформаційної боротьби є те, що на відміну від законів і закономірностей природи вони проявляються тільки через діяльність людей.

information weapon – інформаційна зброя # 1. широкий клас засобів і способів впливу інформаційного на противника від дезінформації і пропаганди до засобів боротьби радіоелектронної # 2. сукупність спеціально організованої інформації та технологій інформаційних, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів, систем комп'ютерних та мереж інформаційно-обчислювальних, що застосовується в ході боротьби інформаційної (війни) для досягнення поставлених цілей. За метою використання інформаційної зброї поділяється на зброю інформаційну атаки та зброю інформаційну забезпечення. Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати впливи деструктивні на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням інформаційної зброї атаки. За способом реалізації інформаційну зброю поділяють на три великих класи: зброя інформаційна алгоритмічна (математична); зброя інформаційна програмна; зброя інформаційна апаратна. Інформаційна зброя, що відноситься до різних класів, може застосовуватися спільно, а також деякі види інформаційної зброї можуть мати риси декількох класів. Алгоритм, що реалізує процес керування системою через дані, що поступають в систему і оброблюються нею та та дозволяють здійснювати цілеспрямоване керування одною системою інформаційною в інтересах іншої.

informational environment of automated system – інформаційне середовище автоматизованої системи # уся інформація, що оброблюється в автоматизованій системі. Інформація розташовується на різноманітних носіях даних і характеризується своєю належністю певному власникові, ступенем конфіденційності, і новизни. Оцінкою інформаційного середовища є множина $I = \{i_1, i_2, .., i_n\}$, елементами якої є показники, що характеризують окремі параметри інформаційного середовища автоматизованої системи. Якщо i_i – показник, що характеризує конфіденційність інформації, тоді i_i може приймати значення: "цілком секретна", "секретна", "для службового користування", "відкрита", порушення цілісності,

важливість доступності, відомча належність і т. ін.

informational need – потреба в інформації # дані, необхідні для керування завданнями, цілями, ризиками і проблемами.

informational-analytical activity – інформаційно-аналітична діяльність # сукупність процесів діяльності інформаційної, спрямованих на забезпечення керівництва відомостями, необхідними для прийняття рішень, а також опрацювання концептуальних пропозицій. Інформаційно-аналітична діяльність є основним видом діяльності служб інформаційно-аналітичних.

information-algorithmic weapon – інформаційно-алгоритмічна зброя # вид зброї інформаційної до якого, звичайно, відносять: алгоритми, що використовують сполучення санкціонованих дій для здійснення доступу несанкціонованого до ресурсів інформаційних; алгоритми застосування санкціонованого (легального) програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

informational-mathematical weapon – інформаційно-математична зброя # див. information-algorithmic weapon.

informational-psychological safety – інформаційно-психологікова безпека # стан захищеності психіки людини від деструктивного інформаційного впливу (впровадження деструктивної інформації у свідомість і (або) підсвідомість людини, що приводить до неадекватного сприйняття нею дійсності). Інформаційно-психологікова безпека є складовою частиною безпеки інформаційної і повинна займати особливе місце при її забезпеченні. Цю особливість визначають специфікою загроз і їхніх джерел у галузі інформаційно-психологікова безпека, особливим характером принципів і завдань при реалізації державної політики в цій галузі.

information-computing process – інформаційно-обчислювальний процес # процес функціонування інформаційно-обчислювального комплексу. Охоплює вирішення задач обчислювальних і забезпечення користувача інформацією.

information-computing task – інформаційно-розрахункова задача # задача, яка поєднує інформаційне завдання і розрахункову задачу.

information-exchange grid – мережа обміну інформацією # див. information exchange network.

information-hardware weapon – інформаційно-апаратна зброя # засоби апаратні, призначені для виконання функцій зброї інформаційної. Прикладом з. і .а. можуть бути закладки апаратні, які впроваджуються в ПЕОМ, що готуються на експорт та їхнє периферійне обладнання. Апаратні закладки маскуються під звичайні пристрої мікроелектроніки і застосовуються для збирання,

оброблення й передавання конфіденційної інформації.

information-logical task – інформаційно-логікова задача # задача, яка об'єднує в собі ознаки завдання інформаційного і задачі логічної.

informative feature – інформативність ознаки # показник ознаки, що відповідає значенню ймовірності виявлення об'єкта за цією ознакою. Чим меншій кількості об'єктів належить ознака, тим більш вона інформативна. Найбільш інформативна ознака іменна, що притаманна тільки одному конкретному об'єктові. Інформативність ознак непрямих в загальному випадкові нижча ніж інформативність ознак прямих # наприклад винятки: інформативність чітких відбитків пальців відповідає інформативності іменних ознак.

informatization – інформатизація # організаційний, соціально-економічний і науково-технічний процес створення оптимальних умов для задоволення інформаційних потреб та реалізації прав громадян, органів державної влади, органів місцевого самоврядування, організацій, громадських об'єднань на основі формування та використання інформаційних ресурсів.

informer – інформатор # *1.* фахівець в якій-небудь галузі знань або виробництва, який здійснює діяльність інформаційну # *2.* особа, що постачає інформацію в службу розвідувальну # *3.* система автоматичного інформування користувачів # *4.* компонент пакета програм прикладних, який призначений для видавання повідомлень про хід вирішення задач даним пакетом.

infosecurity – захист інформації # організаційні, програмні та технічні методи і засоби для обмеження доступу до інформації, що обробляється або зберігається. Види інформації, які належить за v хистити, як правило встановлюються законодавством держави. Це можуть бути: відомості, що відносяться до державної таємниці (інформація в галузі воєнної, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності), розповсюдження яких може нанести шкоду безпеці держави; відомості, що відносяться до службової і комерційної таємниці (інформація, що має сьогочасну або потенційну цінність в силу того, що вона невідома третім особам, якщо до неї нема законного доступу на законній (санкціонованій) основі і власник такої інформації вживає заходи до охорони її конфіденційності); відомості, що мають статус персональних даних (інформація про громадян, що входить до складу державних інформаційних ресурсів, інформаційних ресурсів органів місцевого самоуправління, а також та, що одержується і збирається недержавними організаціями і т. ін.).

infosecurity – інформаційний захистя # *1.* захист інтересів життєво важливих фізичних та юридичних осіб від загроз інформаційних. Він досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки # *2.* сукупність заходів захисту від протидії інформаційної противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що розповсюджується і впроваджується в систему управління. Інформаційний захистя досягається проведенням контрольної розвідки, перевіркою інформації, захистом від вогневого ураження (захоплення) елементів систем інформаційних, а також захистом радіоелектронним. Інформаційний захистя підвищує ефективність забезпечення інформаційного в умовах інформаційної протидії противника.

infrared imager – тепловізор # прилад (система) теплобачення, в якому інфрачервоне (теплове) випромінювання від окремих точок об'єкта, що знаходиться в полі огляду, почергово спрямовується оптичною системою (об'єктивом) на світлоелектричний перетворювач, що перетворює його в електричні сигнали, які підсилюються і відображаються на екрані індикатора. Як правило індикатор показує не саму інтенсивність випромінювання, а її зміну відносно деякого середнього рівня. У сучасних тепловізорах для світло-електричного перетворення використовуються лінійки з фото-діодами (60-200 штук), що утворюють лінійку кадру. Розгортка по вертикалі (сканування) здійснюється шляхом механічного гойдання дзеркала, що направляє світлові промені від об'єктива до фотоприймача. Для пониження рівня шумів перетворювача здійснюється його охолодження рідкими газами в спеціальній посудині або спеціальними мікрогабаритними охолоджуючими пристроями, в яких реалізуються принципи термоелектричного охолодження, розширення газу у вакуумі, термодинамічні цикли Стирлінга і т. ін.

infrared imaging – теплобачення # одержання видимого зображення тіл за їхнім тепловим (інфрачервоним) випромінюванням, власним або відбитим. Використовується для визначення форми і місцезнаходження об'єктів, що знаходяться в темряві або в оптично непрозорих середовищах.

infrastructure – інфраструктура # сукупність галузей та видів діяльності, що використовують як виробничу, так і невиробничу сфери економіки (транспорт, зв'язок, комунальне господарство, загальна і професійна освіта, охорона здоров'я і т. ін.).

infringer – порушник # 1. той, хто порушив будь-які правила, закон, звичай # 2. користувач, який здійснює доступ несанкціонований до інформації. В цьому випадку п. одержує доступ до роботи з включеними до складу системи комп’ютерної засобами. Порушників класифікують за рівнем можливостей, що надаються їм штатними засобами системи. Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень містить функціональні можливості попереднього: перший рівень визначає найнижчий рівень можливостей проведення діалогу з комп’ютерною системою – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції оброблення інформації; другий рівень визначається можливістю створення й запуску власних програм із новими функціями оброблення інформації; третій рівень визначається можливістю керування функціонуванням комп’ютерної системи, тобто впливом на базове програмне забезпечення системи на склад і конфігурацію обладнання; четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів системи, аж до включення до її складу власних засобів з новими функціями оброблення інформації. Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про комп’ютерну систему і комплекс засобів захисту.

initial program load – початкове завантажування програми # коротка програма, яка постійно наявна чи її легко завантажити в комп'ютер, і чиє виконання призводить до завантажування в пам'ять більшої програми, такої як операційна система або її завантажувач.

initial secure device identifier – первинний ідентифікатор захищеного пристрою # ідентифікатор захищеного пристрою встановлений на пристрої виробником.

initialization – ініціалізація # встановлення системи або об’єкта у відомий чи визначений стан.

initiator – ініціатор # виклик логічного об'єкта, що видає примітив запиту сервісу рівня, що знаходиться ниижче.

inquiry – опитування # див. polling, questioning.

insecure signal source – джерело небезпечного сигналу # джерело, від якого можуть розповсюджуватися несанкціоновані сигнали з інформацією, що належить захисту. Джерело небезпечного сигналу може виникати випадково (за рахунок побічного випромінювання і наведень) або створюватися зловмисниками. Джерело небезпечного сигналу є радіо і

електротехнічні елементи і пристрої будь-яких радіоелектронних засобів і систем. Існує велика різноманітність таких засобів і систем. За призначенням їх можна розділити на основні засоби і системи (такі, що забезпечують оброблення, зберігання і передачу інформації, яка потребує захисту) і допоміжні засоби та системи (такі, що забезпечують оброблення, зберігання і передачу всієї іншої інформації). За фізичними властивостями засобів джерело небезпечного сигналу можна класифікувати наступним чином: перетворювачі акусто- елекгріічні: випромінювачі низькочастотних сигналів; випромінювачі високочастотних сигналів; паразитні зв'язки і наведення. Джерела функціонального сигналу відносяться до небезпечних у випадку, коли вони цікавлять зловмисника або противника і до них не застосовані заходи безпеки інформації.

installation – інсталяція # встановлення програмного виробу на ЕОМ.

integrated circuit – інтегральна схема # мініатюрна електронна схема, що містить електронні елементи (транзистори, діоди, резистори і т. ін.) і створена на поверхні або всередині напівпровідникового кристала. Розрізняють і. с. малого ступеня інтеграції (МІС), середнього ступеня інтеграції (СІС), схеми інтегральні великі (ВІС) і схеми інтегральні надвеликі (НВІС).

integrated circuit card – інтелектуальна картка # див. smart card, intelligent card, chip-in card.

integrated communication network – інтегральна мережа передавання даних # мережа комунікаційна, що забезпечує на одному і тому ж обладнанні як комутацію пакетів, так і комутацію каналів.

integrity – цілісність # 1. внутрішня єдність, зв'язаність усіх частин чого-небудь, єдине ціле # 2. в обчислювальній техніці – стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи; автоматичне відновлення у випадку виявлення системою потенційної помилки; автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

integrity – цілісність # властивість збереження точності і повноти активів.

intellect – інтелект # див. intelligence.

intellectual counteraction – інтелектуальна протидія # комплекс завдань, що вирішуються в процесі реагування на дії несанкціоновані в інформаційно-обчислювальній мережі на основі оперативного аналізу стратегії противника, зброї інформаційної, що застосовується противником, технічних можливостей ІОМ, поточних завдань боротьби інформаційної і керування корпорацією, в тому числі, і з використанням засобів штучного інтелекту. Інтелектуальна протидія

підпорядкована наступним цілям інформаційної війни в ІОМ: зниження часу безконтрольної присутності противника в інформаційно- обчислювальній мережі; дезінформування противника в інформаційно-обчислювальній мережі; дезорганізація дій противника в інформаційно-обчислювальній мережі; зниження нецільового навантаження на інформаційно-обчислювальну мережу; впливу на ресурси противника.

intellectual objects retrieval – пошук об'єктів розвідки # цілеспрямовані дії сил та засобів органів розвідки, спрямовані на виявлення об'єктів розвідки (джерел і носіїв інформації, джерел сигналів) для одержання від них даних і відомостей. Пошук об'єктів розвідки здійснюють у просторі і часі, а для об'єктів (джерел), що мають носії інформації у вигляді випромінювання і електричного струму, тільки за частотою сигналу.

intellectual property – інтелектуальна власність # належні будь-кому результати літературної, художньої, наукової, технічної та інших видів творчості.

intelligence – відомості # інформація # див. information.

intelligence – інтелект # здатність до мислення, особливо до його вищих теоретичних рівнів. Окремі інтелектуальні здібності людини можуть бути автоматизовані при створені систем штучного інтелекту.

intelligence – розвідка # 1. сукупність процесів добування, оброблення та доведення споживачам інформації, необхідної для прийняття рішень. В залежності від статусу споживача інформації розвідку можна розділити нарозвідку державну (споживачем інформації є державні структури) і розвідку комерційну (споживачем інформації є комерційні структури), а в залежності від переважання людського або технічного фактора у процесах р. – на агентурну і технічну # 2. у військовій справі – сукупність заходів, що проводяться з метою збирання даних про наявного або ймовірного противника, необхідних для оцінки обстановки і прийняття рішення # 3. орган розвідки.

intelligence agency – орган розвідки # спеціалізовані органи, призначені для добування, оброблення і подання необхідної для прийняття рішень інформації будь-яким державним або комерційним структурам, до складу яких вони входять.

intelligence agent – розвідник # особа, яка займається добуванням, вивченням, узагальненням відомостей про діючого або ймовірного противника.

intelligence contact – розвідувальний контакт # безпосереднє спілкування (стикання) розвідника (або його технічного засобу) з джерелом інформації, при якому розвідник безпосередньо або дистанційно може викрасти, знищити або змінити інформацію. Розвідувальний контакт

може здійснюватися за певних умов просторових, енергетичних, часових.

intelligence data – розвідувальні дані # оброблені відомості розвідувальні, що містять висновки про діяльність джерел (об'єктів) розвідки.

intelligence group – агентурна група # розвідувальна група # див. agent group.

intelligence management – розвідувальне адміністративне керування # в багатьох країнах так називаються керівні органи розвідки, призначені для координації розвідувальної діяльності підпорядкованих їм сил і засобів розвідки.

intelligence network – агентура # *1.* сукупність агентів будь-якої установи, підприємства або організації # *2.* мережа агентів, що створюють для збирання секретних відомостей, проведення підривної роботи.

intelligence object – об'єкт розвідки # особа, організація, об'єкт, місцевість або держава, проти яких проводиться операція розвідувальна.

intelligence object detection – виявлення об'єкта розвідки # виділення об'єкта розвідки (джерел і носіїв інформації, джерел сигналів) на фоні інших об'єктів шляхом пошуку за демаскуючими ознаками. Основу процесу виявлення складає процедура ідентифікації – порівняння поточних ознакових структур, що формуються в процесі пошуку, з еталонною ознаковою структурою об'єкта розвідки.

intelligence operation – розвідувальна операція # сукупність дій, заходів, що проводяться органами розвідки для добування, оброблення і подання керівництву інформації, необхідної для прийняття рішень.

intelligence principle – принцип розвідки # принцип добування інформації, що передбачає активні дії всіх елементів системи розвідки при добуванні інформації, насамперед, пошук оригінальних способів і шляхів вирішення завдань стосовно до конкретних умов.

intelligence source – джерело розвідувальних відомостей # суб'єкти і об'єкти, від яких інформація (дані і відомості) може поступати до розвідників або розвідувальних підрозділів.

intelligence task – розвідувальне завдання # питання (проблема) – загальне або конкретне – з якого необхідно одержати відомості розвідувальні.

intelligencer – інформатор # див. informer.

intelligent card – інтелектуальна картка # див. smart card, chip-in card, integrated circuit card.

intelligent network – інтелектуальна мережа # мережа, яка забезпечує гнучкість впровадження нових можливостей та інтелектуальних сервісів, включно з сервісами, створюваними користувачами, шляхом їх компонування з незалежних функціональних блоків.

intentional resistance – навмисна опірність # опірність навіюванню, що

діє на усвідомлюваному рівні психіки: об'єкт впливу свідомо аналізує те, що йому пробують навіяти, зіставляє навіювання зі своїми знаннями, поглядами, переконаннями і т. ін.

interaction – взаємодія # співдія, співдіяння. Взаємний зв'язок між предметами у дії, а також погоджена дія між ким-, чим-небудь.

interactive user – інтерактивний користувач # діалоговий користувач # оперативний користувач # користувач обчислювальної системи, який працює на терміналі в інтерактивному (діалоговому) режимі.

interactive video – інтерактивне відео # інтеграція відео- і комп'ютерної технології. Користувач здійснює вплив на розвиток сюжету.

interception and repeat attack – атака перехоплення та повтору # спроба реалізації загрози системі, заснована на застосуванні реквізитів доступу або інших даних системи захисту, які використовувалися раніше. Найчастіше здійснюють в системах електронної комерції (електронних фінансових системах, системах електронної торгівлі) у разі застосування незахищеної автентифікації простої.

interchange data modelling facility – засіб моделювання обміну даними # засіб моделювання даних, що підтримує обмін даними між системами керування даними.

interchange standard – стандарт обміну # стандарт, який визначає послуги, доступні для інтерфейсу процесу.

interested party – зацікавлені сторони # особа або організація, яка може впливати на прийняття будь-якого рішення чи дії, підпадати під його вплив або відчувати можливість такого впливу

interface – інтерфейс # 1. сукупність засобів і правил, що забезпечують взаємодію пристроїв обчислювальної системи і (або) програм # 2. сукупність уніфікованих технічних і програмних засобів, що використовуються для сполучення пристроїв в обчислювальній системі або сполучення між системами. Межа між двома функціональними пристроями, що визначається їхніми характеристиками, характеристиками з'єднання, сигналів обміну і т. ін.

interference immunity – захист від завад # *1.* в радіоелектроніці – здатність радіоелектронної апаратури зберігати на необхідному рівні показники якості роботи при впливі радіозавад заданого виду (видів) та рівня. Захист забезпечують підвищенням потужності сигналів, що генеруються, використанням антен спрямованої дії (просторовою селекцією), застосуванням інших видів селекції, що базуються на використанні відмінностей між корисними сигналами та завадами (частотною, часовою, амплітудною, поляризаційною і т. ін.), вибором оптимальної структури сигналів та виду модуляції, кодуванням

інформації, що передається, застосуванням статистичних методів приймання та оброблення сигналів і т.ін. Підвищення з. може бути досягнуто також шляхом підвищення обсягу сигналу тобто за рахунок надмірності по тривалості і ширині спектра, або перевищення сигналу над завадою в місці приймання. Критеріями з. може бути величина, обернена до ймовірності спотворення інформації, або коефіцієнт придушення – відношення середньої потужності завади і сигналу на вході радіоприймача, при якому відбувається придушення радіоприймального пристрою. Розрізняють потенційну (тільки при наявності власного шуму радіоприймача) і реальну заваду # *2.* в обчислювальній техніці – здатність ЕОМ зберігати якість функціонування під впливом зовнішніх завад та наявності додаткових засобів захисту від завад, що не відносяться до принципу її дії або побудови.

interior gateway protocol – протокол внутрішнього шлюзу # протокол розподілу маршрутної інформації до маршрутизаторів в автономній системі.

internal code – нутрішній код # код подання даних, прийнятий для окремого пристрою або групи пристроїв ЕОМ.

internal context – внутрішній контекст # внутрішнє середовище, у якому організація намагається досягти своїх цілей. Внутрішні обставини можуть охоплювати: керівництво організації, організаційну структуру, ролі та відповідальності; політики, цілі та стратегії, які потрібні для їх реалізації; можливості в розумінні термінів ресурсів і знань (наприклад, капіталу, часу, персоналу, процесів, систем і технологій); інформаційні системи, інформаційні потоки та процеси прийняття рішень (формальні й неформальні); взаємовідносини з внутрішніми акціонерами, а також їх розуміння та значимість; внутрішня культура організації; стандарти, настанови й моделі, прийняті організацією; і форма та ступінь договірних відносин.

internal information внутрішні інформаційні відносини # відносини інформаційні в межах систем інформаційних.

internal intelligence – внутрішня розвідка # вид розвідки, яка ведеться з метою виявлення і нейтралізації діяльності всередині країни, яка створює, за думкою властей, загрозу безпеці держави. В авторитарних країнах внутрішня розвідка це продовження контррозвідувальної роботи спеціальних служб. При демократії внутрішню розвідку ведуть з метою виявлення фактів порушення громадянських прав.

internal label – внутрішня мітка # мітка, яка записується на носій даних, і надає інформацію про дані, що записано на носій даних.

internal storage – внутрішня пам’ять # private storage.

Internet – Інтернет # *1.* глобальна система взаємопов'язаних мереж у публічному домені # *2.* приватна комп'ютерна мережа, що використовує Інтернет-протоколи і можливість мережного з'єднання для безпечного колективного використання частини інформації організації або операцій її співробітниками

internet architecture board – консультативно-технічна група Інтернету # група у складі товариства Інтернету, яка наглядає за архітектурою і розвитком протоколів Інтернету, створює стандарти, керує серією документів RFC і готує різноманітні періодичні видання. IAB співпрацює також з іншими організаціями, що займаються технічними питаннями і стандартами Інтернету. До складу IAB входять дві основні підпорядковані групи – група інженерів Інтернету робоча і група Інтернету дослідницька.

internet assigned numbers authority – організація з розподілу адрес в Інтернеті # організація, призначена для контролю розподілу в Інтернеті числових параметрів протоколу IP, гарантуючи, що кожний домен одержує унікальне значення. Крім IP-адресів, IANA є центральним реєстром для інших чисел і даних, що мають відношення до Інтернету.

internet control message protocol – протокол керівних повідомлень Інтернет # протокол рівня 2 з протокольного стеку TCP/IP, який забезпечує сповіщення про помилки і надає іншу інформацію, стосовну обробки IP-пакетів.

internet engineering steering group – інженерна керуюча група Інтернету. # див. Internet Engineering Task Force.

internet engineering task force – робоча група інженерів Інтернету # група у складі групи Інтернету консультативної технічної (IAB), яка обновлює існуючі стандарти Інтернету і створює нові. Члени IETF обмінюються матеріалами з дослідницькою групою Інтернету і рекомендують стандарти для групи керування інженерами Інтернету [Internet Engineering Steering Group (IESG)], що співпрацює разом із IAB. IETF розроблює дев'ять напрямків: додатки, міжмережні служби, керування мережами, функціональні вимоги, маршрутизація, безпека, службові додатки, транспорті! і послуги користувачам.

internet message access protocol – протокол доступу до повідомлень Інтернет # протокол, що надає засоби доступу до повідомлень електронної пошти чи дошки оголошень, які зберігаються на поштовому сервері, і дозволяє поштовим програмам користувача звертатися до них, як до локальних, без дійсного переносу повідомлень.

internet network information center – центр мережевої інформації Інтернет # центр, призначений для реєстрації імен доменів Інтернету і керування базою даних цих

internet protocol – протокол Інтернет # протокол міжмережної взаємодії #

IP-протокол # протокол рівня 3 пакетного передавання даних з протокольного стеку TCP/IP, який для міжмережних сервісв без установлення з'єднань підтримує адресування, специфікування типу сервісу, фрагментування й збирання пакетів та захист.

internet reconnaissance – розвідка в Інтернеті # сукупність заходів, спрямованих на використання можливостей і ресурсів Інтернету для виконання завдань розвідувальних. При належному використанні Інтернету можна одержати економний інструмент, який допоможе аналітикам швидко готувати розвідувальні зведення за темами, які раптово стали актуальними. Інтернет є одним з важливих складових нового застосування розвідки по відкритих джерелах, а також може надати велику допомогу у підготовці персоналу розвідувальних служб та відпрацюванні методик виконання задач розвідки.

Internet Research Steering Group – група керування дослідженнями Інтернету # див. Internet Research Task Force.

Internet Research Task Force – дослідницька група для розвитку Інтернету # проблемний підрозділ групи Інтернету консультативної технічної, який займається протоколами, додатками, архітектурою і технологіями Інтернету. Ним керують голова IRTF і група керування дослідженнями Інтернету [Internet Research Steering Group (IRSG)].

interoperability – **1.** функційна сумісність # інтероперабельність # здатність двох або більше функційних модулів спільно обробляти дані і використовувати цю інформацію.

interpretation – **1.** дешифрування зображень # виявлення, розпізнавання або оцінка об'єктів (цілей) за їхніми зображеннями (фотографічному, телевізійному, тепловому, радіолокаційному, голографічному і т. ін.) # **2.** інтерпретація # роз'яснення або розширення вимоги або системи оцінювання.

interrupt – переривання # призупинення процесу, наприклад, виконання комп'ютерної програми, який був викликаний подією, не пов'язаною з цим процесом, і здійснюється таким чином, щоб процес можна було поновити.

interruption – переривання # призупинення процесу, наприклад, виконання комп'ютерної програми, який був викликаний подією, не пов'язаною з цим процесом, і здійснюється таким чином, щоб процес можна було поновити.

inter-segment attack – міжсегментна атака # атака на мережу обміну інформацією віддалена, при здійсненні якої суб'єкт атаки і об'єкт атаки знаходяться в різних сегментах мережі обміну інформацією, що може суттєво перешкодити проведенню заходів з відбиття атаки.

interstate destabilizing factor – міждержавні дестабілізуючі фактори # конфлікти різноманітних масштабів і проявів (економіка, політика, ідеологія, дипломатія і т. ін.).

intrasegment attack – внутрішньосегментна атака # атака на мережу обміну інформацією віддалена, при здійсненні якої суб'єкт атаки і об'єкт атаки знаходяться в одному сегменті мережі обміну інформацією.

intruder – зловмисник # див. abuser, badguy, Bad-Guy.

intrusion – вторгнення # несанкціонований доступ до мережі або до системи, приєднаної до мережі, тобто навмисний або випадковий несанкціонований доступ до інформаційної системи, включаючи зловмисну діяльність проти інформаційної системи або несанкціоноване використання ресурсів в інформаційній системі

intrusion detection – виявлення вторгнень # формальний процес виявлення вторгнень, що зазвичай характеризується збором знань про аномальний характер використання, а також про те, яка уразливість була використана і яким чином, зокрема те, коли і як це сталося

intrusion detection system – система виявлення вторгнень # технічна система, яка використовується для ідентифікації того факту, що була спроба вторгнення, вторгнення відбувається або відбулося, а також для можливого реагування на вторгнення в інформаційні системи і мережі

intrusion prevention – запобігання вторгненням # формальний процес активного реагування з метою запобігання вторгненням

intrusion prevention system – система запобігання вторгнень # варіант систем виявлення вторгнень, які спеціально розробляються для забезпечення можливості активного реагування

inverse code – інверсний код # обернений код # двійковий код для відображення від'ємних чисел у вигляді порозрядного доповнення до найбільшого значення в даній системі подання чисел.

involute cryptosystem – інволютна криптосистема # криптосистема, у якої процедура зашифровування та розшифровування є однаковими. Зрозуміло, що тільки симетричні криптосистеми можуть бути інволютною криптосистемою.

IP – Internet protocol – протокол Інтернет # протокол міжмережної взаємодії # IP-протокол.

IP datagram – деитаграма IP # базова одиниця даних, що пересилаються в мережах Інтернету. Деитаграма IP складається із заголовка і даних, які часто називають корисним навантаженням (payload). Заголовок д. містить адреси відправника і одержувача.

IPL – initial program load – початкове завантажування програми.

IP multimedia subsystem – мультимедійна підсистема IP-мережі

сукупність елементів опорної мережі, використовуваних для доставки потоків даних мультимедійних сервісів через домен з комутацією пакетів.

IP-network – IP-мережа # мережа, що використовує протокол Інтернет в якості транспортного.

IPS – intrusion prevention system – система запобігання вторгнень.

IPSec – правило IPSec # базова концепція забезпечення захисту даних, що передаються на "IP-рівні" мережі Інтернет. Складається з визначення протоколів, які реалізують визначені функції захисту інформації, так званих AH-протоколу та ESP-протоколу, правил їхнього використання, протоколів керування ключами (IKE-протокол), алгоритмів для автентифікації та шифрування. Специфікації IPSec викладені в групі стандартів RFC. Історично IPSec розроблявся для IP-протоколу, який відповідає IPv6, але зараз може застосовуватися і для IPv*4*. RFC 2401 визначає загальні вимоги до базової архітектури захисту даних на IP-рівні. Визначається такий набір функцій захисту інформації: контроль доступу до даних, цілісність, автентифікація джерела даних, контроль повторного використання пакетів, конфіденційність, контроль трафіка. Для протоколів AH та ESP визначаються два способи застосування до IP-пакета: транспорту та тунелювання. В режимі транспорту захисту підлягають тільки сегмент IP-дейтаграми, що відноситься до транспортного рівня, а в режимі тунелювання – весь IP-пакет.

IP-telephony – IP-телефонія # сукупність послуг телефонного зв'язку, підтримувана на основі протоколу IP.

irrecoverable error – невиправна помилка # помилка, для якої неможливе усунення помилки без використання методів або ресурсів, зовнішніх щодо порушеного функційного модуля.

irreducible code – незвідний код # код, в якому комбінації кодові будуються так, що ні одна з них не є початком іншої, більш довгої.

irreversible code – незворотний код # код, при використанні якого неможливо повністю відновити текст, що передається, в його початковому вигляді.

irreversible encipherement – необоротне шифрування # криптографічний процес, що полягає в детермінованому перетворенні даних до такого виду, що вихідні дані відновити неможливо, не дивлячись на точне знання методу шифрування. Такий підхід може використовуватися для захисту кодів паролів, що зберігаються в пам'яті. При цьому пароль, що пред'являється системі, спочатку кодується, а потім порівнюється із закодованим зразком. Таким чином несанкціонований доступ до таблиці паролів не дозволяє отримати доступ до самої системи.

irreversible encipherment – незворотне шифрування # шифрування, яке продукує зашифрований текст, з якого вихідні дані не можуть бути відтворені.

irreversible encryption – незворотне шифрування # необоротне кодування # шифрування, яке продукує зашифрований текст, з якого вихідні дані не можуть бути відтворені.

IRSG – Internet Research Steering Group – група керування дослідженнями Інтернету.

IRTF – Internet Research Task Force – дослідницька група для розвитку Інтернету.

ISMS project – проект СУІБ # структуровані дії, які виконує організація для впровадження СУІБ.

IT security requirements – профіль захисту: вимоги безпеки # розділ профілю захисту, що містить вимоги, яким повинен задовольняти продукт інформаційних технологій для вирішення завдань захисту (типових, спеціальних і т. ін.). В розділі виставляються функціональні вимоги безпеки, вимоги гарантій безпеки, вимоги до середовища експлуатації. Функціональні вимоги повинні містити тільки типові вимоги, передбачені тільки відповідними розділами «загальних критеріїв». Необхідно забезпечити такий рівень деталізації вимог, який дозволяє продемонструвати їхню відповідність завданням захисту. Функціональні вимоги можуть дозволяти або забороняти використання конкретних методів і засобів захисту. Вимоги гарантій містять посилання на типові вимоги рівнів гарантій «загальних критеріїв», проте допускають і визначення додаткових вимог гарантій. Вимоги до середовища експлуатації є необов'язковими і можуть містити функціональні вимоги та вимоги гарантій, яким повинні задовольняти компоненти інформаційних технологій, що складають середовище експлуатації IT-продукту. На відміну від попередніх розділів, використання типових вимог «загальних критеріїв» є бажаними, але не обов'язковими.

item – елемент # див. element.

ITSEC – information technology security evaluation criterion – європейські критерії безпеки інформаційних технологій.

J

jabber – збійний пакет # пересилання станцією пересилання даних поза межами часового інтервалу, дозволеного протоколом.

jabber control – керування збійним пакетом # у локальній мережі, здатність блока доступу до середовища автоматично переривати пересилання, щоб унеможливити надзвичайно довгий потік вихідних даних.

jam signal – сигнал наявності конфлікту # сигнал, який надсилається станцією пересилання даних, щоб проінформувати інші станції даних, що вони не мають передавати # в мережах CSMA/CD, сигнал затору вказує на виникнення

колізії # в мережах CSMA/CA сигнал затору вказує, що представлена станція я даних має намір передавати.

jitter – фазове тремтіння # джитер # короткочасні некумулятивні варіації значущих моментів цифрового сигналу від його ідеальної позиції у часі.

job – завдання # див. assignment, task, mission.

journal – журнал # *1.* періодичне видання, один із засобів масової інформації і пропаганди, що впливає на громадську думку, формуючи її відповідно до інтересів певних суспільних угруповань і політичних партій. Може використовуватися як засіб впливу психологічного друкованими засобами # *2.* в обчислювальній техніці – набір даних (файл), що використовується операційною або іншою системою для збирання і обліку статистичної інформації, різних повідомлень та інших даних.

journalizing – журналізація # процес записування до журналу системного інформації про повідомлення, запити, виконувані програми, використані набори даних і т. ін.

jurisprudence – право # див. law, science of law, right.

K

KDC – key distribute center – центр розподілу ключів.

key – ключ # *1.* ідентифікатор, який є частиною набору елементів даних # *2.* бітовий рядок, що керує операціями шифрування чи дешифрування # див. cryptographic key.

key – ключ # *1.* пристрій для відкривання замка # *2.* сукупність символів, що використовується для ідентифікації елемента множини, наприклад,запису у файлі або запису бази даних (в індексно-послідовному файлі або в базі даних К. є обов'язковим елементом запису) # *3.* сукупність символів, що використовується для підтвердження повноважень на доступ до деякої інформації # *4.* у криптології – сукупність даних, які визначають вибір конкретного перетворення з усієї множини перетворень, які реалізуються шифром # *5.* у прикладній криптології – символ або група символів (або електричний чи механічний прилади, що трактуються як символи), які управляють операціями зашифровування та розшифровування # *6.* послідовність символів (або їхніх електричні чи механічні еквіваленти) в автоматичних чи автоматизованих криптосистемах, які змішуються з відкритим текстом для вироблення шифртексту # *7.* синонім для всього ключового матеріалу або синхропосилок (cryptovariable) # 8. послідовність випадкових чи псевдовипадкових біт, які використовуються для ініціалізації та періодичної зміни операцій в криптографічних пристроях, які використовуються для шифрування, розшифрування, автентифікації

інформації або для генерації інших ключів.

key agreement – погодження ключів # методи встановлення ключа, при яких спільний ключ генерується за деякою процедурою, в якої беруть участь два (або більше) абонентів. Значення ключа залежить від інформації всіх (або принаймні більше одного) абонентів. Властивістю цих методів є неможливість визначення значення ключа одним з абонентів до початку процедури формування спільного ключа.

key block – Блок пам'яті ключів захисту # спеціальний надшвидкодіючий запам'ятовуючий пристрій малої ємності з прямим доступом, призначений для збереження ключів захисту.

key distribute center – центр розподілу ключів # об'єкт системи захисту, який генерує (чи отримує з будь-якого іншого джерела) та розповсюджує ключі електронним або ще будь-яким чином. Якщо для розповсюдження ключів використовується методи захисту інформації криптографічні, то у абонентів системи та ц. р. к. повинні бути відповідні ключі для таємного зв'язку.

key distribution – розповсюдження ключів # процес або протокол, за допомогою якого секретний ключ стає доступним двом або більшому числу законних абонентів, для подальшого його використання в процесі оброблення інформації криптографічного. Існують два методи встановлення ключів – методи перенесення (або транспортування ключів) та методи формування (погодження ключів). Кожний з цих методів може використовуватися при створенні різних схем розповсюдження ключів.

key distribution – розподіл ключів # передача відповідних ключів абонентам системи оброблення секретної інформації.

key documentation – ключова документація # сукупність документів, які містять відомості щодо створення, застосування і знищення ключів.

key escrowed cryptosystem – криптосистема з депонуванням ключів # криптосистема з відновленням ключів, в якій один ключ зберігається у довірених осіб, а інформація про сеансові ключі, за допомогою яких шифруються повідомлення, зашифровується на цьому ключі та передається разом зши- фртекстом. Ці криптосистеми застосовуються в стандарті США Escrowed Encryption Standard (EES).

key establishment – обмінювання ключами # розповсюдження ключів # див. key distribution.

key generation – генерування ключів # процес породження ключів або вибору відповідного ключа з множини усіх можливих ключів.

key hash function – імітовставка # 1. послідовність даних, одержана за певним правилом з відкритих даних та ключа і яка служить для

забезпечення імітозахисту даних # 2. блок інформації фіксованої довжини, що одержується з тексту відкритого і ключа, однозначно відповідний відкритому текстові.

key installation – ввод ключа # інсталяція ключа # установка ключа # процес уведення ключа до криптосистеми.

key management – керування ключами # адміністративне керування ключами # *1.* у криптології — загальна назва для операцій, що виконуються над криптографічними ключами на всіх етапах життєвого циклу ключів (передвикористан- ня, використання та поствикористання), тобто для процесів генерації, початкової ініціалізації, інсталяції, розподілу, збереження, контролю використання, зміни, анулювання, архівації та знищення # *2.* сукупність процесів генерації, реєстрації, сертифікації, початкової ініціалізації, розподілу, збереження, використання, зміни, виведення з використання, архівації та знищення ключів. Схеми керування ключами для криптосистем симетричних та асиметричних дещо різняться. Для симетричних криптосистем традиційними є дві схеми: прямий обмін ключами (point-to-point) та обмін через посередника (з використанням центра генерації ключів або центра ретрансляції ключів). Для асиметричних криптосистем традиційними є сертифікатііі схеми або схеми, що базуються на ідентифікаторах (identity-based) керування ключами. Системи керування ключами відкритими для асиметричних криптосистем називають ще інфраструктурою відкритих ключів.

key management – керування ключем # генерація, збереження, розподіл, видалення, архівування і застосування ключів згідно зі стратегією захисту.

key recovery – відновлення ключа # процес одержання ключа арбітром для перетворення потоку зашифрованого тексту в його розшифрований еквівалент.

key recovery cryptosystem – криптосистема з відновленням ключів # криптосистема, в якій разом з ключами, що застосовуються для шифрування повідомлень абонентами, у деякої сторонньої особи (арбітра) присутня додаткова інформація про ці ключі, яка може використовуватися для їхнього відновлення.

key sertification center – центр сертифікації ключів # об’єкт системи захисту, який проводить автентифікацію ключів за допомогою механізму підпису цифрового або будь-яким іншим чином.

key space – простір ключів # ключовий простір # множина всіх можливих ключів.

key translation center – центр передавання ключів # об’єкт системи захисту, якому довірено передавати ключі між абонентами, які мають з ц. п. к. спільний ключ.

key transport – транспортування ключів # методи встановлення ключа, при яких ключ генерується одним з абонентів та передається іншому (іншим).

keyed access – доступ за ключем # ключовий доступ # спосіб доступу, при якому для звернення до запису в базі даних необхідно вказати ключовий атрибут.

key-encryption-key – ключ шифрування інших ключів # ключ, який використовують в пересилання інших ключів або захисту інших ключів, що зберігає інформаційна система.

key-operated lock – механічнй замок # замки, для яких характерна наявність ригеля (засува), сувальд, ключа, корпусу і запірної планки. Механічнй замок поділяються на врізані, накладні і навісні. За механізмом секретності розрізняють безсувальдні, сувальдні, циліндрові і сейфові замки.

kit – комплект # див. set.

know-how – ноу-хау # 1. технічні знання, досвід, секрети виробництва, методи, алгоритми, програмне забезпечення, технології, необхідні для вирішення технічних або інших задач. Термін застосовується до технічної і іншої інформації. Роль ноу-хау росте в умовах ринку. В міжнародній практиці під ноу-хау розуміють договір про передачу технічних знань, досвіду, навичок в формі документації. Як правило, він супроводжується направленням фахівців для налагодження виробничого процесу # 2. науково-технічна інформація про останні досягнення та спеціалізовані видання, що містять якісну інформацію про суспільно-економічне та культурно-політичне життя окремих країн і світу у цілому. Вважається, що така інформація є важливою умовою розвитку суспільства інформаційного, яка забезпечує його головні сфери інтелектуальними ресурсами когнітаріату.

knowledge – знання # *1.* продукт діяльності людей, що являє собою ідеальне відтворення в мовній формі подій і закономірних зв’язків об’єктивного світу. Знання є прямою силою, що дозволяє людині фактично володарювати над світом. Межі цієї влади визначаються рівнем знань. Людина, у свою чергу, обумовлює точність і межі інформації, що міститься в знаннях. Мірою сили з. є кількість інформації, що міститься в знаннях. З цього погляду з. може розглядатися як зброя інформаційна у відносинах суперництва # *2.* вид інформації (подібно до програм і даних), що зберігається в базах знань і відображає знання людини фахівця (експерта) в певній предметній частині; множина всіх поточних ситуацій в об’єктах даного типу і способи переходу від одного опису об’єкта до іншого. Для з. характерні внутрішня інтерпретованість, структурованість, зв’язність і активність. Говорячи образно:

“знання = факти + переконання + правила”.

knowledge acquisition – збирання знань # одержання інформації про частину предметну від фахівців- експертів і подання її в формі, необхідній для введення в ЕОМ.

knowledge base – база. знань # семантична модель, призначена для подання в ЕОМ знань, накопичених людиною в певній частині предметній. Є основною складовою частиною інтелектуальних, як правило, систем експертних. Для подання знань застосовують ряд моделей, таких як мережа семантична, фреймова, продукційна та інші моделі.

known plaintext attack – криптоаналітична атака з відомим відкритим текстом # криптоаналітична атака , при якій криптоаналітикові відомі деякі випадкові пари відкритого тексту та відповідного йому шифртексту. Завданням крипто аналітика є визначення ключа або отримання ефективного алгоритму для дешифрування деяких інших шифр текстів # наприклад метод імовірних слів, який охоплює визначення шифртексту, відповідного до слів, які часто зустрічаються в повідомленні (наприклад, слова “секретно”). Більш універсальною атакою цього класу є метод лінійного крипто аналізу.

known-plaintext attack – атака з відомим відкритим текстом # аналітична атака, за якої криптоаналізатор має значну кількість відповідного відкритого тексту та зашифрованого тексту.

KTC – key translation center – центр передавання ключів.

L

label – **1.** гриф # нанесений на носій інформації умовний знак корисності інформації, що міститься на ньому # див. confidentiality classification label, security classification label # **2.** мітка # 1. ідентифікатор, який додається до набору елементів даних # 2. ідентифікатор для розташування в програмі # мітка часто застосовується для позначення оператора # в BASIC число ліній може служити міткою, але не завжди об'єктом пересилання # в Fortran мітка, що складено з п'яти цифр, яка передує оператору, може застосовуватися для посилання на оператора.

LAN – local area network – локальна мережа.

language – мова # 1. сукупність, погоджень і правил, які використовуються для спілкування, відображення і передавання інформації # 2. в техніці обчислювальній – засіб опису даних і алгоритмів вирішення задач.

language information legibility evaluation – оцінювання розбірливості мовної інформації # відношення кількості прийнятих без спотворення одиниць мови (фраз, слів, букв, звуків) до загальної кількості переданих. Зниження вимог

до розбірливості може знижувати надмірність письмової або усної

large scale integration circuit – велика інтегральна схема # мікросхема інтегральна, що містить від декількох сотень до декількох тисяч елементів і компонентів в одному кристалі напівпровідника.

large-scale attack – широкомасштабна атака # див. global attack.

law – закон # право # основи # 1. незалежна ні від чиєї волі, незаперечність, заданість, що склалася в процесі існування даного явища, його зв'язків і відношення з навколишнім світом # 2. постанова державної влади, нормативний акт, прийнятий державною владою; установлені державною владою загальнообов'язкові правила # див. base, basic, ground, foundation, fundament, principle.

layer – рівень # підрозділ архітектури ВВС, який складають з підсистем рангу (N).

layer– рівень # див. level.

leaf – лист # листок (дерева) # вузол, який не має підпорядкованого вузла.

leakage – витік # процес виходу будь-чого з чого-небудь, з-під чогось назовні.

legal extraction of information – легальне добування інформації # одержання даних і відомостей з відкритих джерел інформації.

legal relations object in information sphere – об'єкт правових відносин в інформаційній сфері # інформація документована, ресурси інформаційні, інформаційна продукція, послуги інформаційні, системи інформаційні і їхні мережі, технології інформаційні і засоби їхнього забезпечення.

legend – легенда легенда # вигадана біографія/ім'я, яку співробітник розвідки видає за свою з метою конспірації. Підкріплюється підробленими або чужими документами.

legislation – законодавство # 1. встановлення, видання законів # 2. сукупність усіх законів, що діють у будь-якій державі; юриспруденція.

lens reflector – лінзові відбивачі # радіовідбивачі, що створюються на основі лінз Люнеберга. Лінза являє собою кулю із шарами матеріалів, що мають різноманітні значення діелектричної проникності. При такій конструкції електромагнітні хвилі фокусуються на внутрішній поверхні кулі, покритої металевою радіовідбиваючою плівкою-екраном. Ширина діаграми розсіювання лінзи залежить від розмірів екрануючої поверхні і сягає 140 градусів. Лінзові відбивачі діаметром 60 см і масою 40 кг на довжині хвилі А=10 см має ефективну поверхню розсіювання більшу за 150 м^2, на А=3 см більшу за 1800 м*2*.

level – рівень # 1. ступінь величини, розвитку, значимості будь-чого # 2. шар логічної структури обчислювальної мережі, який описує певний комплекс завдань, що виконуються цією мережею.

level lock – сувальдні замки # замки механічні, що мають ригель,

зблокований з пакетом з 3-6 і більше підпружинених сувальд, змонтованих на одній осі. Сувальди виготовлені у вигляді пластин, що мають з боку сполучення з борідками ключа різні контури. Різноманітні секрети утворюють сувальди, складені разом пакетом. їм відповідають в замку профілі борідки ключа.

level of guarantees – рівень гарантій # див. access level.

level of importance information – рівень важливості інформації # категорія розподілу інформації за її важливістю. Розрізняють наступний розподіл інформації за рівнем важливості: життєво важлива незамінна інформація, наявність якої необхідна для функціонування організації; важлива інформація – інформація, яку можна замінити або відновити, але процес відновлення дуже важкий і зв'язаний з великими затратами; корисна інформація – інформація, яку важко відновити, але організація може ефективно функціювати і без неї; несуттєва інформація – інформація, яка більше не потрібна організації.

level of information security – рівень безпеки інформації # рівень захисту інформації #оцінка ступеня безпеки інформації. Найчастіше визначається співвідношенням між вартістю інформації і витратами на її захист. Рівень безпеки інформації раціональний у випадку, коли забезпечується необхідна безпека інформації і мінімізуються витрати на інформацію, що складаються з витрат на захист інформації та збитків за рахунок попадання інформації до зловмисника і використання її на шкоду власника.

level of risk – рівень ризику # величина ризику, виражена комбінацією наслідків і їх ймовірності.

level of risk – рівень ризику # величина ризику, зазначена в термінах комбінації наслідків та імовірності**.**

level pair – пара рівнів # концепція моделювання, що групує схему з відповідною базою даних. це два суміжні рівні даних. вищий з них завжди містить визначення даних, що зберігаються на нижчому рівні.

license – ліцензія # 1. офіційний документ, який надає дозвіл на право здійснення діяльності в даній галузі. Ліцензування підприємницької діяльності, пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації здійснюється в Україні Державною службою спеціального зв'язку та захисту інформації України # 2. дозвіл на право продажу або надання послуг.

light-sensitive material – світлочутливі матеріали # матеріали, що являють собою тонку желатинову плівку, що містить світлочутливі речовини, на целулоїдній плівці, скляній пластині або цупкому папері. До світлочутливих матеріалів відносять: фото- і кіноплівка, фотопластини,

фотопапір. Характеризуються чутливістю та здатністю роздільною об'єктивною.

likelihood – ймовірність # імовірність # ступінь можливості того, що щось станеться.

limited access information – інформація з обмеженим доступом # інформація, право доступу до якої обмежено встановленими нормами та/або правилами.

line – лінія # 1. елемент зображення # 2. рядок програми, тексту, екрана дисплея # 3. частина ланцюга передавання даних, зовнішня по відношенню до апаратури передавання даних.

line switching – комутування ліній зв'язку # комутування каналів # див. circuit switching.

linear cryptanalysis – лінійний криптоаналіз #метод криптоаналізу, що складається з аналізу лінійного зв'язку між бітами відкритого тексту та бітами відповідного шифртексту. Лінійний криптоаналіз є частковим випадком атаки криптоаналітичної з відомим відкритим текстом та атаки криптоаналітичної лише з відомим шифртекстом.

linear predictive vocoder – вокодер з лінійним передбаченням # вокодери, у яких вхідний мовний сигнал апроксимується кусково-лінійною функцією, кожний поточний відлік якої є лінійною функцією n попередніх відліків. У цих вокодерах мовна інформація передається величиною амплітуди, значеннями коефіцієнта лінійного передбачення, періодом основного тону і рішенням про тон складає 2400 біт/с, але існує можливість зниження її до 800 біт/с і менше з допустимою якістю мови.

linear shift feedback register – лінійний регістр зсуву # пристрій, який обчислює лінійну функцію з лінійним зворотнім зв'язком від «вхідних» даних. Послідовність «вихідних» даних лінійного регістра зсуву є лінійною рекурентною послідовністю. Лінійний регістр зсуву є одним з елементів побудови схем шифрів потокових.

linear transformation – лінійне перетворення # афінне перетворення # affine transformation.

linguistic compatibility – лінгвістична сумісність # вживання однозначності термінів, а також інших мовних засобів, що використовуються в АСОІ, і правил формалізації мови природної, в тому числі методи стискання і розгортання текстів.

link level – канальний рівень # див. channel level.

link-by-link encipherement – лінійне шифрування # поланкове шифрування # шифрування даних, що охоплює ділянку від входу до виходу лінії зв'язку телекомунікаційної системи, характеристики якого не залежать від конкретного користувача лінії зв'язку # див. end-to-end encripherment.

list – список # перелік # відомості # 1. перелік об'єктів # 2. структура даних, яка являє собою логічно зв'язану послідовність записів – елементів

списку # 3. в програмуванні — організація зберігання послідовності даних в пам'яті ЕОМ, яка передбачає послідовне оброблення елементів цієї послідовності, а також динамічну зміну її складу і упорядкування.

liveness – живучість # див. viability.

LMI – layer management interface – інтерфейс керування рівнем.

load – навантаження # в мережах інформаційно-обчислювальних – кількість пакетів даних, що генеруються за одиницю часу усіма джерелами даних і вводяться в мережу для передавання.

local access – локальний доступ доступ за допомогою локального пристрою вводу-виводу ЕОМ.

local area network – локальна мережа # 1) Мережа обчислювальна, яка підтримує в межах певної території один або декілька надшвидкісних каналів передавання цифрової інформації, і надається для короткочасного монопольного використання пристроям, що приєднуються. 2) Обчислювальна мережа, вузли якої розташовані на невеликій відстані один від одного.

local attack – локальна атака # атака на мережу обміну інформацією віддалена, спрямована на окремий сегмент мережі обміну інформацією, а в окремому випадку, на окремий елемент мережі.

local databank – локальний банк даних # банк даних, розташований в одному обчислювальному центрі або в зовнішній пам'яті однієї ЕОМ.

local system environment – середовище локальної системи # абстрактне представлення тієї частини реальної системи, що не має відношення до ВВС. LSE може мати функції, необхідні для взаємозв'язку систем, які не є відкритими.

localised service area – локалізована зона обслуговування # визначена оператором група стільників мережі мобільного зв'язку, не обов'язково суміжних, у яких застосовуються специфічні особливості доступу # наприклад, специфічні сервісии.

locally significant secure device identifiers – локально значимий ідентифікатор захищених пристроїв # ідентифікатор захищеного пристрою що є унікальним і має повноваження в локальному адміністративному домені, в якому використовується пристрій.

location portability – **1.** переносність місцезнаходження # **2.** мобільність місцезнаходження # здатність мережі при зміні місцезнаходження абонента за його запитом реєструвати його номер чи адресу у новому мережному об'єкті (станції тощо) і відповідно переспрямовувати виклики.

location services – сервіс позиціонування # сервіс локалізування # сервіс, пов'язаний з визначенням місцезнаходження абонента.

lock – замок # 1. пристрій для замикання дверей або воріт. Сучасні з. класифікуються наступним чином: механічні, що відкриваються

(закриваються) механічним ключем; механічні кодові; електромеханічні; електронні кодові. Основною характеристикою замка є його стійкість до несанкціонованого відкривання # 2. в обчислювальній техніці – код, структура даних або програма, що використовуються для керування доступом до інформації; операція, що дозволяє тільки одному процесу мати доступ до певного ресурсу.

lock out – захист # 1. прагнення запобігти, убезпечити від несприятливих впливів, втручання # 2. засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні (в тому числі – криптографічні) заходи запобігання несанкціонованому доступові до апаратури, програм і даних.

locked resources – захищені ресурси # ресурси ЕОМ, для яких визначений замок секретності, тобто специфіковане керування доступом.

lockout – блокування # метод розподілу ресурсів, за якого спільні ресурси захищені за допомогою надання доступу лише одному пристрою чи процесові одночасно та блокування інших # наприклад заборона на читання даних під час їх оновлювання.

log – журнал **#** див. journal.

logic bomb – логікова «бомба» # деструктивна логіка, яка спричиняє пошкодження системи опрацювання даних, коли спрацьовує певна умова системи.

logic bomb – логікова бомба # програмна закладка, що здійснює зловмисні дії при виконанні ряду певних логічних умов. Вносять таємно в програмне забезпечення ЕОМ і виконують внаслідок збігу певних обставин або у визначений момент часу з метою спотворення, знищення, модифікування або викрадення даних.

logic trap door – логікова «лазівка» # механізм усередині системи операційної (забезпечення програмного), який дозволяє програмі зловмисника одержати привілейовану функцію або режим роботи (які йому не були дозволені). Логіковими «лазівками» можуть бути різноманітні помилки, що свідомо вводяться зловмисником в програмне забезпечення об’єкта.

logical coding – логічне кодування # процес подання символів алфавіту послідовностями логічних значень.

logical inference – логічний умовиводи # функція систем експертних, яку ще називають вбудованою машиною логічного висновку. Ця машина зіставляє ствердження з фактами бази знань (або бази даних) і намагається генерувати висновок, оснований на узгоджених із твердженням фактах.

logical task – логікова задача # задача обчислювальна, яка вирішується шляхом виконання логічних операцій.

long attack – довготривала атака # віддалена атака на мережу обміну інформацією, що передбачає проведення тривалих за терміном багаторазових атак на об'єкти мережі обміну інформацією, як правило, з використанням різноманітних видів зброї інформаційної.

long-lived key – довгостроковий ключ # див. long-term key.

long-term key – довгостроковий ключ # ключ, криптоперіод якого має відносно велике значення. До довгострокових ключів, звичайно, відносяться майстер-ключі, ключі шифрування ключів, деякі ключові параметри крипто алгоритмів, відкриті ключові параметри схем формування ключів, ключі шифрування даних, які зберігаються в базах даних тощо. Відключ несення ключів до довгострокових здійснюється згідно з принципами керування ключами в системі зв'язку та прийнятої стратегії безпеки в системі автоматизованої.

loop – цикл # див. cycle.

loop assertion – циклічний оператор контролю # *1.* логіковий вираз, який визначає одну чи кілька умов, яких потрібно дотримуватися кожного разу, коли виконується певна частина циклу # *2.* оператор контролю, який має перевірятися протягом виконання циклу.

loop body – тіло циклу # частина циклу, яка виконує основнне призначення циклу.

loophole – лазівка # в обчислювальній техніці – недоробка, помилка в програмному забезпеченні або апаратурі, що дозволяє обійти процеси керування доступом.

loophole – лазівка # помилка в користуванні, пропущенні чи недогляді, який дає змогу обійти чи вимкнути механізми захисту.

loss – втрата # кількісна міра шкоди чи збитків, що випливає з компромісу.

low-frequency compromising source emission – випромінювач небезпечних низькочастотних сигналів # див. low-frequency tell-tale source emission.

low-frequency tell-tale source emission – випромінювач небезпечних низькочастотних сигналів # джерела витоку інформації конфіденційної в звуковому діапазоні частот, що створюються при протіканні струмопроводами радіозасобів (проводами індуктивностей, монтажними і з'єднувальними проводами, доріжками друкованих плат) електричного струму і виникненні при цьому радіовипромінювання. Джерелами небезпечних низькочастотних сигналів можуть бути телефонні апарати, пристрої гучномовного зв'язку, підсилювачі потужності, аудіо- і відеомагнітофони і т. ін.

LSA – localised service area – локалізована зона обслуговування.

LSE – local system environment – середовище локальної системи.

M

MAC – media access control – керування доступом до середовища.

message authentication code – код перевірки достовірності повідомлення # код ідентифікування/аутентифікування повідомлень.

machine code – машинний код # програмний код # див. computer code.

machine intelligence – машинний інтелект # сукупність апаратних і програмних засобів ЕОМ, за допомогою яких забезпечується таке спілкування людини з машиною (інтерфейс), яке за своїм рівнем наближається до спілкування між собою фахівців, що вирішують спільну задачу.

machine medium – машинний носій # носій, інформація з якого може бути введена в ЕОМ без додаткового проміжного перетворення.

machine-readable medium – машинний носій # machine medium.

macro virus – макровіруси # комп'ютерні віруси , написані на мові програмування, що застосовується для написання макросів (наприклад, WordBasic). Макровірус імітує натискання керуючих клавіш для деяких видів програм, які працюють із документами, що приводить до відсиланн документів, відкритих програмою, до випадкових (можливо несанкціонованих) адресатів. Використання макровіруса в якості зброї інформаційної атаки дозволяє вибирати цілком конкретні адресати і функціювати за строго заданою програмою, а також за допомогою зброї інформаційної забезпечення здійснювати транзит інформаційних ресурсів, одержаних несанкціонованим способом. Застосування макровіруса у сполученні з іншими видами інформаційної зброї дозволяє досягнути наступних ефектів: одержання доступу до інформації конфіденційної в мережах обміну інформацією (МОІ); руйнування важливої інформації в МОІ; зниження ефективності роботи користувачів МОІ.

macros – макрос # послідовність команд, що запускається на виконання одним натисканням на клавішу.

magnetic card storage – накопичувач на магнітних картах # нагромаджувач, носієм інформації в якому є магнітні карти.

magnetic disk storage – накопичувач на магнітних дисках # нагромаджувач, носієм інформації в якому є магнітні диски, об'єднані в пакет.

magnetic drum storage – накопичувач на магнітному барабані # нагромаджувач, носієм інформації в якому служить магнітний барабан. Відрізняється високою швидкодією, але малою ємністю.

magnetic insulation – екранування магнітного поля # локалізація і шунтування поля магнітного за допомогою спеціальних екранів. Для ефективного екранування низькочастотних полів застосовуються екрани, виготовлені з феромагнітних матеріалів (пермалою або сталі) з великою відносною

магнітною проникністю. В такому екрані лінії магнітної індукції проходять його стінками, які мають малий магнітний опір порівняно з опором повітря поза екраном. В результаті цього магнітне поле шунтується екраном. Якість екранування залежить від магнітної проникності екрана і опору магнітопроводу, яке буде тим менше, чим товстіший екран і менше у ньому стиків і швів, розташованих поперек напряму ліній магнітної індукції. Екранування високочастотного магнітного поля ґрунтується на використанні явища магнітної індукції, що створює в екрані вихрові струми (струми Фуко). Магнітне поле цих струмів спрямоване назустріч збуджуючому полю, в результаті чого збуджуюче магнітне поле витісняється екраном. Із-за поверхневого ефекту щільність вихрових струмів і напруженість змінного магнітного поля по мірі заглиблення в метал падає по експоненціальному закону. Ефективність е. м. п. залежить від частоти його коливань і від електричних властивостей матеріалу екрана. Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого матеріалу товщиною 0,5-1,5 мм є достатньо ефективним. При е. м. п. заземлення екрана не змінює величини збуджуваних в екрані струмів і не впливає на його ефективність екранування.

magnetic tape storage – накопичувач на магнітній стрічці # нагромаджувач, в якому носієм інформації є магнітна стрічка. Відрізняється великою ємністю, але малою швидкодією.

magneto-optic disk storage – накопичувач на магнітооптичних дисках # нагромаджувач, носієм інформації в якому є диск магнітооптичний.

magnetostrictive material – магнітострикційні матеріали # феромагнітні метали і сплави, а також ферити, що мають добре виражені магнітострикційні властивості (змінюють форму і розміри при намагнічуванні) і застосовуються для виготовлення магнітострикційних аку сто електричних перетворювачів електромагнітної енергії в механічну і і навпаки (випромінювачі акустичних коливань, датчики тиску, фільтри й інші прилади).

magnitude assessment of information security threat – оцінка величини загрози безпеці інформації # для елемента інформації величина загрози може бути визначена у вигляді добутку потенційних збитків від реалізації загрози на ймовірність її реалізації. Так як одержати точні і об’єктивні кількісні значення величини загрози важко, то можлива наближена оцінка при наступних обмеженнях і умовах: максимальні збитки від викрадення інформації відповідають її ціні; в умовах повної невизначеності про наміри зловмисника щодо добування

інформації помилка прогнозу мінімальна, якщо прийняти величину ймовірності реалізації загрози протягом певного періоду часу рівною 0,5. Якщо взяти середнє значення з усіх елементів інформації, то верхня межа загрози становить половину ціни інформації, що підлягає захисту. Очевидно, що з підвищенням ціни інформації стає більшою загроза її безпеці, а це потребує більше ресурсів для захисту цієї інформації.

mail client – поштовий клієнт # програма, яку використовує користувач для написання, читання, прийому, відправлення й інші операції з листами. За допомогою цієї програми користувач підключається і працює з поштовими і News-серверами.

mail fetcher – поштовий клієнт # див. mail client.

mail gateway – поштовий шлюз # шлюз, що забезпечує взаємодію двох чи більше систем електронної пошти, включно з різнотипними. це може потребувати повного приймання повідомлення, транслювання його в інший формат, і передавання іншій системі електронної пошти.

mail server – поштовий сервер # сервер, що розподіляє файли у відповідь на запити, отримані електронною поштою.

main characteristics of psychological warfare objects – основні характеристики об'єктів психологічної війни # характеристики об'єктів психологічного впливу, які підлягають виявленню й врахуванню в війні психологічній: особливості національно-психологічні; особливості індивідуально-особистістні; належність групова; особливості морально-психологічного стану.

main storage – оперативна пам'ять # основна пам'ять # головна пам'ять # 1. програмно адресна пам'ять, швидкодія якої сумірна з швидкодією центрального процесора, призначена для тимчасового зберігання програм і даних. Дані в оперативній пам'яті доступні машинним командам для безпосередніх посилань за адресою або для оброблення # 2. пам'ять оперативна в аспекті її основного призначення: зберігання виконуваних на даний момент програм і оперативно необхідних для цього даних.

maintainability – ремонтопридатність # здатність функційного блока в заданих умовах використання зберігати чи відновлювати стан, в якому він може виконувати необхідну функцію, коли технічне обслуговування виконується в заданих умовах і застосовують заявлені процедури та ресурси.

maintenance – технічне обслуговування # набір заходів, спрямованих на збереження функційного модулю чи його відновлювання до стану, за якого він може виконувати необхідну функцію # технічне обслуговування охоплює такі заходь, як моніторинг,

випробування, вимірювання, заміни, коригування, ремонт, а в деяких випадках і адміністративні дії.

maintenance documentation – експлуатаційна документація # документація конструкторська, яка містить відомості, необхідні для експлуатації виробу (використання за прямим призначенням, з технічного обслуговування, транспортування і зберігання). До експлуатаційної документації відносять технічні описи, інструкції з експлуатації, технічного обслуговування, монтажу, пуску, регулювання і обкатки виробу, формуляри, паспорти, відомості запасного майна і приладдя, відомості експлуатаційних документів і т. ін.

maintenance hook – засіб для технічного обслуговування # лазівка у програмному забезпеченні, що дає змогу легко обслуговувати та розробляти додаткові можливості, які дозволять входити до програми в незвичних точках або без звичайних перевірок.

maintenance panel – панель технічного обслуговування # частина блока обладнання, що його застосовують для взаємодії між пристроєм обладнання та інженером-техніком.

major key – головний ключ # див. master key.

malicious computer virus – зловмисний шкідливий комп'ютерний вірус # вид інформаційної зброї , що відноситься до програм з потенційно небезпечними наслідками. Для шкідливого комп'ютерного вірусу принципове значення мають наступні класифікаційні ознаки: об'єкт впливу (зараження); спосіб зараження об'єкта; принцип маскування; деструктивні можливості. За видом об'єкта зараження шкідливі комп'ютерні віруси поділяють на віруси завантажувальні, віруси файлові, віруси завантажувально-файлові, макровіруси. За способом зараження шкідливі комп'ютерні віруси поділяють на резидентні і нерезидентні. За способом маскування – на вірусі поліморфні, віруси-невидимки (стелс-віруси) та віруси комбіновані. За деструктивними можливостями – на безпечні віруси і і віруси, що виконують деструктивні функції. Особливістю шкідливого комп'ютерного вірусу є його неспрямованість на конкретні програми та властивість самодублювання. Шкідливий комп'ютерний вірус може розмножуватися, впроваджуватися у програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи керування і т. ін.

malicious logic – зловмисно введена логіка # програма, реалізована на апаратному, апаратно-програмному чи програмному забезпеченні, і призначення якої полягає у виконанні деяких неавторизованих або шкідливих дій # наприклад логікова «бомба», троянський кінь, вірус, черв'як.

malicious model – модель зловмисника # модель можливостей, поведінки та способів фізичного проникнення потенційного зловмисника до джерел інформації, що захищається. В умовах відсутності інформації про зловмисника, його кваліфікації, технічної оснащеності для запобігання грубих помилок найкраще переоцінити загрозу, ніж недооцінити, хоча такий підхід може призвести до збільшення витрат на захист.

malware – деструктивне програмне забезпечення # шкідливе програмне забезпечення, спеціально розроблене для ушкодження або руйнування системи за допомогою порушення її конфіденційності, цілісності та/або доступності # прикладами деструктивного програмного засобу є віруси і «троянські коні»

management – адміністративне керування # 1. направлення ходу, руху кого-, чого- небудь # 2. діяльність органів державної влади # 3. великий підрозділ якого-небудь закладу, велика адміністративна установа (наприклад, управління розвідувальне Центральне – координуючий центр товариства розвідувального США) # 4. будь-яка керуюча діяльність. У. має багато видів, форм, характеристик (державне, стратегічне, централізоване, наукове і т. ін.).

management agency – орган керування # 1. орган, призначений для спрямовування діяльності кого-, чого-небудь # 2. складова частина, деталь різних механізмів, пристроїв і т. ін., що виконує певну керуючу функцію # 3. активний діяч інформаційний.

management controls – адміністративний контроль # контроль безпеки (тобто засоби захисту і заходи протидії) інформаційної системи, що зосереджується на керуванні ризиком і керуванні безпекою інформаційної системи.

management domain – домен адміністративного керування # набір систем обмінювання повідомленнями, принаймні один з яких містить агента пересилання повідомлень, яким керує одна організація # домен адміністративного керування може відповідати географічній області # керуюча організація несе особливу відповідальність за адміністрування схеми адресації в цьому наборі систем обмінювання повідомленнями.

management information system – інформаційна система адміністративного керування # система опрацювання інформації, яка підтримує прийняття рішень керівництвом організації.

management of information security system – керування системою захисту інформації # процес, який забезпечує організацію спільної роботи всіх елементів системи захисту інформації та реалізацію виробленої стратегії захисту, а також надає засоби реалізації

організаційно-розпорядчих заходів по захисту інформації у системі обчислювальній.

management system – система керування # набір взаємопов'язаних або взаємодійних елементів організації для визначення політик і цілей, а також процесів для досягнення цих цілей. Система керування може охоплювати одну або кілька дисциплін. Елементи системи охоплюють організаційну структуру, ролі та відповідальності, планування, операції тощо. Сфера застосування системи керування може охоплювати організацію в цілому, специфічні та ідентифіковані функції організації, специфічні та ідентифіковані сектори організації або одну чи більше функцій групи організацій

manager – адміністратор # див. administrator.

manchaster coding – манчестерське кодування # в системах передавання даних – спосіб кодування, за допомогою якого сигнали даних і синхронізуючі сигнали об'єднуються в єдиний послідовний потік.

Manchester encoding – манчестерське кодування # кодування бінарної фази, в якій часовий інтервал, призначений кожному біту, поділяється навпіл переходом, напрям якого визначає значення біта # перехід може відбуватися між двома станами фізичної змінної, такими як напруга, магнітна полярність або інтенсивність світла # якщо фізична змінна є електричною, цей тип кодування залежить від полярності й не містить постійного струму.

mandate – мандат # 1. повноваження, доручення, наказ # 2. документ, що стверджує повноваження даної особи # 3. елемент матриці доступу, що визначає тип доступу певного суб'єкта до певного об'єкта.

mandate of authentication – мандат автентифікації # інформація, яка передається в процесі обміну при сильній автентифікації.

mandatory access control – адміністративне керування доступом # принцип керування доступом, який полягає в тому, що керувати потоками інформації між користувачем і об'єктами дозволено тільки користувачам авторизованим, а звичайні користувачі не мають можливості створити потоки інформації, які могли б призвести до порушення встановлених правил розмежування доступу.

mandatory access control – обов'язкове керування доступом # розмежування доступу суб'єктів до об'єктів, засноване на конфіденційності інформації, що міститься в об'єктах доступу, та офіційному дозволі (допуску) суб'єктів доступу звертатися до інформації такого рівня конфіденційності.

mandatory certification – обов'язкова сертифікація # сертифікація на відповідність вимогам, які віднесені нормативними документами до обов'язкових для виконання.

mandatory confidentiality – адміністративна конфіденційність # послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

mandatory integrity – адміністративна цілісність # послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів керування доступом довірчого.

man-in-the-middle attack – атака методом перехоплення повідомлень і підміни # втручання, завдяки якому зловмисник може читати, додавати і змінювати інформацію, яка передається між двома сторонами без їх відома.

Man-In-The-Middle– атака вставкою # усі повідомлення, що передаються між двома абонентами проходять крізь противника. Таким чином, противник перехоплює всі повідомлення одного абонента та ретранслює їх іншому. При цьому противник може намагатися модифікувати, знищувати перехоплені повідомлення або передавати власні повідомлення. Ця атака наочно демонструє необхідність автентичного передавання відкритих ключів в асиметричних криптосистемах.

manipulation – маніпулювання # 1. здійснення маніпуляції # 2. метод психологічного впливу, спрямований на зміну напрямку активності інших людей, який здійснюється настільки вправно, що залишається не замiченим ними. 3) Процес впливу на суспільну думку і політичну поведінку для спрямування політичної активності в необхідне русло. Мета – підштовхнути маси до схвалення непопулярних рішень та кроків влади.

manipulation detection – виявлення маніпуляцій з даними # процедура, яку застосовують для визначення, чи були дані змінені, випадково чи навмисно.

manual cryptosystem – ручна криптосистема # криптосистема, в якій криптоперетворення відбуваються ручним способом без використання криптообладнання (crypto-equipment) або автоматизованих пристроїв.

marginal check – маргінальний перевірка # випробування, у якому певні режими роботи змінюються щодо їх номінальних значень, щоб виявити несправності чи їх можливість.

marginal test – маргінальний тест # випробування, у якому певні режими роботи змінюються щодо їх номінальних значень, щоб виявити несправності чи їх можливість.

mark – знак # матеріальний предмет (явище, подія), що виступає як представник деякого іншого предмета, властивості або відносин та використовується для придбання, зберігання, перероблення та передавання повідомлень (інформації, знань).

Markoff process – марківський процес # випадковий процес, значення якого в моменти часу, що являють собою

послідовність, яка збільшується, створюють ланцюг Маркова, тобто послідовність випадкових величин, для якої при відомому значенні будь-якої з цих величин сукупність попередніх їй величин не залежить від сукупності наступних за нею величин. Ланцюгом Маркова називають також послідовність випробувань з випадковими виходами, якщо при відомому результаті довільного випробування сукупність результатів попередніх випробувань не залежить від сукупності результатів наступних випробувань.

Markovian process – марківський процес # див. Markoff process.

mask – маска # спеціальна накладка з якимось зображенням.

masking – імітозахист # захист від несанкціонованого модифікування і нав’язування інформації фальшивої.

masking – маскування # 1. метод інформаційного приховування ознак об’єкта спостереження шляхом руйнування його інформаційного портрета # 2. вид оперативного забезпечення протидії інформаційної шляхом приховування правдивої та впровадження в інформаційні мережі противника фальшивої інформації про свої сили, наміри або дії.

masking in optical range – маскування в оптичному діапазоні # сукупність заходів захисту ознак демаскуючих об’єкта, спрямованих на зменшення величини контраст/фон. Використовуються наступні методи маскування: маскування особливостями місцевості; маскування обробленням місцевості; маскування пофарбуванням; маскування штучними масками; маскування повітряними пінами.

masking with artificial mask – маскування штучними масками # маскування за допомогою спеціальних конструкцій — масок оптичних штучних.

masks overlap – маски перекриття # штучні оптичні маски, що охоплюють каркас і маскувальне покриття, які повністю закривають об’єкт. Застосовуються, насамперед, для захисту об’єктів, що перевозяться на відкритих платформах.

masquerade – **1.** маскування # здатність будь-якого логічного об'єкта представлятись у вигляді іншого логічного об'єкта # **2.** нелегальне проникнення # звернення одного об'єкта до іншого об'єкта з метою отримання несанкціонованого доступу.

masquerade attack – маскарад # вид атаки, при якій один об’єкт системи видається за інший. Прикладом такої атаки може бути перехоплення даних процедури автентифікації об’єкта та використання її у подальшому для здійснення незаконної авторизації.

mass media – мас-медіа # засоби масової інформації. Значення терміну свідчить про те, що багато особливостей масових засобів інформаційних зв’язків історично зумовлені розвитком культури і соціальних відносин в умовах

ринкового виробництва на базі індустріального прогресу, які створили об'єктивні передумови для перетворення інформації в предмет купівлі-продажу у формах дешевого й популярного товару, наділеного трьома основними функціями: розважальність, розповсюдження новин про поточні події й рекламування новинок торгівлі та послуг. Завдяки цьому процесу в XX сторіччі преса, радіо, кіно, телебачення та інші інформаційні засоби зв'язку, розраховані на широку аудиторію, органічно сполучаються з різноманітними економічними структурами індустріального розвитку суспільства, що сприяє його успіху і регуляції. Унаслідок електронно-комп'ютерної революції здійснюється концентрація й монополізація інформаційних засобів, які набувають значення рушійних факторів розвитку і культури масової і масового комсьюмеризму в глобальних масштабах. В цьому можна бачити демократизацію суспільних відносин, проте монополізація інформаційних засобів, яка передбачає зосередження інформаційного капіталу в лоні приватного бізнесу, що приносить йому доходи, суперечить суспільній природі інформаційних зв'язків. До сучасних ЗМІ в комунікативістиці відносять – пресу (газети, журнали, книги), радіо, телебачення, кінематограф, звукозаписи, відеозаписи, відеотекс, телетекст рекламні щити і і панелі, домашні відеоцентри, що сполучають телевізійні, телефонні, комп'ютерні та інші лінії зв'язку. Усім цим засобам властиві наступні якості, що об'єднують їх: спрямованість до масової аудиторії, приступність безлічі людей, корпоративний характер виробництва й розповсюдження інформації. Виходячи з цього ЗМІ визначають як форму соціального впливу через інформаційні повідомлення.

master key – головний ключ # майстер-ключ # ключ, що знаходиться на найвищому рівні ієрархії в ієрархічних схемах керування ключами. Застосовується як ключ шифрування ключів, в той час як для його захисту уже не можливо застосовувати методи захисту криптографічні. Звичайно, розповсюджується ручним способом, захищається фізичними або організаційними методами захисту та відноситься до довгострокових ключів.

master password – головний пароль # 1. кореневе слово, що є спільним для певного набору паролів # 2. пароль, призначений для захисту каталогу паролів.

matched keys – сполучені ключі # ключі зашифровування та розшифровування.

material – матеріал # 1. те, з чого що-небудь виготовляють, виробляють, будують тощо # 2. різноманітні відомості, дані, посібники і т. ін., що їх використовують як основу,

джерело для чого-небудь, як доказ чогось.

mathematical compatibility – математична сумісність #можливість використання єдиних математичних методів, моделей і алгоритмів в АСОІ різних рівнів.

mathematical model – математична модель # система математичних залежностей, яка описує структуру або функціонування об'єкта.

mathematical support documentation – документація математичного забезпечення # частина документації проектної, яка містить опис алгоритмів, що застосовуються.

matrix – матриця # сукупність чисел (елементів), розміщених у прямокутній таблиці у вигляді *n* стовпців і m рядків. Якщо *m* = *n*, то матрицю називають квадратною порядку *n*.

MD – management domain – домен адміністративного керування.

MDC – manipulation detection code – код виявлення маніпуляцій.

mean operating time between failures – середнє напрацювання між відмовами # середня тривалість роботи між послідовними відмовами функційного блока за заданих умов.

mean rate accuracy – середня точність вимірювання # допустимий діапазон точності, за винятком похибок, спричинених шумами на вході, які не мають перевищувати заданого порогу, коли пристрій застосовують за нормальних робочих умов.

mean time between failures – середнє напрацювання на відмову # середня тривалість часу між послідовними відмовами функційного блока за заданих умов # середнє напрацювання на відмову може бути отриманий з теоретичної моделі чи із спостережень.

mean time to recovery – середній час відновлювання # для заданого функційного блока – середня тривалість часу, необхідна для відновлювання операцій після відмови.

mean time to restoration – середній час напрацювання до відновлювання # для заданого функційного блока – середня тривалість часу, необхідна для відновлювання операцій після відмови.

meaning industry– зміст індустрії # галузь інформаційної індустрії, до якої відносяться організації, що створюють інтелектуальну власність. Інформацію створюють вчені, інженери, письменники, композитори, художники, фотографи. В цьому їм допомагають видавці, продюсери і організації, які надають первинному змістові «товарний вигляд». Сюди ж входять організації, які самі не створюють нової інформації, але компілюють її, вироблюючи довідники, бази даних, статистичні збірники і т.ін. На частку цих постачальників інформації припадає значна частка прибутків, що одержують в індустрія змісту.

measure – заходи # сукупність дій, засобів для досягнення, здійснення чогось.

measure – міра # показник # змінна величина, значення якої приписують як результат процесу вимірювань. Термін використовують однаково як до базових показників, так і похідних показників та індикаторів # див. criterion.

measurement – вимірювання # процес для визначення значення. У контексті інформаційної безпеки цей процес визначення значення потребує інформації щодо ефективності системи керування інформаційною безпекою та пов’язаних із нею заходів безпеки, використовуючи методики вимірювань, функції вимірювання, аналітичну модель та критерії прийняття рішення.

measurement function – функція вимірювання # алгоритм або виконані обчислення для комбінації двох або більше базових показників або основних заходів.

measurement method – методика вимірювань # логічна послідовність операцій, описана в загальному вигляді, яку застосовують для кількісного визначення атрибута щодо визначеного масштабу. Тип методики вимірювань залежить від природи операцій, які застосовують для кількісного визначення атрибута. Можна зазначити два типи методик: *суб’єктивна*: кількісне визначення на основі судження людини; *об’єктивна*: кількісне визначення на основі цифрових рішень.

measurement result – результати вимірювань # один чи більше індикаторів і відповідна їх інтерпретація, які стосуються інформаційної потреби.

measurement results – результати вимірювання # один або більше показників і пов'язаних з ними інтерпретацій, які служать задоволенню потреби в інформації.

measuring transducer – давач # пристрій, який перетворює фізичну величину в сигнали для оброблення технічними засобами.

mechanical lock – механічнй замок # див. key-operated lock.

mechanism – механізм # сукупність проміжних станів або процесів будь-яких станів.

media – медіа # засоби фізичної підтримки передавання чи зберігання інформації, а також тип подання інформації # наприклад відео, аудіо, текст тощо.

media gateway – медіашлюз # кінцевий пункт пакетної мережі, який пакетизує інформаційні потоки від мережі з комутацією каналів і передає пакетизоване навантаження у пакетну мережу, а також виконує зворотні перетворення для потоків від пакетної мережі до мережі з комутацією каналів.

media gateway control protocol – протокол MEGACO керування медіа шлюзом # протокол, який забезпечує створення, модифікацію і вилучення потоків даних через медіашлюз та контроль їх форматів.

media gateway control protocol – протокол керування медіа шлюзом # протокол контролера медіашлюзів, який забезпечує керування

встановленням з'єднання між кількома інтерфейсами медіа шлюзів.

media gateway controller – контро́лер медіа шлюзів # об'єкт мережі, який виконує функції керування викликами у розподіленій пакетній системі комутації.

media server – медіа сервер # сервер, який накопичує і обробляє медіа-потоки мультимедійних сервісів, тобто синхронізовані потоки інформації різного типу (голос та відео, тощо).

medium – **1.** носій # пристрій, що несе, переміщає будь-що, а також взагалі те, що охоплює, несе в собі будь-що # **2.** середовище # див. environment # **3.** медіа # в однині # див. media.

medium that extend beyond the control zone – носій, що розповсюджуються за межі контрольованої зони # носії інформації, для яких є можливим вихід за межі зони контрольованої. До таких носіїв можна віднести: людей; паперові і машинні носії з документами і публікаціями; продукцію, матеріали, сировину, обладнання, газоподібні, рідинні і тверді відходи, частки радіоактивного випромінювання; акустичні, електричні, магнітні і електромагнітні сигнали і випромінювання, електричний струм, що розповсюджуються проводами електроживлення, телефонної мережі, охоронної і пожежної сигналізації і т.ін. Ці носії можуть містити інформацію семантичну і ознакову, а також речовини демаскуючі. За дальністю розповсюдження вказані носії поділяють на три групи: носії без обмеження відстані (люди, документи, які перевозять або переносять, продукція, відходи та інші матеріальні носії); носії, що розповсюджуються за межі прямої видимості (акустичні хвилі великої потужності, радіохвилі в діапазонах довгих, середніх та коротких хвиль, електричний струм з інформацією в кабелях, світло (через світловоди), рідинні та газоподібні відходи; носії, що розповсюджуються в межах прямої видимості (світло, мова, радіохвилі в ультракороткохвильовому діапазоні, слабкострумові електричні сигнали, радіоактивні промені.

meet-in-the-middle attack – зустрічна криптоаналітична атака # в широкому розумінні – метод оптимізації за пам'яттю та часом процедури прямого перебирання рішень. В частковому – криптоаналітична атака з відомим відкритим текстом на криптосистеми з подвійним шифруванням.

MEGACO – media gateway control protocol – протокол MEGACO керування медіа шлюзом.

memory – пам'ять # 1. здатність до відтворення минулого досвіду, одна з основних властивостей людини, що виражається в здатності довго зберігати інформації про події зовнішнього світу, реакціях організму і багаторазово вводити її у сферу свідомості і поведінки. Виділяють процеси

запам’ятовування, зберігання і відтворення, що включають узнавання і спомин, тобто пригадування # 2. функційна частина ЕОМ, призначена для приймання, зберігання і видавання даних. Розрізняють пам’ять внутрішню (основну, оперативну) і зовнішню.

memory clearing – очищення пам’яті # знищення даних у пам’яті шляхом установлення полів цих даних в заданий або випадковий стан.

memory lock – замок пам’яті # код у дескрипторі сегмента або сторінки віртуальної пам’яті, що використовується для обмеження доступу. При цьому до сегмента можуть звертатися тільки процеси, що мають у своєму дескрипторі відповідний ключ.

memory protection – захист пам’яті # механізм контролю доступу до якої-небудь області пам’яті з урахуванням розроблених звернень. Дозволений режим звернення може бути різним для різних процесів. При розмітці області оперативної пам’яті можуть використовуватися граничні регістри; конкретні зафіксовані ділянки пам’яті можуть контролюватися за допомогою замків; доступ до конкретних слів може контролюватися за допомогою тегів (ознак даних). *З.* п. є одним із багатьох способів управління доступом або використання пам’яті і дозволяє запобігти некоректному втручанню користувача, забезпечити захист системи або виконує відразу обидві функції.

message – повідомлення # 1. те, що повідомляється, звістка, інформація # 2. впорядкована послідовність символів, призначена для передавання інформації # 3. довільна кількість інформації, початок і закінчення якої визначені, призначена для передавання від одного абонента іншому в будь-якій формі, що відповідає виду зв’язку.

message authentication – автентифікування повідомлення # перевірка того, що повідомлення було надіслане передбачуваним ініціатором для передбачуваного отримувача, та що повідомлення не було змінено під час пересилання.

message authentication code – код автентифікації повідомлення # бітовий рядок, який є функцією обох даних (відкритого тексту чи шифрувального тексту) і таємний ключ, що прикріплюються до даних для надання можливості автентифікації даних # функція, яку застосовують для створення коду автентифікації повідомлення, зазвичай є функцією одностороннього опрацювання.

message authentication code – код перевірки достовірності повідомлення # код ідентифікування/аутентифікування повідомлень # результат застосування до повідомлення варіанта хеш-функції з ключем. Найчастіше в ролі такої функції виступає алгоритм DES в режимі зчеплення блоків або алгоритм в режимі вироблення імітовставки.

message identification service – сервіс ідентифікування повідомлень # сервіс, який дає змогу системі пересилання повідомлень надавати агентові користувача унікальну ідентифікацію для кожного повідомлення чи дослідження, що представляється чи доставляється системою # наприклад відмітка часу.

message origin – джерело повідомлень # частина комунікаційної системи, яка породжує повідомлення; пристрій, програма або система, що формує повідомлення.

message switching – комутування повідомлень # комутація, при якій здійснюється приймання повідомлень даних, їхнього накопичення і наступне передавання.

metadata – метадані # дані про дані чи елементи даних, можливо, також їх описи даних, дані про право власності на дані, шляхи доступу, права доступу та мінливість даних.

metaknowledge – метазнання # знання про структуру, використання та керування знаннями # метазнання можуть бути ефективним механізмом контролю в експертних системах та інших системах, базованих на знаннях.

metals detector – металодетектори # металошукачі # засоби виявлення елементів закладок, що реагують на наявність в зоні пошуку електропровідних матеріалів, насамперед, металів, і дозволяють виявляти корпуси або інші металеві деталі закладки.

method – метод # 1. система принципів та способів пізнавально-теоретичної і практичної діяльності # 2. спосіб, прийом або система прийомів для досягнення якої-небудь мети, для виконання певної операції.

method of studying documents – метод вивчення документів # метод вивчення об’єктів психологічної війни на основі використання документів, в тому числі архівних. В мирний час такими документами можуть бути: офіційні державні документи ймовірного противника та інших держав; аналітичні матеріали спеціалізованих науково-дослідних організацій і закладів; архівні джерела; вітчизняна й зарубіжна преса; спеціальна література; передачі радіо й телебачення і т.ін. В бойовій обстановці найважливішими джерелами інформації психологічного характеру є відомості розвідувальні і трофейні документи, матеріали радіоперехоплення і т. ін. Фахівці знаходять в них відомості, які характеризують політичний і морально-психологічний стан військовослужбовців і населення противника, а також дані, необхідні для підготовки пропагандистських і інформаційно-довідкових матеріалів.

methodology – методологія # 1. наука про методи пізнання й перетворення світу # 2. сукупність прийомів дослідження, що їх застосовують в будь-якій науці відповідно до специфіки об’єкту її пізнання.

methods – методика # сукупність взаємозв’язаних способів та

прийомів доцільного проведення будь-якої роботи.

metrology – метрологія # наука про вимірювання з великою точністю. Завданнями метрології є встановлення систем одиниць вимірювання, створення і зберігання основних еталонів цих одиниць і забезпечення перевірки точності практичних вимірювань.

MGCP – media gateway control protocol – протокол керування медіа шлюзом.

MIB – management information base – база інформації керування.

microformat camera – мікроформатні фотографічні апарати # група апаратів фотографічних достатньо простої конструкції, що заряджаються вузькою фотоплівкою шириною 8-16 мм, і призначені для оперативного потайного фотографування об'єктів спостереження або копіювання документів. Ранні мікроформатні фотографічні апарати мають горизонтальне компонування апарата з об'єктивом, втопленим у корпус, який містить дві частини, одна з яких рухома і є одночасно захисним кожухом, важелем зводу і протягу плівки до наступного кадру. Нові моделі мікроформатних фотографічних апаратів мають традиційну форму, найчастіше є півавтоматичними з пружинним приводом, який дозволяє працювати в будь-яких кліматичний умовах, і передбачають можливість дистанційного управління процесом зйомки.

military blockade – воєнна блокада # спосіб воєнних дій, що полягає в ізоляції (порушення зовнішніх зв'язків) ворожої держави, великого угруповання військ, міста, порту та інших об'єктів. Метою воєнної блокади можуть бути: підривання воєнно-економічної могутності, виснаження угруповання противника з наступним його розгромом або примушенням до капітуляції і т. ін. Воєнна блокада може бути повною або частковою, сухопутною, морською, повітряною або змішаною. В залежності від масштабу і змісту завдань, кількості залучених сил та засобів воєнної блокади поділяють на стратегічну і оперативну. Воєнна блокада, що проводиться в тактичному масштабі, називають блокуванням.

military intelligence – воєнна розвідка # добування, збирання та вивчення даних про воєнно-політичну обстановку в окремих країнах та коаліціях держав ймовірного або діючого противника, його збройні сили і воєнно-економічний потенціал, склад, положення, характер дій та наміри угруповань військ (сил), а також про театр воєнних дій; вид забезпечення воєнних дій.

military legislation – воєнне законодавство # сукупність законів та інших нормативно-правових актів, що регулюють відносини у сфері будівництва, життя і діяльності збройних сил.

military security – воєнна безпека # положення, що характеризує можливість забезпечення інтересів безпеки національної засобами збройного насильства. Зовнішній аспект воєнна безпека відображає здатність нації протидіяти або стримувати вплив воєнної сили із-за кордону. Це досягають наявністю сучасних збройних сил, формуванням системи колективної та загальної безпеки, входженням до складу тих чи інших воєнно-політичних союзів. Внутрішній аспект воєнної безпеки зв'язаний з деструктивними проявами гонки озброєнь, мілітаризації суспільної свідомості, збільшенням політичної ролі армії у державі. Відмова від мілітаризації економіки й усіх сфер суспільного життя, деполітизація армії, пріоритет інтересів національної безпеки над інтересами військових ведуть до зміцнення воєнної безпеки держави.

minimum privilege – мінімум привілеїв # обмеження прав доступу об'єкта лише на ті права, які потрібні для виконання дозволених задач.

minimum-distance code – код з мінімальною відстанню # код, в якому перехід від одного допустимого значення до наступного супроводжується мінімальними змінами в комбінації кодовій. Дозволяє виявляти в даних, що передаються, тільки поодинокі помилки.

mirroring – віддзеркалювання # синхронне дублювання даних у комп'ютерній мережі.

misinformation – дезінформація # *1.* свідоме поширення неправильної інформації # *2.* навмисне поширення неправильних відомостей про власні збройні сили і плани воєнних дій, щоб увести в оману противника # *3.* спосіб захисту інформації технічного, що полягає у формуванні свідомо хибної (фальшивої) інформації для виключення несанкціонованого одержання істинної.

misinformation – дезінформування # див. disinformation, deception message.

misinformation by combining true and false signs – дезінформування сполученням істинних і хибних ознак # спосіб дезінформування, заснований на заміні фальшивими ознаками незначної, але найбільш цінної інформації, що відноситься до об'єкта, який потребує захисту, та їхнє використання поряд із рештою істинних ознак.

misleading information – дезінформація # див. misinformation.

mission – завдання # див. assignment, task, job.

mistake – помилка [користувача] # дії людини чи бездіяльність, що може призвести до непередбачуваного результату.

MITM – Man-In-The-Middle – атака вставкою.

mobility with service discontinuity – мобільність з перериванням обслуговування # можливість для

користувача змінювати свою точку доступу до мережі таким чином, що при зміні точки поточний сеанс обміну даними повністю припиняється і потім стартує знову. Мається на увазі, що, як правило, користувач завершує сеанс обміну даними ще до зміни точки доступу.

mode – режим # система правил, заходів, запроваджуваних для досягнення певної мети.

model – модель # матеріальний об'єкт, система математичних залежностей або програма, що імітують структуру або функціонування досліджуваного об'єкта. Основна вимога до моделі – її адекватність об'єкту.

model of threats to information – модель загроз для інформації # формалізований опис методів та засобів здійснення загроз для інформації.

model of threats to information – модель загроз для інформації # формалізований опис методів та засобів здійснення загроз для інформації.

modem – модем # 1. функційний блок (модулятор-демодулятор), який забезпечує модуляцію і демодуляцію сигналів # 2. пристрій, який перетворює цифрові сигнали в аналогову форму й навпаки для передавання їх лініями зв'язку аналогового типу (найчастіше телефонними лініями). Для забезпечення сумісності протоколи роботи м., види перетворень сигналів, швидкості передавання даних стандартизуються рекомендаціями Міжнародної спілки електрозв'язку серії V. Ускладнені м., окрім операцій передавання та прийому, здатні автоматично телефонувати, повторювати виклик або відповідати на нього. Для функціонування м. необхідне програмне забезпечення зв'язку.

modification – модифікація # 1. видозміна, перетворення, поява нових ознак, властивостей; якісно відмінні стани чого-небудь # 2. зміна користувачем або процесом інформації, що міститься в об'єкті.

modification detection – виявлення модифікацій # процедура, що її застосовують для визначення, чи були дані змінені, випадково чи навмисно.

modification detection code – код виявлення модифікацій # бітовий рядок, який є функцією даних до яких він приєднаний, для виявлення маніпуляцій # отримане повідомлення (дані плюс MDC) може потім бути зашифровано для досягнення секретності чи автентифікації даних # функція, яка застосовується для створення MDC, має бути загальнодоступною.

modulation – модуляція # термін, що відображає в широкому розумінні змінювання за заданим законом величин, що характеризують фізичний процес. У радіотехніці м. називають змінювання параметрів високочастотних коливань радіопередавача згідно з інформацією, що передається. В залежності від змінюваного

параметра (наприклад, амплітуди, частоти, фази або параметрів імпульсної послідовності) розрізняють відповідно основні види модуляції: амплітудну, кутову (частотну, фазову) та імпульсну. Частота модулюючого сигналу повинна бути малою порівняно з несучою.

module strength – модульна міцність # спосіб та ступінь, в якій діяльність одного модуля пов'язана з іншими # сильна зв'язаність передбачає широкі зв'язки між діями модуля # види зв'язаності можуть бути класифіковані від сильних до слабких: функційна зв'язаність – інформаційна формаційна зв'язаність – зв'язаність з обмінювання даними – часова зв'язаність – логікова зв'язаність – випадкова зв'язаність # протилежність із спряженням.

modulo-N check – контроль за модулем N # контроль за надмірністю, що ґрунтується на використанні залишку від ділення контрольованих даних, які розглядаються як числа, на N.

money– гроші # металеві та паперові знаки, що є мірою вартості при купівлі й продажу.

monitoring – моніторинг # безперервне слідкування за станом навколишнього середовища і управління ним, своєчасне інформуванням людей про можливе настання несприятливих, критичних або недопустимих ситуацій. Прикладом використання моніторингу є експертні системи, в яких порівнюються результати спостережень за поведінкою об’єкта з критичними точками, критичними властивостями й слабкими місцями.

monitoring – моніторинг # визначення стану системи, процесу або роботи, для визначення стану може бути необхідно перевіряти, контролювати або критично вивчати.

motion detector – детектор руху # див. video-monitoring system motion detector.

move – переміщення # відправлення даних з одного місця зберігання до іншого.

MPLS – multi protocol label switching – багатопротокольна комутація за мітками.

multi protocol label switching – багатопротокольна комутація за мітками # механізм прискорення передавання пакетів транспортною мережею шляхом додавання до пакетів малої за обсягом мітки, яка дозволяє їх комутувати без аналізу всього заголовка, при цьому для потоку пакетів, що передаються певним маршрутом, застосовується спільна мітка.

multicast connection – 1. багатоадресне з’єднання # 2. групове з’єднання # окрмий випадок розподільного з’єднання, у якому забезпечується доставка інформації лише до частини можливих приймачів.

multi-endpoint-connection – багатопунктове з’єднання # з’єднання, що має більше двох кінцевих пунктів.

multifactor authentication – багатофакторна автентифікація #

автентифікація принаймні за двома незалежними факторами автентифікації.

multilevel security – багаторівневий захист # режим захисту при обробленні даних, коли користувачі з різним статусом в частині забезпечення секретності мають обмежені можливості звернення до бази даних, яка містить інформацію з різними грифами секретності.

multimedia service – мультимедійний сервіс # сервіс, у якому виконується обмін інформацією більш ніж одного типу # наприклад відео, дані, звук, графіка, текст, зображення.

multimedia terminal – мультимедійний термінал # термінал, що одночасно підтримує обмін інформацією більш ніж одного типу (відео, голос, дані тощо).

multiple access – множинний доступ # в мережах передавання даних доступ багатьох станцій до широкомовного каналу, що дозволяє усунути змагання шляхом виявлення конфлікту і виконання повторного передавання.

multiple computer complex – багатомашинний обчислювальний комплекс # див. computer complex.

multiplexing – мультиплексування # ущільнення сигналів при передаванні даних для декількох пристроїв по одному каналу. Мультиплексні канали і мультиплексори відіграють велику роль в розвитку сучасних супермагістралей інформаційних.

multipoint tunneling – багатоточкове тунелювання # тунелювання, створене на основі технології мереж віртуальних приватних, яке допускає багато сеансів усередині тунелю.

multipoint-to-multipoint connection – багатопунктно-багатопунктове з'єднання # з'єднання «багато точок – багато точок» # з'єднання групи кінцевих пунктів (джерел) з групою кінцевих пунктів призначення для двобічного асиметричного чи симетричного зв'язку.

multipoint-to-point connection – багатопунктно-пунктове з'єднання # з'єднання «багато точок – точка» # з'єднання багатьох кінцевих пунктів (джрел) з одним кінцевим пунктом (призначенням) для однобічного (збиральне з'єднання) або двобічного симетричного чи асиметричного зв'язку.

multiservice network – мультисервісна мережа # телекомунікаційна мережа, що забезпечує обмін інформаційним навантаженням як в реальному (голос, відео тощо), так і в нереальному часі (дані) на базі єдиної транспортної мультипротокольної платформи.

multiservice service platform – мультисервісна платформа надання послуг # сукупність програмно-апаратних ресурсів мультисервісної мережі, які забезпечують надання сервісів.

multiservice terminal – мультисервісний термінал # термінал, що підтримує два чи більше телекомунікаційних сервісів.

multi-zone information security principle – принцип

багатозональності захисту інформації # принцип технічного захисту інформації, що визначає диференційований доступ санкціонований різноманітних категорій користувачів до джерел інформації і реалізується шляхом розподілу простору, який займає об’єкт захисту, на зони контрольовані.

mutant virus – привид # вірус-мутант # комп’ютерний вірус , здатний до сам о кодування. Вірус-привид містять у собі алгоритми шифрування-розшифрування, які виключають можливість повторення однакових ланцюжків байт вірусного коду у будь-яких двох файлах, інфікованих одним і тим же вірус-привид.

mutual authentication – взаємна автентифікація # автентифікація ідентичності об'єктів, в якій самі об'єкти забезпечують гарантії ідентичності один одного.

mutual suspicion – загальна недовіра # відношення між взаємодіючими об'єктами, за яких жоден об'єкт не залежить від іншого об'єкта для правильного чи безпечно функціювання щодо певної властивості.

mystery – таємниця # див. secrecy, secret.

MIS – m anagement information system – інформаційна система адміністративного керування.

N

name – ім'я # лінгвістична конструкція, що відповідає об'єкту в деяких ділянках міркування.

name qualification – обмеження імені # асоби для посилання на мовні конструкції в рамках частини програми щодо тієї частини ідентифікатора, який оголошений для мовної конструкції в цій частині # наприклад застосовується для посилань на компоненти запису (B OF A в COBOL), члени бібліотеки, мовні конструкції в модулі.

name space – простір імен # множина усіх можливих імен, доступних через службу імен. Простір імен декларує угоди і синтаксис іменування об’єктів.

naming-authority – уповноважений з найменування # уповноважений з реєстрування, що визначає місцезнаходження імен відповідно до конкретних правил. Якщо уповноважений з найменування визначає місце розташування символьних імен, то він відомий як уповноважений символьних імен, а якщо він визначає адресу – то як уповноважений з адресації.

naming-domain – пойменований домен # набір імен, що надаються об'єктам конкретного типу. Якщо імена є символьними, то набір відомий як регіон символьних імен. Якщо імена є адресами, набір відомий як регіон адрес.

naming-subdomain – пойменований субдомен # піднабір пойменованого регіону, що відділений від усіх інших

пойменованих підрегіонів такого пойменованого регіону.

national computer security center – національний центр комп'ютерної безпеки # підрозділ агентства національної безпеки, призначений для підтримки і стимулювання розповсюдження захищених систем в закладах Федерального уряду. Центр також здійснює координацію в галузі аналізу і розробки систем з гарантованим захистом.

national databank – національний банк даних # сукупність взаємозв'язаних масивів даних про територію країни і її адміністративно-територіальний поділ, природні ресурси, виробничо-економічну структуру народного господарства, національне багатство,інфраструктуру, населення і трудові ресурси, а також засоби керування цими масивами. Національний банк даних існує в ряді країн у зв'язку з необхідністю удосконалення інформаційного забезпечення процесів державного планування і управління народним господарством. В широкому розумінні слова він являє собою інформаційно-пошукову систему, яка складається з окремих (галузевих, відомчих, територіальних або цільових), але взаємозв'язаних банків даних, в яких реалізуються: принцип фактографічної системи (національний банк даних має централізовані масиви або банки даних, які безпосередньо забезпечують органи управління укрупненою інформацією); принцип адресної системи (національний банк даних забезпечує можливість звернення за детальною інформацією в локальні банки даних). Національний банк даних забезпечує також єдине і однозначне кодування інформації на основі централізованого введення класифікаторів або систем однозначного кодування.

national information security concept – концепція інформаційної безпеки держави # систематизована сукупність відомостей про безпеку інформаційну держави та шляхи її забезпечення. В концепції проводиться системна класифікація факторів дестабілізуючих і загроз інформаційних безпеці особистості, суспільства і держави; обґрунтовуються основні положення по організації забезпечення інформаційної безпеки держави; розроблюються пропозиції по способах і формах забезпечення інформаційної безпеки. Основу забезпечення інформаційної безпеки держави складають засоби і способи захисту державної таємниці. Для конкретної особистості такими способами і засобами можуть бути: судовий захист прав і свобод у використанні інформації; адміністративний захист її життєво важливих інтересів в інформованості з боку територіальних або відомчих органів інформаційної безпеки; автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої,

сімейної і професійної таємниці. Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом з тим, при наявності у них власних органів інформаційної безпеки суттєво розширюються їхні можливості у сфері автономного захисту.

national security – національна безпека # категорія політичної науки (політології), яка характеризує стан соціальних інститутів, який забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості та суспільства. Національна безпека як категорія політології відображає зв'язок безпеки з нацією. В цьому плані вона характеризує стан нації як цілісної системи, що охоплює суспільні відносини і суспільну свідомість, інститути суспільства, їхня діяльність, які сприяють або шкодять реалізації національних інтересів у конкретній обстановці, що склалася історично. Суть національної безпеки – у протидії і компенсації будь-яких деструктивних заворушень, що формуються всередині суспільства або за його межами, які шкодять потребам життєдіяльності і розвитку суспільства та особистості. В національній безпеці виділяють три рівні безпеки: особистості, суспільства і держави. їхнє місце і роль динамічні та визначаються характером суспільних відносин, політичним устроєм, ступенем внутрішніх та зовнішніх загроз. У критичні для нації періоди може домінувати безпека суспільства або держави. Як правило, авторитарні та тоталітарні режими, які постійно створюють такі критичні умови, висувають на передній план безпеку держави за рахунок безпеки особистості. Для демократичних суспільств найбільш цінні свобода та безпека особистості. Для них безпека держави і суспільства не є самоціллю, а функцією забезпечення свободи і безпеки особистості. В змістовному плані в національній безпеці. розрізняють різноманітні галузі, структурні елементи, до яких, у першу чергу, відносяться: безпека політична, економічна, воєнна, екологічна, інформаційна та безпека культурного розвитку нації.

National Security Agency – агенство національної безпеки # основна служба розвідувальна Сполучених Штатів Америки в галузі радіоелектронної розвідки. АНБ створене в 1952 році в складі міністерства оборони. До його складу входить Центральна служба безпеки (ЦСБ), яка відповідає в США за криптографію й криптоаналіз. Перед ЦСБ стоять два завдання: дешифрування іноземних шифрів і забезпечення безпеки американських телекомунікаційних систем.

national-psychological peculiarities – національно-психологічні особливості # форма прояву психології національної; одна з основних характеристик об'єктів психологічної війни, специфіку якої

необхідно враховувати, для досягнення максимального ефекту впливу психологічного. Об'єкти психологічного впливу (військовослужбовці й населення противника) – це люди, які думають, відчувають, переживають, сприймають сказане у відповідності до закономірностей, притаманних даній етнічній спільності. Якщо способи психологічного впливу на війська й населення противника, зміст і форма подавання агітаційно-пропагандистських матеріалів не відповідають національно-психологічним особливостям об'єкта, то сам вплив може бути або даремним, або приведе до протилежного результату.

natural binary code – натуральний двійковий код # зважений код, комбінації якого одержують при піднесенні числа 2 до степенів із натуральними показниками.

necessary bandwidth – необхідна смуга радіочастот # мінімальна смуга частот певного класу випромінювання, необхідна для передавання повідомлень із заданою якістю.

need-to-know – треба знати # законна вимога потенційного отримувача даних, щоб знати, отримати доступ та володіти будь-якою конфіденційною інформацією, представленою цими даними.

negotiated QoS – узгоджена якість обслуговування # якість обслуговування, встановлена мережею після узгодження кожного атрибуту, отриманого у запиті якості обслуговування, з наявним станом мережних ресурсів.

network – мережа # 1. зв'язковий орієнтований граф # 2. засіб теледоступу — мережа передавання даних, мережа обчислювальна.

network administration – адміністрування мережі # повсякденна експлуатація і адміністрування мережних процесів і засобів, що їх використовує мережа

network analyzer – мережний аналізатор # пристрій або програмне забезпечення, що його використовують для спостереження й аналізу інформаційного мережного трафіка # до проведення аналізу інформаційного потоку інформація повинна бути зібрана певним чином наприклад, за допомогою використання мережного сніферу

network element – мережний елемент # інформаційна система, приєднана до мережі

network level – мережний рівень # третій рівень програмної структури мережі обчислювальної, що здійснює керування маршрутизацією інформації.

network management – **1.** адміністративне керування мережею # функції управління мережею обчислювальною, зв'язані з умиканням і вимиканням системи, каналів передавання даних, терміналів, з діагностикою несправностей, збором статистики, підготовкою звітів і т. ін. # **2.** мережний менеджмент # процес

планування, розроблення, реалізації, експлуатації, моніторингу та підтримки мережі

network mobility – мобільність мережі # здатність мережі, в якій з'єднані один з одним ряд стаціонарних і рухомих вузлів, при своєму переміщенні змінювати пункт приєднання до іншої мережі.

network monitoring – мережний моніторинг # процес постійного спостереження і перевірки даних, які фіксують мережну діяльність і операції, включаючи журнали аудиту і попередження про небезпеку, і пов'язаний з цим аналіз

network portability – переносність мережі # **2.** мобільність мережі # сервіс, що дозволяє абоненту зберігати свій номер в процесі хендовера доступу на іншу мережу (без зміни свого місцезнаходження).

network security – захист обчислювальної мережі # виключення або суттєве утруднення несанкціонованого доступу користувачів до елементів та ресурсів обчислювальної мережі шляхом використання апаратних, програмних і методів криптографічних та засобів захисту, а також проведення організаційних заходів.

network security policy – політика мережної безпеки # сукупність положень, правил і практичних прийомів, що встановлюють підхід організації до використання її мережних ресурсів і визначають, як має забезпечуватися захист її мережної інфраструктури і сервісів.

network sniffer – мережний сніфер # пристрій або програмне забезпечення, які використовують для збирання інформації, що проходить через мережі

network spy – мережний шпигун # комбінований засіб зброї інформаційної, основою якого є черв'як мережний. Основні етапи функціонування ш. м.: інсталяція в пам'яті ПЕОМ, що атакується; очікування запиту з віддаленої атакуючої ПЕОМ і обмін з нею повідомленнями про готовність до атаки; передавання перехопленої інформації на атакуючі ПЕОМ і надання атакуючій ПЕОМ контролю над ПЕОМ, що атакується. Основні функції ш. м.: перехоплення і передавання інформації, що вводиться з клавіатури на атакуючу ПЕОМ (подолання системи захисту інформації, порушення конфіденційності інформації); перехоплення й передавання екранної інформації на атакуючу ПЕОМ (порушення конфіденційності інформації); перехоплення й передавання на атакуючу ПЕОМ інформації про ПЕОМ, що атакується, наприклад, про тип операційної системи, параметри ПЕОМ, програми, що виконуються (ведення розвідки комп'ютерної); передавання контролю над ПЕОМ, що атакується, атакуючому комп'ютерові. Результатом такого передавання можуть бути віддалений

запуск програм, знищення або модифікація інформації та іншівпливи деструктивні.

network worm – мережний черв'як # комп'ютерний вірус , що має властивість самостійного розповсюдження в мережах обміну інформацією та заражає елементи мережі обміну інформацією, функційні сегменти мережі обміну інформацією або мережа обміну інформацією цілком. Основні етапи функціювання мережного черв'яка: пошук в мережа обміну інформацією цілі впливу; передавання по мережі обміну інформацією системи керування автоматизованої свого коду на ПЕОМ, що атакується; одержання керування в системі операційній ПЕОМ, що атакується; перехід до дій за першим етапом. Основною проблемою при функціюванні мережного черв'яка є одержання керування в операційній системі ПЕОМ, що атакується. Для цього необхідно визначити ідентифікатор і пароль абонента або уразливі місця механізмів захисту інформації. Тому мережний черв'як повинен мати спеціальний програмний модуль подолання рубежів захисту (наприклад, перехоплення паролю).

networks convergence – конвергенція мереж # реалізація спільних архітектурних принципів побудови телекомунікаційних мереж, підтримка єдиних сумісних протоколів та інтерфейсів, а також можливостей різних мережних платформ надавати аналогічні види послуг незалежно від типу технологій доступу.

neutralization of threats subsystem – підсистема нейтралізації загроз # частина системи охорони об'єктів, що має у своєму складі функціонально об'єднаних людей і засоби для фізичного і психологічного впливу на зловмисників, що проникли на територію, що охороняється, а також засоби гасіння пожежі.

new generation network – мережа наступного покоління # мультисервісна мережа на базі пакетних систем комутації та широкосмугових транспортних технологій, яка надає користувачам можливість вибору телекомунікаційних сервісів різних операторів і постачальників, забезпечує якість сервісів та їх незалежність від транспортних технологій, підтримує конвергенцію мереж та узагальнену рухомість абонентів.

news agency – агенство новин # організація, що здійснює збирання, оброблення і розповсюдження інформації для газет, журналів, видавництв, радіо і телебачення, державних, науково-культурних та інших закладів. Інша назва – інформаційне агентство. Великі агентства мають власні кореспондентські пункти й передплатників в різних країнах світу, використують для їх обслуговування найновішою

електронно-інформаційною технікою і ефективно діючими системами комерційних служб. В США до числа таких агентств відносять Ассошіейтед Пресс (Associated Press – AP), кооперативне за своєю структурою (засноване у Нью-Йорку в 1848 р.) і приватне за своїм статусом (засноване у 1907 р.) агентство Юнайдет Пресс Інтернейшнл – ЮПІ (Uneted Press International – UPI) із штаб квартирою у Нью-Йорку, Нашвіллі і Далласі. За масштабами своєї діяльності вони є світовими. У Великобританії такими агенством новин є Рейтер (Reuters), у Франції – Агентство Франс Пресс – АФП (Agence France Presse – AFP), у Німеччині Дойче Прессе-Агентур – ДПА (Deutche Presse-Agentur – DPA), в Італії – Адженція Національе Стампа Ассочата – АНСА (Agenzia Nazionale Stampa Associata) – ANSA).

next generation network – мережа наступного покоління # мультисервісна мережа на базі пакетних систем комутації та широкосмугових транспортних технологій, яка надає користувачам можливість вибору телекомунікаційних сервісів різних операторів і постачальників, забезпечує якість сервісів та їх незалежність від транспортних технологій, підтримує конвергенцію мереж та узагальнену рухомість абонентів.

next-bit testing – тестування наступного біту # тестування ансамблю. Ансамбль витримує тестування наступного біту, якщо він є непередбачуваним.

NGN – **1.** next generation network # **2.** new generation network – мережа наступного покоління.

NIDS – network intrusion detection system – система виявлення вторгнень до мережі.

NIST – national institute of standards and technology – національний інститу́т станда́ртів і технології.

node – вузол # *1.* точка в мережі даних, в якій один або декілька функціональних пристроїв об'єднують канали передавання даних або ланцюги даних # *2.* частина пристрою # *3.* в Інтернеті – коротка назва моста, маршрутизатора, комутатора, шлюзу або хоста.

noise – шум # порушення в роботі, яке впливає на сигнал, й може спотворити інформацію, яка передається сигналом.

noise burst signal – сигнал шуму # у шинній мережі з маркерним доступом або в кільцевій мережі з маркерним доступом, сигнал, що вказує на те, що середовищі є активність пересилання, але вона в результаті не призвела до реального кадру.

noise combating code – завадостійкий код # код, що дозволяє виявляти із заданою точністю і виправляти помилки, що виникають при пересиланні інформації.

noise generator – генератор завад # засоби придушення закладних

пристроїв, призначені для активної боротьби із закладками шляхом пониження відношення сигнал/шум до безпечних для інформації значень, що дозволяє забезпечити превентивний захист інформації без попереднього виявлення і локалізації закладних пристроїв. Розрізняють генератори завад із лінійним зашумленням і генератори завад із просторовим зашумленням.

noise generator with linear noise – генератор завад із лінійним зашумленням # генератор завад, виходи якого приєднуються до проводів телефонної лінії або електромережі і в них подаються електричні сигнали, що перекривають небезпечні сигнали по спектру і потужності.

noise generator with spatial noise – генератор завад із просторовим зашумленням # генератор завад, призначений для створення відповідного рівня електромагнітних завад у приміщенні і на вході приймача зловмисника. Для ефективного придушення сигналу закладки рівень завади (загороджувальної або прицільної) у смузі спектра сигналу повинен у декілька разів перевищувати рівень сигналу.

noise immunity – *1.* захист від завад # див. interference immunity # *2.* завадостійкість # див. noise stability.

noise stability – завадостійкість # *1.* в радіоелектроніці – здатність радіоелектронної апаратури зберігати якість функціонування на необхідному рівні під впливом радіозавад при відсутності засобів захисту від завад, що не відносяться до принципу її дії або побудови # *2.* в обчислювальній техніці – здатність ЕОМ зберігати якість функціонування під впливом зовнішніх завад та відсутності додаткових засобів захисту від завад, що не відносяться до принципу її дії або побудови.

noise stability of communications systems – завадостійкість системи зв'язку # здатність системи зв'язку розрізняти (відновлювати) сигнали із заданою достовірністю. Визначення завадостійкості всієї системи в цілому – завдання у більшості випадків дуже складне. Тому часто визначають завадостійкість окремих ланок системи: приймача при заданому способі передавання, системи кодування або системи модуляції при заданому способі прийому і т.ін. Розрізняють реальну і потенційну (за Котельніковпм) або таку, яку можна гранично досягти. їхнє порівняння для конкретного пристрою дозволяє оцінити його якість, наприклад, знання потенційної завадостійкості приймача при різноманітних способах передавання дозволяє вибрати з них найбільш досконалі.

noise susceptibility – сприйнятливість ЕОМ до завад # здатність ЕОМ знижувати якість функціонування при дії на неї завад.

noises – шуми # 1. звуки з неясно вираженою тональністю # 2.

випадкові завади в каналі зв’язку, які спотворюють повідомлення. Якість інформації, що одержують, залежить від завадозахищеності і завадостійкості засобів зв’язку, з однієї сторони, і від кількості нерелевантних даних, введених до складу повідомлення, з іншої сторони (шуму інформаційного).

nomadicity – неперервність доступу # властивість сервісу зберігати неперервність з’єднання між двома компонентами інформаційної інфраструктури при їх русі в просторі.

nomadism – номадизм # можливість для користувача змінювати свою точку доступу до мережі таким чином, що при зміні точки поточний сеанс обміну даними повністю припиняється і потім стартує знову. Мається на увазі, що, як правило, користувач завершує сеанс обміну даними ще до зміни точки доступу.

nonconformity – невідповідність # невиконання вимоги.

non-deterministic algorithm – алгоритм недетермінований # алгоритм, який реалізують недетермінованою однострічковою машиною Тьюрінга.

non-linear distortion – нелінійні спотворення # спотворення сигналу, що проявляються у появі в частотному спектрі вихідного сигналу додаткових складових, які відсутні у вхідному сигналі. Нелінійні спотворення викликають елементи радіоприймача, що мають нелінійну залежність між входом і виходом. Вони виникають при перевищенні відношення значень максимальної і мінімальної напруг сигналу на вході приймача його динамічного діапазону. Нелінійні спотворення призводять до зміни інформаційних параметрів сигналу на вході демодулятора і, як наслідок, до спотворення інформації після демодуляції.

non-repudiation – **1.** незаперечність авторства # можливість довести здійснення запитаної події або дії і ініціювання її джерел # **2.** неможливість відмови # здатність до захисту від заперечення участі одного з об'єктів, який приймає участь у всіх діях або в їх частині.

non-repudiation – неспростовність # спроможність надати докази появи заявленої події або дії та їх джерела

non-repudiation – причетність # властивість системи оброблення інформації, яка полягає в тому, що суб’єкти системи захищені від заперечення причетності до утворення або передачі інформації та заперечення причетності до одержання інформації.

nonresident– нерезидентний вірус # комп’ютерний вірус , який не залишається в оперативній пам’яті після завершення програми-переносника вірусу і є активним обмежений час, а потім “гине”.

non-session-based services – несеансові сервіси # послуги, надання яких не потребує сеансів обміну даними.

norm – стандарт # див. standard.

normalization – нормування # процес перетворення відношень в одне чи

кілька більш простих відношень без атрибутів надмірності чи невідповідностей для підтримки реферальної цілісності.

normalize – нормування # зміна подання кількості, вираженням її в інших одиницях, так щоб її діапазон був уведений в границях заданого інтервалу.

normative document – нормативний документ # офіційний документ, який містить певні правила, стандарти, нормалі, нормативи і умови.

normative documentation – нормативна [нормативно-технічна] документація # вид документації технічної, що встановлює норми, правила, технічні і організаційно-методичні вимоги, обов'язкові або рекомендовані до застосування. Охоплює всі категорії і види стандартів, тактико-технічні (технічні) завдання, технічні умови, норми і правила, інструкції, методичні вказівки і т. ін. В залежності від категорії нормативної документації затверджується Держстандартом, міністерствами (відомствами) і підприємствами.

notarization – **1.** нотаризація # реєстрація даних довіреною третьою особою, що забезпечує наступне підтвердження правильності їхніх характеристик, таких як зміст, відправник, час і одержувач # **2.** нотаріальне засвідчення # процедура підтвердження нотаріальними органами наявності певних обставин, з якими можуть пов'язуватися права та обов'язки сторін, що мають доказове значення.

notarization – завірення # реєстрація даних у довіреної третьої особи з метою забезпечення надалі впевненості в правильності таких характеристик як зміст, джерело даних, час відправлення чи одержання тощо.

notion – поняття # див. concept, idea.

novelty effect – ефект новизни # психологічний ефект, що виникає при сприйнятті людьми один одного. Полягає в тому, що по відношенню до знайомої людини найбільше значення має остання, тобто більш нова інформація про неї, а по відношенню до незнайомої людини більше значення має перша інформація.

NSA – National Security Agency– агенство національної безпеки.

NTP – network time protoco – мережний протокол синхронізації часу.

number – номер # порядкове число предмета в ряді інших однорідних.

number – число # дійсна величина в певній системі числення.

number portability – **1.** переносність номера # **2.** мобільність номера # сервіс, що дозволяє абоненту зберігати свій номер при зміні локального розташування.

numbers theory – теорія чисел # наука про цілі числа.

numeric code – цифровий код # код, набір знаків якого містить тільки цифри.

numerical characteristics of random variables – числові характеристики

випадкових величин # функціонали розподілу ймовірностей випадкової величини, які характеризують різноманітні її властивості. Найважливіша з них – математичне очікування. Більшість інших характеристик є похідними поняттями і виражаються у вигляді математичних очікувань функцій від випадкової величини, як, наприклад, дисперсії.

O

object – **1.** мета # те, до чого хтось прагне, чого хоче досягти; ціль # **2.** об'єкт # 1. певна частина реальної дійсності, що оточує нас (предмет, процес, явище) # 2. в мережах обчислювальних – комплекс взаємопов'язаних спільною метою функцій одного рівня; елемент проблемної структури обчислювальної мережі # 3. в теоріїзахисту інформації пасивна сутність, яка підлягає захисту.

object identifier – ідентифікатор об'єкта # унікальний атрибут об'єкта комп'ютерної системи, що дозволяє однозначно виділити даний об'єкт серед подібних.

object integrity – цілісність об'єкта # властивість об'єкта доступу, що характеризує його авторизований

object integrity label – мітка цілісності об'єкта # сукупність атрибутів об'єкта доступу, що забезпечує його цілісність.

object of using information weapons – об'єкт застосування інформаційної зброї # комп'ютерні й зв'язкові системи, що використовуються державними організаціями при виконанні функцій керівництва; воєнна інфраструктура інформаційна, що вирішує завдання управління військами і бойовими засобами, збором і обробленням інформації в інтересах збройних сил; інформаційні і керуючі структури банків, транспортних і промислових підприємств; засоби масової інформації, в першу чергу електронні (радіо, телебачення і т. ін.).

object protection – захист об'єкта # засоби захисту об'єктів типу сейфів, файлів і т. ін.

object/subject identification and authentication – ідентифікування і встановлення автентичності об'єкта/суб'єкта # сукупність заходів ідентифікації та автентифікації, кінцевою метою яких є допуск об'єкта/суб'єкта до інформації обмеженого використання у випадку позитивного закінчення перевірки або відмова допуску у випадку негативного закінчення перевірки. Об'єктами ідентифікації і встановлення автентичності в системі обчислювальній можуть бути: людина (оператор, користувач, посадова особа); технічний засіб (термінал, дисплей, ЕОМ); документи; носії інформації; інформація на дисплеї, табло і т.ін. Установлення автентичності об'єкта може здійснюватися людиною, апаратним пристроєм, програмою, обчислювальною системою і т.ін. В системах автоматизованих

застосування вказаних методів з метою захисту інформації при її обміні передбачає конфіденційність образів і імен об’єктів.

objective – **1.** ціль # **2.** мета # результат, який має бути досягнуто. Цілі можуть бути стратегічними, тактичними або операційними. Цілі може бути поставлено до різних дисциплін (таких як фінанси, охорона здоров’я та цілі щодо навколишнього середовища) і їх можна використовувати на різних рівнях (таких як стратегічний, для організації в цілому, цілі проекту, продукту та процесу. Цілі може бути виражено різними способами, наприклад як розширення випуску продукції, як цільовий показник, як операційний критерій, як ціль інформаційної безпеки чи використання різних слів з подібним значенням (цілі, наміри або кінцеві цілі). У контексті систем керування інформаційною безпекою цілі інформаційної безпеки встановлює організація в межах політики інформаційної безпеки для досягнення певних результатів

object's activity sign – ознака діяльності об’єкта # ознаки, що характеризують етапи і режими функціонування об’єкта, наприклад, етапи створення нової продукції: наукові дослідження, підготовка до виробництва, виготовлення нової продукції, її випробування і т. ін.

objects specific features in infrared radiation range – видові ознаки об’єктів у діапазоні інфрачервоного випромінювання # ознаки видові, що добуваються за допомогою спеціальних приладів (нічного бачення, тепловізорів). До них належать: геометричні характеристики зовнішнього вигляду об’єкта (форма, розміри, деталі поверхні); температура поверхні.

objects specific features in radio emission range – видові ознаки об’єктів у діапазоні радіовипромінювання # ознаки видові, що добуваються за допомогою радіолокаційних станцій. До них належать: ефективна площа розсіювання; геометричні характеристики (форма, розміри, яскравість, деталі); електропровідність поверхні.

objects specific features in visible optical radiation range – видові ознаки об’єктів у діапазоні видимого оптичного випромінювання # ознаки видові, що добуваються при візуально-оптичному спостереженні у видимому діапазоні оптичного випромінювання. До них відносяться: фотометричні та геометричні характеристики об’єктів (форма, розміри об’єкта, колір, структура, малюнок і деталі його поверхні); тіні, дим, пил, сліди на ґрунті, снігу, воді; взаємне розташування елементів групового (складного) об’єкта; розташування об’єкта відносно інших відомих об’єктів.

observation – спостереження # спосіб добування інформації дистанційного на основі одержання і аналізу

зображення об’єкта спостереження (документа, людини, предмета, простору і т. ін.). При спостереженні добуваються, в основному, ознаки об’єктів видові. Проте можливе добування інформації семантичної, якщо об’єкт с. являє собою документ, схему, креслення і т.ін. Об’єкти можуть спостерігатися безпосередньо – очима або за допомогою технічних засобів. Розрізняють наступні способи спостереження з використанням технічних засобів: спостереження візуально-оптичне; спостереження в інфрачервоному діапазоні; спостереження з консервацією зображення; спостереження телевізійне; спостереження лазерне; спостереження радіолокаційне; спостереження радіотеплолокаційне, спостереження гідролокаційне.

observation report – повідомлення про проблему # документально оформлене оцінювачем повідомлення, в якому він просить роз'яснень або вказує на проблему, що виникла при оцінюванні.

observation subsystem – підсистема спостереження #частина системи охорони об’єктів, що забезпечує можливість дистанційного візуального контролю за територією, що охороняється, та діями зловмисників. Основу підсистему спостереження найчастіше складають телевізійні засоби спостереження. До неї входять також засоби освітлення, що забезпечують необхідний рівень освітленості території в нічний час.

offensive information impact – наступальний інформаційний вплив # активний, цілеспрямований, узгоджений за завданнями, місцем і часом вплив залучених до ведення боротьби інформаційної сил і засобів протягом певного часу в заданому районі по окремих інформаційних об’єктах системи управління противника або його ресурсу інформаційного в цілому. При цьому можуть здійснюватися різноманітні удари інформаційні.

offensive information operation – наступальна інформаційна операція # операція інформаційна, що має за мету завоювання переваги інформаційної над противником. В цій операції головні зусилля спрямовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, що проводяться в межах боротьби інформаційної, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

offset track – зміщена доріжка # доріжка, як частина методу захисту від копіювання, що записана у нестандартному положенні на диску.

offside legend – відступна легенда # метод організації, координації, проведення і контролю над проведенням таємної операції розвідувальної, при якому на випадок провалу офіційна влада

може легко «відхреститися» від причетності держави до такої операції.

one-key cryptosystem – симетрична криптосистема # див. symmetric cryptosystem, classical cryptosystem, secret-key cryptosystem.

one-way encryption – однобічне шифрування # шифрування, яке продукує зашифрований текст, з якого вихідні дані не можуть бути відтворені. Незворотне шифрування є корисним під час автентифікації # наприклад, пароль може бути незворотним чином зашифрований, а отриманий зашифрований текст збережений. Паролі, представлені пізніше, будуть також незворотно зашифровані, і порівнюватимуться дві послідовності зашифрованого тексту. Якщо вони ідентичні, представлений пароль правильний.

one-way function – необоротна функція # одностороння функція # функція f така, що: f обчислюють за допомогою алгоритму поліноміального; для зворотної функції f^{-1} не існує поліноміального алгоритму обчислення. Ф. в. є центральним поняттям в багатьох розділах криптології, зокрема, в асиметричній криптографії.

one-way propagation time – час одностороннього розповсюдження # деякий час, потрібний для переміщення між двома найбільш віддаленими станціями даних в мережі з загальною шиною.

on-line user – інтерактивний користувач # див. interactive user.

OOB – out of band – поза смугою.

open guard – відкриті засоби захисту # захист, стан якого оцінюється як ІСТИНА.

open key distribution – відкритий розподіл ключів # механізм розповсюдження ключів незахищеними каналами. Базується на використання дискретного логарифмування.

open source – відкриті джерела # джерела інформація, доступні широкому загалу, головним чином, засоби масової інформації (преса, телебачення, і радіо).

open system – відкрита система # 1. система, яка взаємодіє з навколишнім середовищем – людиною, джерелами інформації, іншими системами # 2. система, здатна розширюватися за рахунок засобів середовища, в якому вона функціонує.

open system – відкрита система # подання у рамках узагальненої абстрактної моделі тих аспектів справжньої відкритої системи, які мають відношення до її зв'язку з іншими реальними відкритими системами.

open system interconnection environment – середовище ВВС # сукупність абстрактних понять, елементів, функцій, служб, протоколів, тощо, визначених в еталонній моделі ВВС, і розроблених на їх основі стандартів, застосування яких забезпечує взаємозв’язок відкритих систем.

open systems interconnection – взаємозв'язок відкритих систем #

взаємозв'язок комп'ютерних систем відповідно до стандартів ВВС та рекомендацій CCITT для обмінювання даними.

open systems interconnection model – модель взаємозв’язку відкритих систем # модель запропонована Міжнародною організацією по стандартизації (ISO) модель мережі із семи рівнів, для кожного з яких створені свої стандарти і загальні моделі.

open systems interconnection reference model – еталонна модель взаємозв'язку відкритих систем #

operation – операція # дія # ряд дій, заходів, пов’язаних з досягнення певної мети # див. action.

operational controls – операційний контроль # контроль безпеки (тобто засоби захисту і заходи протидії, які переважно запроваджуються і виконуються людьми (на відміну від систем).

operational data security – операційна безпека даних # захищеність даних від несанкціонованого, навмисного чи випадкового їхнього розкривання, модифікування або знищення під час оброблення даних.

operational environment – операційне середовище # системне середовище # середовище, яке створюється засобами системи операційної.

operational game – оперативна гра # передача фальшивої інформації противнику (і одержання у відповідь точних відомостей) співробітником розвідки, який видає себе за ворожого агента, або полоненим і перевербованим агентом. Це може здійснюватися, наприклад, через обмін даними по рації (радіогра).

operational protection method – операційний метод захисту # метод захисту інформаційний від доступу несанкціонованого в операційній системі.

operational system – операційна система # інформаційна система, яка виступає як інтерфейс між пристроями обчислювальної системи і прикладними програмами.

opponent – противник # 1. особа, що вороже ставиться до кого-, чого-небудь, протидіє комусь, чомусь # 2. вороже військо, ворожі збройні сили; ворог.

opposition – протиборство # див. confrontation, antagonism.

opposition – протидія # див. counteraction.

optical disk storage – накопичувач на оптичних дисках # накопичувач, носієм інформації в якому є диск оптичний. Відрізняється високою швидкодією і дуже великою ємністю.

optical line – волоконно-оптична лінія зв’язку # лінія зв’язку, у якій сигнали передаються по кабелю волоконно-оптичному.

optimal coding – оптимальне кодування # 1. кодування, що забезпечує оптимальні умови передавання повідомлень по даному каналу зв’язку # 2. кодування, при якому елементарні символи в закодованому повідомленні зустрічаються в середньому з однаковою частотою.

optimum code – оптимальний код # код, при використанні якого по каналу зв'язку за фіксований відрізок часу передається максимальна кількість інформації.

opto-electronic concealment – оптико-електронне маскування # комплекс заходів, спрямованих на приховування військових об'єктів від оптичних (оптико-електронних) засобів розвідки противника. Здійснюється шляхом: використання маскувальних властивостей місцевості, темного часу доби, а також метеорологічних умов, які обмежують можливості цих засобів; проведення заходів з світломаскування; використання укриттів, штучних масок, димів, аерозолів; улаштування фальшивих споруд та об'єктів.

orange book – помаранчева книга # том помаранчевого кольору, що містить опис стандартів обслуговування в мережі типу кембриджського кільця # див. trusted computer system criterion.

organization – організація # 1. створення, засновування чого-небудь, із залученням до цього процесу інших # 2. об'єднання людей, суспільних груп, держав на базі спільності інтересів, мети, програми дій і т.ін. # 3. особливості будови чого-небудь, структура.

organization compatibility – сумісність організаційна # поєднання організаційної структури ACOI різних рівнів і різного функціонального призначення.

organization documentation – документація організаційного забезпечення # частина документації проектної, яка містить рішення про організаційну структуру і інструкції персоналу.

organization of obtaining information – організація добування інформації # перший етап технології добування інформації, який передбачає реалізацію наступних заходів: структурування (декомпозицію) завдань, поставлених користувачами інформації; розроблення задуму заходів добування інформації; планування заходів; постановка завдань виконавцям заходів; нормативне і оперативне управління діями виконавців і режимами роботи технічних засобів. Організації добування інформації займаються підрозділи планування і управління органів розвідки.

organization study of psychological warfare objects – організація вивчення об'єктів психологічної війни # організація роботи органів психологічної війни, спрямованої на збирання й аналіз відомостей, що характеризують об'єкти психологічного впливу відповідно до процесу вивчення об'єктів психологічної війни.

organizational-legal protection method – організаційно-правовий метод захисту # комплекс організаційних заходів з підтримки безпеки обчислювальної системи та відповідні закони держави в галузі безпеки інформації.

organs of sense – орган чуття # органи зору, слуху, гравітації, нюху, смаку, дотику, що складаються з чутливих нервових клітин і допоміжних структур. Сприймають і попередньо аналізують різноманітні подразнення, що одержуються організмом із зовнішнього і внутрішнього середовища; передають інформацію в центральну нервову систему. Орган чуття сприяють найбільш досконалому пристосуванню організму до навколишнього світу.

OSI environment – середовище ВВС # абстрактне подання набору понять, елементів, функцій, сервісів і протоколів, як визначено еталонною моделлю ВВС та похідними специфічними стандартами, які під час застосуванні дозволяють здійснювати взаємозв'язок між відкритими системами.

OSI management – адміністративне керування ВВС # засоби керування, координування та моніторингу ресурсів, що дозволяють здійснювати зв'язок у середовищі ВВС.

OSI model – open systems interconnection model – модель взаємозв’язку відкритих систем

OSI reference model – еталонна модель ВВС # модель, яка описує загальні принципи взаємозв'язку відкритих систем та архітектуру мережі, що випливають з цих принципів # модель, описана в ISO 7498 та CCITT X.200, являє собою основу для координації розробляння стандартів, які стосуються моделі.

OSI – open systems interconnection – взаємозв'язок відкритих систем, ВВС.

OSIE – OSI environment – середовище ВВС.

outsource – аутсорсинг # укладання угоди, де зовнішня організація виконує частину функцій або процесів організації. Зовнішня організація перебуває поза межами сфери застосування системи керування**,** хоча функції або процеси, передані на аутсорсинг, входять до сфери застосування

overall verdict – загальний вердикт # позитивний або негативний висновок оцінювача за результатами оцінки.

overload – перевантаження # забезпечення надмірною кількістю чого-небудь.

oversight verdict – вердикт органу оцінювання # висновок органу оцінювання, який підтверджує або відхиляє загальний вердикт, який заснований на результатах діяльності з нагляду за оцінюванням.

owner – власник # господар певних речей, майна і т.ін. на правах приватного або суспільного володіння.

P

PABX – private automated branch (telephone) exchange – приватна АТС автоматичного телефонного зв'язку.

packet – пакет # *1.* в протоколах TCP/IP – дані, що передаються між рівнями мережним і канальним. Також узагальнений термін для даних, що передаються в Інтернеті # *2.*

послідовність бітів, розташованих у певному форматі, який містить контрольні дані та, можливо, дані користувача, які передають і комутують як одне ціле.

packet assembler/disassembler – збирач/розбирач пакетів # функційний блок, який дає змогу термінальному обладнанню даних, не обладнаному для пересилання пакетів, отримати доступ до мережі пакетної комутації.

packet error rate – **1.** інтенсивність спотворення пакетів # **2.** ймовірність спотворення пакетів # відношення кількості прийнятих пакетів з помилками до загальної кількості прийнятих за достатньо значний проміжок часу.

packet flow – потік пакетів # послідовність пакетів одного типу, ідентифікована спільними адресою і номерами портів.

packet fragmentation – фрагментація пакетів # розділення пакетів на менші частини для узгодження з вимогами фізичної мережі, через яку вони повинні передаватися.

packet insertion rate – **1.** інтенсивність вставляння пакетів # **2.** ймовірність вставки пакетів # відношення кількості пакетів, доставлених не за адресою, до загальної кількості прийнятих за достатньо значний проміжок часу.

packet loss rate – інтенсивність втрат пакетів # ймовірність втрат пакетів # відношення кількості втрачених пакетів до загальної кількості переданих за достатньо значний проміжок часу.

packet mode terminal – пакетний термінал # термінальне обладнання даних, яке може контролювати, форматувати, передавати та приймати пакети.

packet reassembly – розбирання пакетів # відновлення попередньо фрагментованих пакетів перед передаванням їх транспортному рівню.

packet switching – комутування пакетів # у мережі пересилання даних, процес маршрутизації та пересилання даних за допомогою адресних пакетів, так що між двома вузлами кожен канал пересилання динамічно розподіляється на пакети, що мають різні адреси.

packet switching – комутувуання пакетів # 1. комутація повідомлень даних, при якій повідомлення приймаються, накопичуються і передаються у вигляді пакетів даних # 2.метод динамічного розподілу комунікаційних ресурсів між взаємодіючими об’єктами.

packet switching network – мережа з комутацією пакетів # мережа передавання даних, в якій повідомлення, що передається, розділяється на декілька спеціально оформлених порцій – пакетів, кожний з яких передається незалежно, часто навіть різними каналами зв’язку.

packet switching system – пакетна система комутації # територіально розподілений апаратно-програмний

комплекс, утворений на базі пакетних технологій канального, мережного та транспортного рівнів для надання телекомунікаційних мультимедійних сервісів.

packet transfer mode – режим пересилання пакетів # спосіб пересилання даних, за допомогою пакетного пересилання та комутації пакетів, що дає змогу динамічно розподіляти ресурси мережі серед багатьох з'єднань.

packing – пакування # операція, що виконується, коли дані пакуються.

packing density – щільність пакування (даних) # кількість символів даних, що зберігаються на одиницю довжини, області чи об'єму # щільність даних зазвичай виражають в символах на міліметр (cpmm) або символах на радіан (cprad) # на дисках, зазвичай, вказують загальну ємність диска, записана на одній або з обох сторін, а не щільність даних.

PAD – packet assembler/disassembler – збирач/розбирач пакетів.

padlocking – замикання # використання спеціальних методів захисту даних або програмного забезпечення від несанкціонованого копіювання.

page – сторінка # встановлена порція інформації для обміну між пам’яттю і пристроєм перекачки в системі із сторінковим обміном.

PAI – protocol-addressing-information – протокольна адресна інформація

panic – паніка # психологічний стан, який викликаний загрозливим впливом зовнішніх умов та виражений у почутті дошкульного страху, що охоплює людину або багатьох людей, нестримного неконтрольованого намагання уникнути небезпечної ситуації.

PAP – password authentication protocol – протокол розпізнавання за паролем.

parameter specification – специфікація параметрів # опис типу й способу передавання параметрів, а також обмежень, яким вони повинні задовольняти.

parapsycology – парапсихологія # позначення галузі досліджень, що ставить за мету вивчення форм сприйняття, що здійснюється без участі органів чуття, а також форм впливу живої істоти на фізичні явища поза організмом без зусилля м’язів (бажанням, думкою і т. ін.). П. використовується для пояснення психічних явищ, що не мають чіткого наукового обґрунтування: екстрасенсорного сприйняття, телепатії, телекінезу і т.ін. Інша назва парапсихології — психотроніка.

parasitic virus – паразитичний вірус # комп’ютерний вірус , який при розповсюдженні своїх копій обов’язково змінює вміст програм, файлів або дискових секторів. До цього виду вірусів відносяться усі віруси, які не є “черв’яками” або “супутниками”.

parity check – контроль на парність (парності) # метод контролю даних, при якому сума за модулем 2 двійкових одиниць в машинному слові, включаючи контрольний розряд, повинна мати певне значення – бути завжди парною або непарною.

parity-check code – код з контролем на парність # двійковий код, в якому до кожної комбінації кодової приєднується додатковий контрольний розряд, що допомагає зберегти прийняту в системі одну і ту ж парність двійкових блоків.

partial information security system protection criterion – часткові показники ефективності системи захисту інформації # показники, що характеризують ефективність захисту інформації з окремих сторін. Такими показниками можуть бути: ймовірність виявлення і розпізнавання органами розвідки об'єктів захисту; похибки вимірювання ознак об'єктів захисту; якість розбірливості мови на виході приймача злов- мисника; достовірність (ймовірність помилки) дискретного елемента інформації (букви, цифри, елемента зображення). На основі різноманітних композицій часткових показників, найчастіше їхньої «зваженої» суми формується критерій ефективності системи захисту інформації глобальний.

parts – частина # 1. доля, окрема одиниця, на які підрозділяється ціле # 2. предмет як складовий елемент якого-небудь цілого # 3. відділ якого-небудь закладу.

party – сторона # особа або група осіб, яких стосується діяльність або успіх організації.

passive attack – пасивна атака # атака на віддалену мережу обміну інформацією, яку здійснюють з метою порушення політики безпеки інформації. Пасивна атака не здійснює безпосереднього впливу на роботу мережі.

passive hiding – пасивне приховування інформації # приховування інформації ослабленням енергетичних характеристик фізичних полів або зниження концентрації речовин.

passive information accumulation – пасивне накопичення інформації # нагромадження інформації, при якому інформація, що поступає, просто «складується», при чому приймаються заходи до забезпечення її збереження і повторного зчитування.

passive object – пасивний об'єкт # об'єкт комп'ютерної системи, над яким виконується дія і (або) який служить джерелом чи приймальником інформації.

passive threat – пасивна загроза # загроза несанкціонованого розкриття інформації без зміни стану системи опрацювання даних # наприклад загроза, яка призвела б до відновлювання конфіденційної інформації за допомогою перехоплення переданих даних.

passive wiretapping – пасивне перехоплення # перехоплення, що обмежується отриманням даних.

password – пароль # *1.* ідентифікатор суб'єкта доступу (найчастіше рядок символів), що є його (суб'єкта) секретом і використовується в процедурі автентифікації # *2.* символьний рядок, який

застосовується як інформація про автентифікацію.

password authentication protocol – протокол розпізнавання за паролем # протокол, що надає одноранговим об'єктам двопунктового з'єднання можливість автентифікувати один одного.

password code – код пароля # пароль, позначений системою знаків за правилами, встановленими вибраною системою кодування. При виборі кода пароля виходять з того якою повинен бути його розмір (довжина паролю), стійкість до несанкціонованого підбору та способи застосування.

password protection – **1.** захист кодів паролів # сукупність застережних заходів, спрямованих на те, щоб дійсні коди паролів були недоступні стороннім особам. Рекомендуються наступні основні заходи обережності для захисту кодів паролів: паролі ніколи не слід зберігати в обчислювальній системі в явному вигляді, вони завжди повинні бути зашифровані; паролі не слід друкувати (відображати) в явному вигляді на терміналі користувача (за виключенням термінала оператора служби безпеки інформації, який повинен знаходитися в ізольованому приміщенні); пароль необхідно міняти як можна частіше і по випадковому закону (чим більший період часу використовується один і той же пароль, тим більша ймовірність його розкривання); система ніколи не повинна виробляти новий пароль в кінці сеансу зв'язку навіть у зашифрованому вигляді, так як це може дозволити порушникові легко ним скористатися. Для закриття кодів паролів можна використати метод шифрування необоротного і більш складний метод "необоротного безладного складення", коли паролі за допомогою спеціального полінома перетворюються в зашифрований пароль. Найбільш ефективним захистом пароля від несанкціонованого доступу вважається розділення його на дві частини: одну – для запам'ятовування користувачем, іншу – для зберігання на спеціальному носії. На випадок утрати або викрадення носія пароля у користувача буде час заявити про це у службу безпеки інформації, а ця служба може встигнути змінити пароль . # **2.** захист паролем # захист за допомогою пароля # спосіб захисту даних, що полягає у перевірці відповідності наданого суб'єктом доступу пароля еталонному паролю для надання доступу до об'єкта доступу. Являє собою один з видів простої автентифікації.

path – шлях # маршрут # послідовність гілок, яка з'єднує два вузли мережі, застосовуючи кожну гілку лише один раз # шлях може складатись лише з однієї гілки # між будь-якими двома вузлами може існувати більше одного шляху.

PC – personal computer – персональний комп’ютер.

PCI – protocol control information – інформація керування протоколом.

PDA – personal data assistant – персональний асистент даних.

PDU – protocol data unit – протокольний блок даних.

peer entities – одноранговий об'єкт # однорангові логічні об’єкти # об'єкти в одній або різних відкритих системах, що знаходяться на одному рівні # зв'язок між об'єктами, розташованими в тій самій відкритій системі, виходить за рамки ICI.

peer-entity authentication – автентифікація однорангового логічного об'єкта # підтвердження того, що рівноправний логічний об'єкт у будь-якій асоціації є заявленим логічним об'єктом.

peer-to-peer network – однорангова мережа # комп'ютерна мережа, яка містить лише вузли, аналогічні за можливостями керування або роботи.

penetration – проникнення # несанкціонований доступ до системи опрацювання даних.

penetration testing – тест на проникнення # вивчання функцій системи опрацювання даних для знаходження засобів обходу комп'ютерної безпеки.

penetration testing – тестування на проникнення # випробування, метою яких є здійснення спроби обминути або відключити механізми захисту.

perception – пізнання # див. cognition.

perfect cryptosecurity – абсолютна криптостійкість # криптостійкість, що визначається за умов наявності у крипто аналітика нескінченного часу та нескінченних обчислювальних можливостей. Досягнення к. а. за Шеноном означає, що відкритий та шифртекст є статистично незалежними. Шеноном показано, що абсолютна криптостійкість досягається тільки тоді, якщо довжина ключа є не меншою від довжини відкритого тексту та ключ обирається з ключового простору дійсно випадково. Інша назва криптостійкість у теоретико-інформаційному сенсі.

performance – **1.** результативність # результат, який можна виміряти. Результативність може відноситися до кількісних або якісних показників. Результативність може бути пов’язана з керуванням діяльністю, процесами, продуктами (в тому числі послугами), системами або організаціями # **2.** показник діяльності # вимірний результат # показник діяльності може бути пов'язаний як з кількісними, так і якісними результатами # показник діяльності може відноситися до керування роботами, процесами, продуктами (включаючи послуги), системами або організаціями.

period – період # проміжок часу, протягом якого відбувається якийсь процес.

periodic check of information security– періодичний контроль захисту інформації # контроль захисту інформації з метою систематичного спостереження за рівнем захисту.

Здійснюється вибірково (стосовно до окремих тем робіт, структурних підрозділів або всієї організації) на основі планів, затверджених керівником організації, а також вищими органами. Найбільш часто повинен проводитися періодичний контроль на хімічних підприємствах, так як незначні порушення в технологічному процесі можуть призвести до витоку демаскуючих речовин. Для визначення концентрації демаскуючих речовин регулярно беруться біля підприємства проби повітря, води, ґрунту, снігу, рослинності. Періодичний (щоденний, щотижневий, щомісячний) контроль повинен проводитися співробітниками організації стосовно джерел інформації, з якими вони працюють. Загальний (в межах всієї організації) періодичний контроль здійснюється два рази на рік з метою ретельної перевірки працездатності всіх елементів і системи захисту інформації в цілому.

periodic sign – періодична ознака # ознака, що проявляється через певні рівні проміжки часу.

permanent sign – постійна ознака # ознака, що не змінюється протягом життєвого циклу об'єкта.

permanent storage – постійна пам'ять # частина пам'яті оперативної комп'ютера персонального, яка розташована в пристрої запам'ятовуючому постійному і містить програми базової системи вводу-виводу.

permissible action – прийнятна дія # дія, що відповідає певним правилам чи обмеженням.

persistent data – сталі дані # дані, які зберігаються в інформаційній системі на протязі більш ніж одного сеансу керування даними.

personal computer – персональний комп'ютер # персональна ЕОМ.

personal data – персональні дані # див. private data.

personal identification number – номер ідентифікаційний персональний # вид паролю, що, звичайно, складається тільки з цифр, і який, як правило, має бути пред'явлений нарівні з ідентифікатором, що носиться.

personal indication – іменна ознака # ознака, що належить тільки одному конкретному об'єктові.

personal information security – інформаційна безпека особистості # захищеність психіки і свідомості людини від небезпечних впливів інформаційних: маніпулювання, дезінформування, спонукання до самогубства, образ і т. ін.

personal security – безпека особистості # положення, при якому особистості не загрожує небезпека. Безпека особистості полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, які дозволили би їй розвивати і реалізовувати соціально значимі здібності і потреби, не зазнаючи при цьому протидії держави і суспільства.

personal-identification code – ідентифікатор користувача # див. userid.

personality – особистість # 1. людина як суб'єкт відносин і свідомої діяльності # 2. відносно стійка система поведінки індивіда, побудована насамперед на основі введення в соціальний контекст. Стрижневим формуванням о. є самооцінка, яка будується на оцінках індивіда іншими людьми і його оцінюванні цих інших.

personalization – персоналізація # процес занесення на пластикову картку даних, які дозволяють ідентифікувати саму карту, її власника, а також перевірити платежеспроможність картки при її прийманні до оплати або видачі готівки.

persuasion – переконаність # див. conviction.

persuasiveness – переконливість # див. convincingness.

phase distortion – фазові спотворення # спотворення сигналу, що виникають через порушення фазових співвідношень між окремими спектральними складовими сигналу при проходженні його колами тракту приймача.

phase jitter – фазове тремтіння # тремтіння, що виражаються як частка значущого інтервалу.

phishing – фішинг # шахрайство, за допомогою якого в електронний пошті користувача виявляють особисту чи конфіденційну інформацію, яку шахрай може потім незаконно використовувати.

phisical security – фізичний захист # використовувані засоби для забезпечення фізичного захисту ресурсів від навмисної чи випадкової загрози.

photographic camera – апарат фотографічний # оптико-механічний прилад для одержання оптичного зображення об'єкта, що фотографують, на світлочутливому шарі фотоматеріалу. Всі фотографічні апарати складаються зі світлонепроникного корпусу із закріпленим на його передній стінці об'єктивом, пристрою для розташування або фіксації світлочутливого матеріалу, розташованого біля задньої стінки корпусу, і затвора, призначеного для пропускання протягом певного часу (часу експозиції) світлового потоку від об'єкта, що фотографують. Крім того, фотографічний апарат обладнуються допоміжними вузлами і механізмами, які полегшують та автоматизують процес зйомки, дозволяють розширити його можливості, покращити технічні параметри. За розмірами світлочутливих матеріалів фотографічний апарат поділяються на п'ять груп: мікроформатні, півформатні, мало-, середньо- і великоформатні. За призначенням фотографічного апарату поділяються на широкого застосування і спеціального застосування. В залежності від способу наведення на

різкість фотографічні апарати можна розділити на наступні групи: з наведенням на різкість за зображенням на екрані фотографічного апарату (дзеркальні або SLR – апарат фотографічний); з наведенням по монокулярному далекомірному пристрою, що механічно зв'язаний з об'єктивом фотографічного апарату; з нерухомим жорстко встановленим об'єктивом, сфокусованим на гіперфокальну відстань; з пристроєм автоматичного фокусування. За технічною оснащеністю фотографічні апарати поділяються на три класи: простий, середній, високий. За показниками оснащення фотографічного апарату вбудованими експонометрами, а також за ступенем автоматизації встановлення експозиційних параметрів а. ф. ділять на три групи: з ручною установкою, з півавтоматичною і з автоматичною установкою експозиції.

photographic material – фотографічні матеріали # див. light-sensitive material.

physical medium – фізичне середовище # див. environment.

physical protection method – фізичний метод захисту # метод захисту, що полягає в обмеженні фізичного доступу до об'єктів інформаційної системи, що охороняються.

physical protection of computer systems – фізичний захист комп'ютерних систем # захист, що здійснюється шляхом застосування пристроїв, які би виключали доступ до інформації в системі комп'ютерній без порушення фізичної цілісності комп'ютерів. В ряді випадків принциповим є застосування заходів, що виключають негласний (в тому числі і регулярний) доступ до комп'ютера з метою копіювання або модифікації інформації. Засобами фізичного захисту комп'ютерних систем можуть бути: опечатування системного блока та інших елементів комп'ютерних систем спеціальними пломбами або печаткою керівника служби безпеки; використання спеціальних уставок в «кишеню» дисковода, обладнаних замком з фіксацією на ключ; застосування спеціальних замків, що блокують клавіатуру комп'ютера; організація зберігання магнітних і оптичних носіїв в сейфах або у спеціальних дискетіпіцях. що закриваються на замок.

physical security – безпосередній захист # заходи, що передбачають фізичний захист ресурсів від навмисних або випадкових загроз.

PICS – protocol implementation conformance statement – заявка про відповідність реалізації протоколу.

piezoelectric material – п'єзоелектричні матеріали # кристалічні речовини, в яких при стисканні або розтяганні в певних напрямах виникає електрична поляризація навіть при відсутності електричного поля (прямий п'єзоефект). Наслідком прямого п'єзоефекту є зворотний п'єзоефект – поява механічної деформації

внаслідок дії електричного поля. Зв'язок між механічними і електричними змінними (деформацією і електричним полем) носить в обох випадках лінійний характер. П'єзоелектричні матеріали використовують для виготовлення перетворювачів п'єзоелектричних. П'єзоелектричні матеріали є природно або штучно вирощені монокристали (кварц, дігідрофосфати калію і амонію, сегнетова сіль та ін.) і полікристалічні тверді розчини, попередньо піддані поляризації в електричному полі (п'єзокераміка).

piggyback entry – несанкційований вхід [засобами зареєстрованого користувача] # несанкціонований доступ до системи опрацювання даних через законне під'єднування авторизованого користувача.

pilotless vehicle – літальний безпілотний апарат # апарат літальний, на борті якого не передбачено розташування екіпажу. Розрізняють літальні безпілотні апарати легші і важчі за повітря, для атмосферних і космічних польотів, воєнного і цивільного призначення, одноразового і багаторазового застосування, з керуванням від бортового програмного пристрою або з телекеруванням (дискретним або безперервним) # див. remotely piloted vehicle.

PIN – personal identification number – номер ідентифікаційний персональний.

PIN – personal identification number – персональний ідентифікаційний код.

PKCS – public-key cryptography standards – стандарт шифрування з відкритим ключем.

PKI – public key infrastructure – інфраструктура відкритих ключів.

plaintext – незашифрований текст # дані, семантичний вміст яких доступний без застосування криптографічних методів.

platform – платформа # рівний підвищений майданчик.

playback – відтворювання # технологія, за якої історія виконання всієї чи частини програми записується таким чином, що вхід і вихід можуть відновлюватися під керуванням користувача, можливо, у прямому чи зворотному напрямку # відтворювання застосовується під час налагодженні.

point of presence – пункт присутності # місце, де існує телекомунікаційне обладнання певного сервісу обміну даними чи певного оператора, окремим випадком є пункт присутності Інтернет (IPoP – Internet PoP).

point-to-multipoint connection – з'єднання «точка – багато точок» # з'єднання, яке забезпечує взаємозв'язок одної точки мережі з багатьма іншими.

point-to-point connection – з'єднання «точка – точка» # з'єднання, яке забезпечує взаємозв'язок двох точок мережі.

point-to-point protocol – **1.** протокол обміну даними «точка-точка» # **2.**

протокол PPP # протокол, який забезпечує захищені з'єднання маршрутизатора з маршрутизатором, комп'ютера з мережею тощо через синхронні чи асинхронні канали.

point-to-point tunnelling protocol – **1.** тунельний протокол обміну даними «точка-точка» # **2.** протокол PPTP # протокол рівня 2, який інкапсулює для передавання кадри протоколу двопунктового зв'язку PPP в IP-дейтаграми.

policy – **1.** політика # 1. загальні наміри та напрямок розвитку організації, формально затверджені його вищим керівництвом # 2. цілі і завдання, що їх ставлять суспільні класи в боротьбі за свої інтереси; методи і засоби досягнення цих цілей і завдань # 3. лінія поведінки у чому-небудь, певне ставлення до кого-, чого-небудь # **2.** стратегія # див. security policy.

political security – політична безпека # національна безпека здатність і можливості нації та її державних інститутів самостійно вирішувати питання державного устрою, незалежно проводити внутрішню і зовнішню політику в інтересах особистості та суспільства. Політична безпека передбачає наявність стійкого політичного суверенітету в межах міждержавних відносин і політичної стабільності суспільства, що досягають формуванням політичної системи, яка би забезпечувала баланс інтересів різноманітних соціальних груп з опорою на пріоритет особистості. Відсутність як першого, так і другого неминуче руйнує політичну безпеку країни.

polling – опитування # метод збирання первинної інформації шляхом звернення із запитаннями до певної групи людей. З допомогою о. отримують як фактичну інформацію (інформацію про події), так і відомості про погляди, оцінки і особисті думки опитуваних.

polycemy – полісемія # наявність різних лексичних значень в одного й того самого слова.

polygram – поліграма # послідовність кількох символів алфавіту. Послідовність із *l* символів алфавіту називають також *l*-грамою.

polygraph – поліграф # детектор брехні, дія якого заснована на хімічних змінах в організмі людини, що відчуває психологічний стрес. При стресі підвищується вміст адреналіну в крові, збільшується потреба організму в кисні, що, у свою чергу, викликає збільшення частоти пульсу, підвищення кров'яного тиску, частоти і глибини дихання. Коли джерело стресу зникає, організм випрацьовує норадреналін, який нейтралізує дію надлишкового адреналіну. Для відображення даних в п. використовують не менш двох самописців: кардіографічний і пневмографічний.

polymorphic virus – поліморфний вірус # вірус комп'ютерний, що змінює свою структуру.

polynomial code – поліноміальний код # код з виправленням помилок, в якому контрольні розряди є остачею від ділення на поліном, який називається утворюючим.

polyphag – поліфаг # антивірусна програма, що розпізнає відомі їй віруси за характерними ділянками їхнього коду.

POP – post office protocol – протокол електронної пошти.

PoP – point of presence – пункт присутності.

port – порт # *1.* функційний блок, через який дані можуть входити у мережу або залишати її # *2.* кінцева точка, через яку сигнали можуть входити чи виходити з мережі # *3.* кінцева точка з'єднання. У контексті Інтернет-протоколу порт являє собою кінцеву точку логікового каналу з'єднання TCP або повідомлень UDP. Протоколи застосунків на основі TCP або UDP зазвичай мають призначені за промовчуванням номери портів, наприклад, порт 80 для протоколу HTTP.

portrait – портрет # загальна характеристика, сукупність характерних рис кого-, чого-небудь.

positioning time – час позиціонування # час, потрібний важілю доступу у пристрої зберігання з прямим доступом, для розташування на відповідній доріжці.

post office protocol – протокол електронної пошти # протокол, що є клієнтським застосуванням, використовуваним для витягнення пошти з поштового сервера (найбільш поширеним є POP3). Для електронної пошти існує також універсальний протокол X.400, який визначає „конверт” для її повідомлень, які таким чином приймають стандартний формат.

post-development review – аналіз функціювання розробленої системи # дослідження впливу системи після досягнення стабілізованого стану експлуатаційного використання.

post-implementation review – аналіз функціювання впровадженої системи # дослідження впливу системи після досягнення стабілізованого стану експлуатаційного використання.

postmortem dump – аварійний роздрук # роздруківка, яка виробляється під час ненормального припинення виконання програми.

potential threat to security of information in local computer network – загроза потенційні безпеці інформації в локальній обчислювальній мережі # загрози, пов’язані з наявністю навмисних і випадкових каналів несанкціонованого доступу до інформації в мережі обчислювальній локальні. Зі сторони “периметра” системи вони можуть бути наступними: доступ до ЛОМ із сторони штатної ПЕОМ (сервера); доступ в ЛОМ із сторони кабельних ліній зв’язку. Несанкціонований доступ в ЛОМ із сторони кабельних ліній може здійснюватися наступними каналами: із сторони штатного користувача-порушника однієї ПЕОМ при зверненні до іншої

інформації, в тому числі до файл-сервера; при приєднанні сторонньої ПЕОМ та іншої сторонньої апаратури; при побічних електромагнітних випромінюваннях і наведеннях інформації. Крім того, в результаті аварійних ситуацій, відмов апаратури, помилок операторів і розробників програмного забезпечення ЛОМ, можливі переадресування інформації, відображення і видача її на робочих місцях, для неї не призначених, втрата інформації в результаті її випадкового стирання або пожежі.

power – влада # див. authority.

PP – protection profile – профіль захисту.

PPP – point-to-point protocol – протокол обміну даними «точка-точка» # див. point-to-point protocol.

PPTP – point-to-point tunnelling protocol – **1.** тунельний протокол обміну даними «точка-точка» # **2.** протокол PPTP.

predefined identifier – наперед заданий ідентифікатор # ідентифікатор, який визначається як частина мови програмування # наприклад зарезервоване слово # якщо наперед заданий ідентифікатор не зарезервовано, то декларація, що застосовує цей ідентифікатор, перевизначає своє значення для обсягу декларації.

predefined type – наперед заданий тип # тип даних, на який посилається наперед заданий ідентифікатор, для якого мова програмування забезпечує відповідні операції.

prefix code – префіксний код # код, що складається зі слів різної довжини, причому ніякий більш короткий код не є початком (префіксом) більш довгого.

pressmark – шифр # див. cipher.

preventing the leakage of information through mortgage eavesdropping devices – запобігання витоку інформації через закладні підслуховуючі пристрої # спосіб протидії підслухуванню, що охоплює виявлення, локалізацію і вилучення або придушення закладних пристроїв. Відповідно до цього засоби запобігання витоку поділяються на засоби радіоконтролю приміщень, засоби пошуку невипромінюючих закладних пристроїв і засоби придушення закладних пристроїв.

prevention – запобігання # недопущення чогось заздалегідь, відвертання.

prevention of information leakage through exposure to radiation and guidance – запобігання витоку інформації через побічні випромінювання і наведення # спосіб протидії витоку інформації за допомогою небезпечних сигналів, що створюються випромінюваннями і наведеннями електромагнітними побічними. Способи і засоби захисту інформації через побічні електромагнітні випромінювання і наведення повинні задовольняти наступним вимогам: небезпечні

сигнали, які можуть нести конфіденційну інформацію, повинні бути ослаблені до рівня, що виключає зняття з них інформації на межі контрольованої зони; засоби захисту не повинні вносити помітних спотворень в роботу функціональних пристроїв, що використовуються в організації, і не ускладнювати процес користування ними. Запобігання витоку інформації небезпечними сигналами здійснюється шляхом придушення небезпечних електричних сигналів акустоелектричних перетворювачів і екранування побічних полів.

prevention of information leakage through material channels – запобігання витоку інформації матеріально-речовими каналами # спосіб протидії зняттю інформації з матеріально-речовинних носіїв інформації, що охоплює захист інформації, яку містять відходи і захист демаскуючих речовин.

prevention unauthorized recording of voice information on a voice recorder – запобігання несанкціонованому запису мовної інформації на диктофон # виявлення працюючого диктофону, прихованого в кишені, портфелі, сумці або інших речах, що носяться, та порушення роботи диктофону таким чином, щоб якість записаної інформації була нижчою за допустимий рівень. Вирішення навіть першого завдання дозволяє прийняти заходи захисту інформації, в тому числі: припинити переговори або нараду; знижувати рівень конфіденційності розмови, не допускаючи висловлювань, які можуть після їхнього документування на диктофон заподіяти шкоду організації або учасникам переговорів.

preventive maintenance – профілактичне технічне обслуговування # технічне обслуговування, що виконується з заданими інтервалами чи відповідно до встановлених критеріїв з метою зменшення ймовірності виникнення аварії чи деградації функціювання функційного блока.

price – ціна # 1. вартість товару, що виражена у грошах # 2. грошове відшкодування за товар, послуги, плата.

price of information – ціна інформації # вартість інформації, виражена у грошах. Складається із собівартості інформації та прибутку від інформації. Собівартість визначається витратами власника інформації на її одержання, наприклад: проведення досліджень в наукових лабораторіях, аналітичних центрах, групах і т. ін.; купівля інформації на ринку інформації; добування інформації за допомогою протиправних дій. Прибуток від інформації з огляду її особливостей може приймати різноманітні форми, причому вираз його у грошах не є найбільш розповсюдженою формою. В загальному випадку прибуток від інформації може бути одержаний в результаті наступних дій: продажу інформації на ринку; матеріалізації

інформації в продукції з новими якостями або технології, що приносить прибуток; використання інформації для прийняття більш ефективних рішень. Остання форма прибутку від інформації не стільки очевидна, проте вона найбільш розповсюджена, тому що будь-яка діяльність людини це послідовність прийняття нею рішень.

primacy effect – ефект первинності # психологічний ефект, суть якого в тому, що ймовірність пригадування декількох перших елементів однорідного матеріалу більш висока, ніж середніх (при цьому, чим більший обсяг пред’явленого матеріалу і чим вищий темп його подавання, тим менша кількість перших елементів запам’ятовується).

primality test – тест на простоту # алгоритм вирішення задачі розпізнавання приналежності натурального числа до класу чисел простих. Розрізнюють тести на простоту детерміновані, ймовірнісні та гіпотетичні.

primary index – первинний індекс # індекс для первинних ключів.

primary key – первинний ключ # ключ, який визначає один запис.

prime number – просте число # натуральне число, яке більше *1* та ділиться націло тільки на *1* та на само себе.

primitive name – просте ім'я # ім'я, що ідентифікує об'єкт і надається призначеним уповноваженим з найменування. Внутрішня структура імені не повинна цікавити або мати значення для користувачів такого імені.

principal – суб'єкт # об'єкт, який може обмінювати дані з іншим об'єктом за захищеним з'єднанням. Для ідентифікування суб'єкта застосовують пов'язаний контекст захисту, в якому задані його права доступу.

principle – принцип # основи # першооснова; те, що лежить в основі певної теорії науки # див. base, basic, ground, foundation, fundament, law.

privacy – конфіденційність # секретність # приватність # право окремих осіб контролювати або впливати на збір і збереження інформації, котра стосується цих осіб, і на визначення тих, ким і для кого може бути розкрита ця інформація. Оскільки цей термін стосується прав окремих осіб, він не може бути точно визначений і його використання варто уникати, за винятком обґрунтованих випадків для запитуваного захисту # див. confidentiality.

privacy key – ключ секретності # ключ, значення якого система обчислювальна використовує для визначення того, чи повинен ресурс захищений бути доступним тому процесові, який видав дане значення ключа.

privacy lock – замок секретності # див. protection lock.

privacy protection – захист конфіденційності # заходи, спрямовані на забезпечення конфіденційності # заходи

охоплюють захист даних та обмеження щодо збору, об'єднання та опрацювання даних про особу.

private – приватний # стосується характеристик мовних конструкцій, що безпосередньо не є доступними користувачеві цих мовних конструкцій.

private data – особисті дані # індивідуальні дані # приватні дані # дані, власником і користувачем яких є окрема особа (обмежена група осіб, окрема установа).

private domain name – ім'я приватного домену # атрибут, який визначає приватний домен керування щодо країни чи щодо домену адміністративного керування.

private key – приватний ключ # ключ, призначений для перетворення криптографічного у кріпи осіістсмі асиметричній, виключно тим її елементом, який є власником цього ключа. Зворотне криптографічне перетворення може бути виконане із застосуванням відповідного ключа відкритого.

private management domain – приватний домен керування # адміністративний домен, керований організацією, яка не є телекомунікаційним оператором, визнаним телекомунікаційним органом даної країни.

private part – закрита частина # частина декларації пакету, яка надає структурні деталі, необхідні для процесу розробляння, але є нерелевантною і недоступною для функційних користувачів пакету.

private storage – внутрішня пам’ять # пам’ять, яка вбудована в обчислювальний пристрій і безпосередньо керується цим пристроєм.

private terminal – індивідуальний термінал # приватний термінал # термінал, що знаходиться в розпорядженні одного користувача; термінал індивідуального використання.

private type privileged instruction – приватний тип привілейованої операції # в межах програми – тип даних, структура, набір значень та операції є визначеними, але доступність до яких обмежується привілейованими частинами цієї програми # наприклад в Ada для користувачів доступні лише призначення, рівність та нерівність, за винятком будь-яких явно доступних операцій.

private virtual network – приватні віртуальні мережа # 1. зашифрований або інкапсульований процес комунікації, який безпечним чином передає дані з однієї точки в іншу. Безпека цих даних забезпечена стійкою технологією шифрування, і дані, що передаються, проходять через відкриту, незахищену, маршрутизовану мережу # 2. розподілена мережа корпоративна, яка використовує Інтернет для передавання даних та спеціальні технології захисту каналів зв’язку між своїми вузлами. Таким чином, в Інтернеті створюється захищена піл.мережа, між абонентами якої

організований захищений (конфіденційний, цілісний) зв'язок. Такі захищені канали найчастіше реалізуються за допомогою методів захисту криптографічних інформації, зокрема, застосуванням шифраторів IP-пакетів.

privilege – повноваження # право суб'єкта доступу (користувача або процесу) на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів.

privilege – привілей # авторизація, що надається ідентифікованому користувачу на використання певної послуги керування даними для доступу до особливих даних або процесів.

privilege list – перелік #

privileged user – привілейований користувач # користувач обчислювальної системи, який має порівняно з іншими користувачами більші права і привілеї при роботі з системою обчислювальною (наприклад, більш високий пріоритет).

PRMD – private management domain – приватний домен керування.

probabilistic algorithm – ймовірнісний алгоритм # який крім входу w(n) отримує випадкову двійкову послідовність $r \in 0,1^{1(n)}$, далі працює як звичайний детермінований алгоритм та подає на вихід правильний зв'язок із ймовірністю не менше ніж $1 - \epsilon$, де ϵ – похибка ймовірнісного алгоритма.

probability – ймовірність # математична числова характеристика ступеня можливості появи якої-небудь випадкової події при тих чи інших визначених умовах, що можуть повторюватися необмежену кількість разів.

probability process – імовірнісний процес # випадковий процес # див. random process, stochastic process.

probe – зондування # попереднє обережне вияснення чого-небудь і кого-небудь; розвідування.

problem – проблема # складне теоретичне або практичне питання, що потребує розв'язання, вивчення, дослідження.

problem –# 1. питання, яке розв'язується шляхом обчислень за визначеною умовою # 2. основна одиниця роботи обчислювальної системи, яка потребує виділення ресурсів.

problem comment – коментар проблемний # коментар, який розглядає важливе для слухачів питання, досліджує широку панораму подій, дії уряду або командування противника, глибоко аналізує факти.

problem of intellectual counteraction – завдання інтелектуальної протидії # комплекс завдань інтелектуальної протидії в мережах обміну інформацією, вирішення яких спрямоване на досягнення мети інформаційної боротьби. Якщо інтелектуальна протидія, заснована на впровадженні об'єкта атаки хибного, то формулюються чотири основні завдання інтелектуальної протидії: завдання класифікації

несанкціонованого доступу; завдання вибору виду інформаційної протидії; завдання вибору зони інтелектуальної протидії; завдання здійснення інтелектуальної протидії за допомогою хибного об'єкта атаки.

problem space – проблемний простір # концептуальна чи формальна область, визначена усіма можливими станами, які можуть застосовуватися під час аналізі взаємодій між елементами та операціями, що розглядаються під час вирішенні конкретної задачі чи проблеми.

procedural fraud – процедурне шахрайство # неправомочне використання роумінгу та інших бізнес-процедур (наприклад білінгу) з метою зменшення оплати послуг зв'язку.

procedural security – процедурна безпека # адміністративні заходи з комп'ютерної безпеки # цими заходами можуть бути операційні та підзвітні процедури, процедури розслідування порушень в області безпеки, а також огляду контрольних журналів.

procedure – процедура # офіційно встановлений чи прийнятий за звичаєм порядок, послідовність дій для здійснення або оформлення якихось справ.

procedure of access to classified material – процедура допуску до державної таємниці # офіційно встановлений порядок, послідовність дій для здійснення допуску посадової особи або громадянина до таємниці державної. Як правило така процедура передбачає: прийняття на себе зобов'язань перед державою за нерозповсюдже- ння довірених їм відомостей, що складають державну таємницю; згоду на часткові, тимчасові обмеження їхніх прав у відповідності до закону; письмова згода на проведення по відношенню до них повноважними органами перевірочних заходів; визначення видів, розмірів і порядку надання пільг, передбачених законом; ознайомлення з нормами законодавства держави про державну таємницю, які передбачають відповідальність за його порушення; прийняття рішення керівником органу державної влади, підприємства, закладу або організації про допуск особи, що оформляється, до державної таємниці.

procedure of access to secret clearance – процедура допуску до державної таємниці # див. procedure of access to classified material.

procedure of confirmation of data characteristics in telecommunication systems – процедура підтвердження характеристик даних в телекомунікаційних системах # процедура, яка передбачає наявність арбітра, який є довіреною особою взаємодіючих абонентів і може підтвердити цілісність, час передавання документів, а також запобігти можливості відмови джерела від видачі будь-якого повідомлення, а споживача – від його приймання.

procedure of ensuring integrity of data in telecommunication systems – процедура забезпечення цілісності даних в телекомунікаційних системах # процедура, яка передбачає введення в кожне повідомлення деякої додаткової інформації, яка є функцією від змісту повідомлення. В рекомендаціях МОС розглядаються методи забезпечення цілісності двох типів: перші забезпечують цілісність поодинокого блока даних, інші – цілісність потоку блоків даних або окремих полів цих блоків. При цьому забезпечення цілісності потоку блоків даних не має сенсу без забезпечення цілісності окремих блоків. Ці методи застосовуються в двох режимах – при передаванні даних по віртуальному з'єднанню і при використанні дейтаграмного передавання. В першому випадку виявляються невпорядкованість, втрати, повтори, вставки даних за допомогою спеціальної нумерації блоків або введенням міток часу. В дейтаграмному режимі мітки часу можуть забезпечити тільки обмежений захист цілісності послідовності блоків даних і запобігти переадресуванню окремих блоків.

procedure of filling flow in telecommunication systems – процедура заповнення потоку в телекомунікаційних системах # процедура, призначена для запобігання аналізу трафіка. Ефективність застосування цієї процедури підвищується, якщо одночасно з нею передбачене лінійне шифрування всього потоку даних, тобто потоки інформації і заповнення стають нерозбірливими.

procedure of managing access to resources of telecommunication system – процедура керування доступом до ресурсів телекомунікаційної системи # процедура, що виконується на основі множини правил і формальних моделей, що використовуються як аргумент доступу до інформації про ресурси (класифікацію) та ідентифікатори абонентів. Службова інформація для керування доступом (паролі абонентів, списки дозволених операцій, персональні ідентифікатори, часові обмежувачі і т. ін.) містяться в локальних базах даних забезпечення безпеки мережі.

procedure of route management in telecommunication system – процедура керування маршрутом в телекомунікаційній системі # процедура, призначена для організації передавання тільки маршрутами, утвореними за допомогою надійних і безпечних технічних засобів і систем. При цьому може бути організований контроль з боку одержувача, який у випадку виникнення підозри про компрометацію використовуваної системи захисту може вимагати зміну маршруту.

process – процес # *1.* сукупність взаємопов'язаних або взаємовпливових дій, що перетворює

вхідні дані на вихідні # 2. активний компонент інформаційної системи

process – процес # послідовність передбачених подій, яка визначається об’єктом або явищем і відбувається в заданих умовах; хід подій, що відбуваються у відповідності з наміченою метою або результатом.

process object – об’єкт-процес # програма, що виконується у даний момент часу, яка повністю характеризується своїм контекстом # поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т. ін.

processing linkage – процес з’єднання # надання можливої взаємодії між процесами.

processor – процесор # поняття моделювання, що представляє певну комбінацію апаратного та програмного забезпечення, що може надавати послуги одному або кульком процесорам або людині-користувачу.

procuring – добування #дія, спрямована на діставання, роздобування кого-що-небудь.

product object – об’єкт комп’ютерної системи # елемент ресурсу системи комп’ютерної, що знаходиться під керуванням комплексу засобів захисту і характеризується певними атрибутами й положенням. При розгляді взаємодії двох об’єктів комп’ютерної системи, що виступають як приймачі або джерела інформації, виділяють об’єкт пасивний, над яким виконується операція, і активний об’єкт, який виконує або ініціює цю операцію. Розглядаються такі типи об’єктів комп’ютерної системи: об’єкти-користувачі, об'єкти-процеси і пасивні об’єкти. Поняттю «суб’єкт» часто відповідає суперпозиція об’єкта-користувача й об’єкта-процесу. Об’єкти- користувачі і об’єкти-процеси є такими тільки всередині конкретного домену. В інших доменах об’єкти залишаються в пасивному стані. Це дозволяє одному об’єкту-процесу керувати іншим об’єктом-процесом або навіть об’єктом-користувачем, оскільки останній залишається «пасивним» з точки зору керуючого об’єкта. Пасивний об’єкт переходить в стан об’єкта-користувача, коли індивід (фізична особа) «входить» в систему. Цей об’єкт-користувач виступає для комплексу засобів захисту як образ фізичного користувача. За цим процесом іде активізація об’єкта-процесу за ініціативою користувача. Цей об’єкт-процес є керуючим для пасивних об’єктів усередині домену користувача. Взаємодія двох об’єктів комп’ютерної системи (звернення активного об’єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об’єктами і (або) зміни стану системи.

products – продукція # сукупність продуктів діяльності, виробництва.

profile – профіль # 1. обриси будь-чого збоку # 2. сукупність основних типових рис будь-чого.

profile list – перелік повноважень# перелік об'єктів з зазначенням прав доступу з боку користувача або процесу, з яким пов'язаний цей перелік.

program authorization – авторизація програми # установлення обмежень на доступ до системної програми або програми користувача з боку інших програм і користувачів.

program bug – програмна закладка # потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері.

program check – контроль програмний # вид контролю функціонального, що здійснюється за допомогою програмних засобів. К. п. поділяється на програмно-логічний, алгоритмічний і тестовий.

program compatibility – сумісність програмна # можливість використання програм в АСОІ різних рівнів і різного функціонального призначення.

program document – програмний документ # документ, який містить відомості, необхідні для розробки, виготовлення, експлуатації і супроводження забезпечення програмного.

program specification – специфікація програми # точне й повне формулювання задачі, що містить інформацію, необхідну для побудови алгоритму (програми) вирішення цієї задачі.

program validation – атестація програми # авторитетне підтвердження якості програми на основі загальноприйнятої або офіційної процедури; комплекс перевірок, що забезпечує одержання гарантії відповідності програми своєму призначенню.

program viability – живучість програмного виробу # показник якості програмного виробу, що характеризує його здатність зберігати нормальне функціонування при машинних збоях або частковому виході обладнання з ладу.

program worm – програмний черв'як # програмна закладка, що маскується під системні засоби пошуку вільних обчислювальних ресурсів в мережі.

programed-logic check – програмно-логічний контроль # контроль програмний, найбільш розповсюджена форма якого ґрунтується на подвійному обрахунку з порівнянням одержаних результатів. Програмно-логічний контроль дозволяє надійно виявляти збої, і для його здійснення не потрібно додаткового обладнання. Проте при цьому більш ніж вдвоє знижується продуктивність ЕОМ, не виявляються систематичні збої, неможливо вказати місце відмови або збою, потрібна додаткова ємність пам'яті для програми обчислень.

programmable breakpoint – програмована точка переривання # точка переривання, яка автоматично викликає попередньо зазначений процес налагодження під час ініціюванні.

programmatic check authenticity – контроль достовірності програмний #

метод контролю достовірності оброблення інформації на основі реалізації додаткових операцій, що мають математичний або логічний зв'язок з алгоритмом оброблення даних. Порівняння результатів цих додаткових операцій з результатами оброблення даних дозволяє встановити з певною ймовірністю наявність або відсутність помилок.

programming language – мова програмування #формалізована мова, призначена для опису алгоритмів вирішення задач на ЕОМ.

program-sensitive fault – програмочутливий збій # може бути виявленим внаслідок виконання певної послідовності команд.

prohibited area – заборонена зона # район або місцевість, куди нелегко проникнути і де важко організувати збирання відомостей розвідувальних. Заборонена зона – частина країни, куди закритий доступ іноземним дипломатам, а отже, і представникам іноземних спеціальних служб, що діють під дипломатичним прикриттям. Відомості із з. з. поступають в іноземні спеціальні служби від нелегалів, накопичуються в результаті непрямого спостереження (допити біженців, перебіжчиків і т. ін.), а також в ході ведення розвідки космічної і радіоелектронної.

project – проект # 1. сукупність документів (розрахунків, креслень тощо), необхідних для виготовлення виробу, зведення споруд тощо # 2. попередній, гаданий текст будь-якого документа # 3. план, задум організації, влаштування, заснування будь-чого.

proof – доведення # див. proving.

proof of correctness – доказ правильності # докази, які є результатом від застосування доведення правильності.

proofness – захищеність # див. protectability, immunity.

property – власність # належність чогось кому-, чому-небудь із правом розпоряджатися.

proprietary – власність # див. property.

protectability – захищеність # здатність до оборони, охорони когось, чогось від нападу, замаху, удару, ворожих дій і т. ін.

protectability of automated system – захищеність автоматизованої системи # здатність системи автоматизованої протистояти доступу несанкціонованому до інформації, а також її випадковому спотворенню або руйнуванню. Захищеність автоматизованої системи є змінною величиною, залежить вид багатьох факторів і повинна підтримуватися на усіх етапах життєвого циклу системи. Для забезпечення захищеності використовується велика кількість методів, які умовно поділяють на три основні групи: керування доступом до інформації; резервування інформації та інших ресурсів; приховування (в тому числі криптографічними та стеганографічними методами).

protectability of information – захищеність інформації # забезпечення цілісності, конфіденційності і доступності інформації. З.і. досягається забезпеченням захисту інформації від несанкціонованої змінювання, від несанкціонованого одержання, від несанкціонованого утримування.

protected object attestation – атестація захищеного об’єкта # офіційне підтвердження наявності на захищеному об’єкті необхідних і достатніх умов, які забезпечують виконання встановлених вимог керівних документів і норм ефективності захисту інформації.

protecting presentation context – захист контексту відображення # контекст відображення, який пов'язує захист синтаксису передавання з абстрактним синтаксисом.

protecting transfer syntax – захист синтаксису передавання # синтаксис передавання на основі процесів кодування/декодування, які використовують перетворення захисту.

protection – охорона # захист # див. guard, guarding, lock out.

protection against compromising emanation – захист від побічного електромагнітного випромінювання і наведень # захист, що здійснюється, якщо рівень сигналу на межі встановленої зони перевищує допустимі для перехоплення випромінювання або наведення значення. Захисні заходи можуть носити різноманітний характер в залежності від складності, вартості і часу, витраченого на їхню реалізацію. Такими заходами можуть бути: доопрацювання апаратури з метою зменшення рівня сигналів, встановлення спеціальних фільтрів, паралельно працюючих апаратних генераторів шуму, спеціальних екранів та інші заходи. Суттєвим заходом є використання в каналах і лініях зв’язку волоконно-оптичних систем передавання, в яких відсутнє електромагнітне випромінювання.

protection certificate – сертифікат захисту # документ, що засвідчує відповідність засобів обчислювальної техніки або автоматизованої системи набору вимог по захисту від несанкціонованого доступу до інформації і дає право розробникові використовувати або розповсюджувати їх як захищених.

protection class – клас захищеності # певна сукупність вимог із захисту засобів обчислювальної техніки (автоматизованої системи) від несанкціонованого доступу до інформації.

protection exception – виняткова ситуація у захисті; виняток у захисті # виняток, що виникає, коли програма намагається отримати доступ до захищеної області на пристрої зберігання даних.

protection from unauthorized access – захист від несанкціонованого доступу # 1. попередження або суттєве утруднення доступу несанкціонованого до інформації (програм та даних) шляхом

використання апаратних, програмних і методів криптографічних та засобів захисту, а також проведення організаційних заходів. Найбільш розповсюдженим програмним методом захисту є система паролів # 2. діяльність, спрямована на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів захисту інформації.

protection group administrator – адміністратор групового доступу # особа, права якої в рівній мірі належать декільком користувачам.

protection information level – рівень захисту інформації # сукупність вимог, у тому числі нормованих, що визначаються режимом доступу до інформації та загрозами її безпеці.

protection key – ключ захисту # код, який присвоюється програмі і повинен збігатися з ключами захисту пам'яті всіх блоків, що виділені програмі.

protection level certification – сертифікація рівня захисту # процес установлення відповідності засобу обчислювальної техніки або автоматизованої системи набору певних вимог по захисту.

protection lock – замок захисту # програмний механізм перевірки паролів при зверненні до бази даних або до її фрагментів (файлів, областей), що забезпечує обмеження доступу до записів.

protection mechanism model – модель механізму захисту # див. security mechanism model.

protection method – метод захисту # система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним (апаратно-програмним) або апаратним методом.

protection model – модель захисту # абстрактний (формалізований або неформалізований) опис комплексу програмно-технічних засобів і (або) організаційних заходів захисту від несанкціонованого доступу.

protection of computer systems – клас захищеності засобів обчислювальної техніки # характеристика засобів обчислювальної техніки, що впливають на захищеність і описуються певною групою вимог, що варіюються за рівнем і глибиною в залежності від класу захищеності.

protection of consumers – захист прав користувачів # сукупність правил, методів і засобів, спрямованих на забезпечення безперешкодного та своєчасного доступу користувачів до програм і даних та захист їхньої інформації від використання іншими особами.

protection of intellectual property – захист інтелектуальної власності # проблема, що постає перед авторами текстів, які без дозволу піддаються мультимедійним перетворенням і розповсюдженню по супермагістралям інформаційним або у формі піратських дискозаписів,

коли множина операторських маніпуляцій стирає видимі межі власності інтелектуальної і встановлення на неї юридичних прав ускладнюється.

protection of state secrets – захист державної таємниці # сукупність заходів, спрямованих на забезпечення захисту відомостей, що складають державну таємницю, і їхніх носіїв у відповідності до чинного законодавства. *3.* д. т. потребує створення потужних механізмів, насамперед організаційних структур.

protection profile – профіль захисту # спеціальний нормативний документ, що регламентує сукупність завдань захисту, функціональних вимог безпеки, вимог гарантій безпеки та їхнього обґрунтування. Профіль захисту визначає вимоги безпеки до певної певної категорії продуктів інформаційної технології, не уточнюючи методи й засоби їхньої реалізації. За допомогою п. з. споживачі формують свої вимоги до розробників ІТ-продуктів. Профіль захисту містить вступ, опис ІТ-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, додаткові відомості, обґрунтування. Він служить керівництвом для виробника і розробника ІТ-продукту, які повинні на його основі і технічних рекомендацій, що запропоновані ним, розробити проект захисту, який служить керівництвом для аналізу кваліфікаційного і сертифікації ІТ-продукту.

protection stability – стійкість захисту # імовірність неподолання захисту порушником за певний проміжок часу.

protocol – протокол # *1.* сукупність чітких правил, які визначають організацію взаємодії і обміну даними між окремими процесами # *2.* набір правил і форматів (семантичних і синтаксичних), які обумовлюють поведінку зв’язку логічних об’єктів при виконанні своїх функцій.

protocol converter – конвертер протоколів # пристрій чи програма, що здійснює транслювання між різними протоколами, які обслуговують схожі функції.

protocol data unit – протокольний блок даних # набір даних, заданих у протоколі заданого рівня й що складено з протокольної Керувальної інформації цього рівня й, можливо, даних користувача цього рівня.

protocol stack – протокольний стек # стек протоколів # ієрархічно впорядкована група протоколів зв’язку, на кожному рівні якої відповідний протокол визначає функціональність і режим роботи, і які сумісно підтримують множину мережних функцій.

protocol-addressing-information – протокольна адресна інформація # елементи протокольної контрольної інформації, що містять адресну інформацію.

prototype – прототип # модель або попередня реалізація, що підходить для оцінки конструкції системи,

продуктивності та виробничого потенціалу, чи для кращого розуміння чи визначення вимог.

provider – провайдер # організація, що надає послуги доступу до Інтернету. Умови підключення визначаються договором, що укладається з користувачем.

proving – доведення # *1.* дія за значенням довести, доводити # *2.* логікова форма встановлення істинності будь-якого судження на підставі інших суджень, істинність яких перевірена практикою.

provocation – провокація # навмисні дії проти окремих осіб, організацій, розвідувальних служб або урядів країн тощо з метою підбурити їх на згубні для них учинки або рішення. Агент-провокатор, як правило, вдається до розповсюдження фальшивих відомостей, дезінформації.

proxy server – **1.** сервер-посередник # **2.** повноважний сервер, проксі-сервер # програма-посередник, яка діє як клієнт, і як сервер з метою здійснення запитів від імені інших клієнтів, і яка обслуговує ці запити або пересилає їх після трансляції до інших серверів, при цьому інтерпретує і, якщо треба, перезаписує повідомлення запиту перед його спрямуванням до іншого сервера.

pseudonym – псевдонім # кличка або символічне позначення, яке присвоюється розвідникові або агентові з метою забезпечення безпеки його листування або переговорів з керівним центром (на випадок перехоплення повідомлення противником).

pseudoprime number – псевдопросте число # число складене, яке не визначається тестом на простоту ймовірнісним.

pseudorandom generator – псевдовипадковий генератор # див. random sequence generator.

PSTN – public switched telephone network – телефонна мережа загального користування.

psychological operations object – об’єкт психологічних операцій # об’єкти психологічної війни у вузькому розумінні цього поняття. Це конкретні люди: особовий склад цих чи інших військових підрозділів противника; персонал органів управління й забезпечення; службовці об’єктів соціально-економічноїінфраструктури (залізничних, дорожніх, авіаційних, портових вузлів і споруд); напевно, визначені категорії населення (наприклад, національні, релігійні та інші меншини). В залежності від характеру воєнної, політичної, економічної ситуації об’єкти психологічних операцій можуть мінятися й уточнюватися. Так, в оборонній операції ними можуть бути: частини (підрозділи) першого ешелону військ, що ведуть наступ; особовий склад підрозділів, оточених в результаті проведення контратак; особовий склад тактичних десантів, що діють в смузі оборони з’єднання.

psychological warfare – орган психологічної війни # орган керування війною психологічною і люди (фахівці, офіцери, військові підрозділи) для її ведення. Орган психологічної війни повинен бути здатним до швидкого розгортання, оперативного слідкування за обстановкою в різноманітних регіонах, спроможним до виконання поставлених завдань в будь-яких умовах. На озброєнні органу психологічної війни знаходяться різноманітні види засобів психологічної війни технічних.

psychological warfare object – мета психологічної війни # 1.зміна в бажаному напрямку психологічних характеристик людей (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому # 2.спотворення інформації, що одержується політичним керівництвом, командуванням і особовим складом збройних сил противника, і нав'язування їм фальшивої або беззмістовної інформації, яка позбавляє його можливості правильно сприймати події або поточну обстановку і приймати правильні рішення. Мета психологічної війни призводить до вирішення наступних головних завдань: запобігання можливого воєнного конфлікту; ослаблення морального духу особового складу збройних сил і цивільного населення противника; схилення його до відмови від участі в бойових діях; створення передумов для досягнення намічених воєнно-політичних цілей з мінімальними людськими втратами і матеріальними затратами. Мету і завдання психологічної війни можна класифікувати і уточнювати відповідно до умов ведення психологічної війни (мета і і завдання психологічної війни у мирний, воєнний і післявоєнний час, а також в ході миротворчих операцій), об'єктів психологічної війни (військовослужбовців, цивільного населення, вищого воєнно-політичного керівництва противника і його союзників, а також світової суспільної думки і країн-союзників), часу ведення психологічної війни (стратегічні, оперативні, тактичних).

psychological warfare object – об'єкт психологічної війни # особовий склад і все цивільне населення противника, а також союзних йому держав.

psychological warfare objects studying method – метод вивчення об'єктів психологічної війни # система методів, що використовується для вивчення об'єктів психологічної війни. До методів вивчення об'єктів психологічної війни відносять методи спостереження, експерименту, опитування, вивчення документів, радіоперехоплення, узагальнення незалежних характеристик, узагальнення

соціологічної і і психологічної статистики.

psychological warfare objects studying methods – методика вивчення об'єктів психологічної війни # сукупність взаємозв'язаних принципів, методів і організаційних заходів реалізації складного й довготривалого процесу збирання, оброблення і накопичення інформації про об'єкти психологічної війни.

public communication network – мережа зв'язку загального користування # складова частина взаємозв'язаної мережі зв'язку держави, відкрита для користування всім фізичним і юридичним особам, в послугах якої цим особам не може бути відмовлено.

public data – дані колективного користування # загальнодоступна інформація: дані, доступні великій кількості користувачів як у пакетному, так і в інтерактивному режимах.

public key – відкритий ключ # ключ, призначений для виконання перетворення криптографічного будь-яким елементом криптосистеми асиметричної. Обернене криптографічне перетворення може бути виконано тільки з застосуванням відповідного ключа приватного.

public key certificate – сертифікат відкритого ключа # див. certificate.

public key cryptography – шифрування з відкритим ключем # криптографічний метод, в якому використовуються окремі ключі для зашифровуванняі розшифровування.

public key cryptography – шифрування із відкритим ключем # криптографія, в якій для шифрування та дешифрування застосовується відкритий ключ і відповідний приватний ключ. Якщо для шифрування застосовується відкритий ключ, для розшифрування застосовується відповідний приватний ключ, і навпаки.

public relations in the field of information security – суспільні відносини в галузі інформаційної безпеки # відносини у суспільстві при створенні і застосуванні механізмів захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері. Ці відносини зв'язані з цілим рядом прав, обмежень, обов'язків та відповідальністю: із правом на захист держави і суспільства від впливу недостовірної, хибної інформації; із правом на захист інформації документованої, ресурсів інформаційних та продукції інформаційної як речової власності; із правом на захист інформації та інших нематеріальних об'єктів як інтелектуальної власності; із правом на захист систем інформаційних, технологій інформаційних і засобів їхнього забезпечення як речової власності; із правом на захист особистості в умовах інформатизації; із обмеженням права на розкриття особистої таємниці, а також іншої

інформації обмеженого доступу без санкцій її власника; із обов'язками – захисту держави і суспільства від шкідливого впливу інформації, захисту самої інформації, захисту прав особистості, захисту таємниці (особистої, державної і т.ін.); з відповідальністю – за порушення прав і свобод особистості, за порушення таємниці та інших обмежень доступу до інформації, за злочини комп'ютерні.

public resources – загальнодоступні ресурси # ресурси, доступ до яких не обмежений.

public-key cryptosystem – *криптосистема з відкритим* ключем # криптосистема, в якій використовується два ключі - секретний (приватний) і відкритий, причому ні один із ключів не може бути обчислений з іншого за певний час. Секретний ключ тримається в таємниці, в той час як відкритий ключ може бути розісланий всім абонентам, з якими здійснюється взаємодія. Користуючись відкритим ключем будь-який з абонентів може послати захищене повідомлення авторові відкритого ключа. При цьому розшифрувати це повідомлення можна тільки секретним ключем, який відповідає відкритому. Такі криптосистеми називають також двоключовими або асиметричними. Вони засновуються на так званих важкооборотних (односторонніх, односпрямованих) функціях та забезпечують тільки практичну стійкість. Одним з основних застосувань криптосистему з відкритим ключем є керування ключами та створення електронного цифрового підпису.

PVN – private virtual network – приватні віртуальні мережа

Q

QA – quality assurance – гарантування якості.

QoS – quality of service – якість обслуговування.

QoS profile – профіль якості обслуговування # сукупність параметрів якості обслуговування, які визначають вимоги до ефективності мережі переносу інформації у конкретному сеансі зв'язку.

qualification – кваліфікація # засоби для посилання на мовні конструкції в рамках частини програми щодо тієї частини ідентифікатора, який оголошений для мовної конструкції в цій частині # наприклад застосовується для посилань на компоненти запису (B OF A в COBOL), члени бібліотеки, мовні конструкції в модулі.

quality assurance – гарантування якості # заплановані систематичні заходи, що необхідні для забезпечення того, щоб компонент чи система відповідали встановленим технічним вимогам.

quality of service – якість обслуговування # оцінка ступеня задоволення споживача мережними сервісами.

quantum cryptography – квантова криптографія # галузь криптографії, що вивчає криптографічні перетворення інформації на основі принципу невизначеності квантової механіки.

questioning – опитування # див. polling, inquiry.

questionnaire – анкета # лист для опитування, який самостійно заповнюють опитувані за вказаними в ньому правилами. Анкетні опитування широко використовують для одержання інформації про фактичний стан речей в галузі, яку вивчають, їхній оцінці, поглядах, інтересах і мотивах діяльності опитуваних (респондентів).

quota – квота # *1.* частка, частина, певна норма # *2.* обмеження можливості використання певного ресурсу системи комп'ютерної користувачем або процесом.

R

radar concealment – радіолокаційне # комплекс організаційно-технічних заходів, здійснюваних з метою перешкодити визначенню радіолокаційною станцією противника складу і дислокації об'єктів, а також зниження дальності дії по них радіолокаційної станції противника. Радіолокаційне маскування застосовують також для введення противника в оману шляхом створення фальшивих цілей для його радіолокаційної станції спостереження. Базується на обмеженій роздільній здатності радіолокаційної станції та на використанні різних штучних відбивачів, які на екранах радіолокаційної станції дають відмітки, що мало відрізняються від відміток об'єктів, які маскуються.

radar contrast – радіолокаційна контрастність # різниця у відбитті радіохвиль яким-небудь окремим об'єктом і оточуючими його предметами та фоном. Радіолокаційна контрастність цілі залежить від ступеня її відбивної здатності в порівнянні з фоном.

radar image – радіолокаційне зображення # образ об'єкта, який одержують на різних пристроях індикації при добуванні інформації активними радіолокаційними засобами. Радіолокаційне зображення місцевості одержують за допомогою панорамних радіолокаційних станцій та радіолокаційних станцій бічного огляду.

radiator – випромінювач # *1.* пристрій, за допомогою якого здійснюють випромінювання # *2.* випромінюючий елемент антени, зв'язаний з фідером.

radio – радіо # частина складних слів, що вказує на зв'язок із поняттям «радіо» або «радіоактивність».

radio [electronic] warfare – боротьба радіоелектронна # комплекс взаємопов'язаних заходів та дій з виявлення і подальшого придушення радіоелектронного або знищення засобів радіоелектронних та систем противника, а також відповідного

захисту своїх радіоелектронних засобів та систем.

radio concealment – радіотехнічне маскування # маскування дійсної дислокації радіопередавальних пристроїв, здійснюване для зниження ефективності радіорозвідки противника. Радіотехнічне маскування здійснюють шляхом скорочення часу роботи на передавання, випромінювання мінімально необхідної потужності, використання спрямованого передавання, зміни робочих частот, встановлення режиму радіомовчання (повного припинення роботи на передавання), використання раді од езінформації.

radio direction finder – радіоперехоплювач # радіоприймач # радіотехнічний приймально-індикаторний пристрій для визначення радіопеленга (пеленга) на джерела випромінювання електромагнітного. Основу р. складає радіоприймач з антеною, діаграма спрямованості якої має гострий максимум або мінімум. Обертаючи антену в напрямку досягнення максимуму (мінімуму) сигналу на виході антени, визначають напрямок на джерело радіовипромінювання.

radio electronic protection – радіоелектронний захист # сукупність заходів забезпечення стійкої роботи засобів управління і розвідки в умовах ведення противником боротьби радіоелектронної, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

radio frequency emission – радіовипромінювання # радіочастотне випромінювання # див. radio frequency emission.

radio frequency emission – радіочастотне випромінювання # електромагнітні коливання (хвилі) в діапазоні радіочастот, що поширюються (випромінюються) в просторі.

radio interception complex – комплекс засобів радіоперехоплення # сукупність організаційно, функціонально та конструктивно взаємопов’язаних засобів, призначених для виявлення, приймання та реєстрації радіовипромінювання і добування з них семантичної інформації, ознак сигналів демаскуючих і формування зображень об’єктів при перехопленні сигналів телевізійних або факсимільних. Типовий комплекс засобів радіоперехоплення охоплює: приймальні антени; радіоприймач; аналізатор технічних характеристик сигналів; радіопеленгатор; пристрої реєструючі.

radio interruptions – радіозавади #радіосигнали, що ускладнюють або зовсім порушують роботу радіотехнічних засобів, систем радіозв’язку, заважають розбірливості та якості звукового прийому, створюють порушення телевізійного і радіолокаційного зображення, спотворюють телеграфні

знаки і т.ін. В залежності від походження завади можуть бути природні і штучні, навмисні і ненавмисні.

radio misinformation – радіодезінформування # навмисне перекручення повідомлень, що передаються по радіозв'язку, з метою створення у користувачів цих повідомлень хибного уявлення. Р. використовується для введення противника в оману шляхом передавання фальшивих повідомлень, перекручень дійсного режиму роботи та розташування випромінюючих засобів радіоелектронних за рахунок уведення в дію фальшивих станцій, посилення роботи передавальних радіоелектронних засобів на другорядних напрямках при збереженні попереднього або скороченні режиму їхньої роботи на головному напрямку і т.ін.

radio receiver selectivity – вибірковість радіоприймача # здатність радіоприймача виділяти корисний сигнал із сигналів різноманітних частот, що приймаються антеною. Вибірковість радіоприймача оцінюють двома основними показниками: шириною смуги пропускання і коефіцієнтом прямокутності амплітудно-частотної характеристики радіоприймача, реальна форма якої має дзвону ватнії вигляд.

radio transpa rent material – радіопрозорі матеріали # конструкційні діелектрики з двосторонньою провідністю, що пропускають без суттєвих утрат і спотворень електромагнітні коливання радіочастотного діапазону. Призначаються в основному для виготовлення обтічників, що захищають антени радіолокаційних станцій та інші радіотехнічні засоби від впливу навколишнього середовища.

radio-absorbing material – радіопоглинальні матеріали # неметалічні матеріали, які в результаті взаємодії з радіохвилями здійснюють їхнє поглинання, розсіювання і інтерференцію. У відповідності до принципів дії радіопоглинальні матеріали поділяють на градієнтні (поглинальні), інтерференційні і комбіновані. Застосовуються для маскування від радіолокаційного виявлення різноманітних об'єктів; екранування радіоприймальних пристроїв; обладнання спеціальних камер, в яких випробовуються радіоелектронні засоби; біологічного захисту від впливу потужного радіовипромінювання. Розрізняють широкодіапазонні і вузькодіапазонні радіопоглинальні матеріали. Широкодіапазонні матеріали ефективно поглинають електромагнітну енергію при відношенні максимальної до мінімальної довжини падаючої хвилі *3-5*; вузькосмугові, якщо це відношення не перевищує *1,5-2*. В ряді випадків знаходять застосування

матеріали, що працюють практично тільки на фіксованій хвилі.

radiodate – радіодані # частоти, пакети частот, індекси, паролі, позивні адресні коди радіостанцій.

radioelectronic concealment – радіоелектронне маскування # комплекс технічних та організаційних заходів, спрямованих на зниження ефективності розвідки радіоелектронної противника. Радіоелектронне маскування поділяють на маскування радіотехнічне, радіолокаційне, гідроакустичне і оптико-електронне.

radio-frequency – радіочастота # радіодані # див. radiodate.

radiointerseption – радіоперехоплення # перехоплення інформації шляхом виявлення, приймання та реєстрації радіовипромінювання з метою подальшого розкривання змісту повідомлень, які передаються за допомогою різноманітних засобів радіозв'язку; спосіб радіорозвідки.

radio-locating characteristics of objects – радіолокаційні характеристики об'єктів # характеристики, що визначають можливість виявлення, розпізнавання цілей і вимірювання параметрів їхнього руху засобами радіолокації. Основною радіолокаційних характеристик об'єктів є здатність цілі відбивна (інтенсивність відбитого сигналу), яка залежить від геометричних розмірів, конфігурації, матеріалу, ракурсу цілі, довжини хвилі РЛС і виду поляризації електромагнітних хвиль. Практична неможливість врахування усіх перелічених факторів привела до необхідності введення спеціальної розрахункової величини – поверхні розсіювання ефективної цілі (об'єкта), яка враховує відбивні властивості реальних цілей (об'єктів) складної форми (літаки, кораблі, штучні відбивачі і

radioreflectors – радіовідбивачі # засоби приховування інформаційного об'єктів радіолокаційного спостереження. До радіовідбивачів відносять кутові, лінзові, дипольні та перевипромінюючі антенні решітки. Відбивачі кутикові, лінзові, перевипромінюючі антенні решітки, розташовані поблизу об'єкта, що потребує захисту, створюють на екрані РІІС багаточисельні яскраві засвітлення, серед яких важко виявити сам об'єкт. Для маскування повітряних об'єктів застосовують відбивачі дипольні.

radiotransparent masks – радіопрозорі маски # маски оптичні штучні, що виготовляються з радіопрозорих матеріалів (склопластику, пінопласту та ін.), як правило, у вигляді кулі, для прихування демаскуючих ознак і фізичного захисту антен.

RADIUS – remote authentication dial-in user service – сервіс віддаленого автентифікування користувачів по комутованих лініях.

radix – основа системи числення # в системі числення, число, яке зведено в ступінь, позначають через показник, а потім, помножене на мантису, щоб визначити

представлене число # наприклад число 10 у виразі 3,15 x 10^3 = 3150 # в англійській мові термін «radix» застарів у цьому сенсі через його використання в позиційних системах числення.

RAID – redundant array of inexpensive disks – масив недорогих дискових накопичувачів з надлишковістю.

raise – [спричиняти] виняток # спричинення винятку, про що повідомляє виникнення певного стану.

raise statement – оператор винятку # простий оператор, який поширює виняток або викликає його.

random number generator – генератор випадкових чисел # пристрій для одержання послідовності незалежних випадкових чисел із розподілом імовірностей, який є близьким до рівномірного розподілу в інтервалі від 0 до 1, при якому ймовірність попадання випадкової величини в будь-який відрізок, що входить у даний інтервал, дорівнює довжині цього відрізка.

random process – випадковий процес # процес, один або декілька параметрів якого міняються випадково, у відповідності з деяким імовірнісним законом розподілу.

random sequence generator – генератор псевдовипадкових послідовностей # поліноміальний алгоритм G, який випадковий паросток $x \in /0,1/^n$ перетворює у послідовність $G(x) \in /0,1/^{l(n)}$, яка є нерозрізненим ансамблем від випадкової величини, рівно мірно розподіленої на $/0,1/^{l(n)}$.

random signal generator – генератор випадкових сигналів # пристрій, призначений для вироблення сигналів випадкових, величини яких мають цілком визначені ймовірнісні характеристики. Найбільш розповсюджені генератори випадкових сигналів з рівномірним законом розподілу на основі використання фізичних процесів, що мають випадкові характеристики: дробовий ефект, радіоактивний розпад і т.ін. При моделюванні випадкових процесів на ЕОМ випадкові числа з необхідними законами розподілу одержують за допомогою спеціальних пристроїв – датчиків випадкових чисел, що охоплюють генератори випадкових сигналів. Розрізняють датчики випадкових чисел, що використовують джерела фізичних випадкових процесів, а також датчики, які дають псевдовипадкові послідовності.

random-password generator – генератор випадкових паролів # програмно-апаратний засіб, що являє собою генератор випадкових чисел, які використовуються як паролі.

range – діапазон # різниця між найвищим та найнижчим значенням, яке може приймати величина чи функція # див. band, bandwidth.

RAS – remote access service – сервіс віддаленого доступу.

reaction – реакція # дія, стан, процес, що виникають за певних умов у відповідь на будь-які впливи, подразнення, враження.

read protection – захист від читання # заборона звернення до файла для виконання операції читання даних.

real open system – реальна відкрита система # реальна система, що взаємодіє з іншими реальними системами і відповідає стандартам ВВС.

real system – реальна система # сукупність одного чи декількох комп'ютерів, програмного забезпечення, периферійних пристроїв, терміналів, операторів, фізичних процесів, засобів передавання інформації тощо, об'єднаних в одну автономну систему, що здатна обробляти та/чи пересилати інформацію.

real time transport control protocol – протокол керування транспортуванням у реальному часі # протокол зі стеку TCP/IP, який функціонує сумісно з транспортним протоколом реального часу незалежно від протоколів нижчих транспортного і мережного рівнів, і дозволяє контролювати доставку даних, зокрема виявляти приймачам втрати пакетів і компенсувати джитер затримки.

real time transport protocol – транспортний протокол реального часу # протокол з протокольного стеку TCP/IP, який надає застосуванням засоби передавання мультимедійних даних через пакетну мережу у реальному часі з негарантованою якістю обслуговування.

receiver – приймач # апарат для приймання будь-чого (сигналів, мови, музики, зображення) за допомогою електромагнітних, акустичних та інших хвиль. Приймач виконує функцію, зворотні функції передавача. Він здійснює: вибір (селекцію) носія з необхідною для одержувача інформацією; підсилення прийнятого сигналу до значень, необхідних для знімання інформації; знімання інформації з носія (демодуляція, декодування); перетворення інформації в форму сигналу, доступну користувачу (людині, технічному пристрою).

receiver pass пропускання радіоприймача # стот, по краях якої коефіцієнт підсилення радіоприймача від входу до детектора зменшується відносно найбільшої величини у встановлене число разів.

recipient – одержувач # виклик логічного об'єкта, що одержує примітив індикації сервісу рівня, що знаходиться нижче.

recognizable signs – розпізнавальні ознаки # ознаки, що описують об'єкт в статичному стані: його призначення, належність, параметри.

reconfiguration – реконфігурація # модифікація конфігурації функційного блока після виявлення несправності чи помилки з метою запобігання виходу з ладу чи повернення цього функційного блока до стану, у якому він може виконувати необхідну функцію.

reconnaissance – розвідка # зондування # див. intelligence, scouting, surveillance, secret service, probe, sounding.

reconnaissance contact condition – умова розвідувального контакту # умови, за яких стає можливим розвідувальний контакт. Поділяються на просторові, енергетичні і часові.

reconnaissance pilotless vehicle – розвідувальний безпілотний апарат літальний # безпілотний літальний апарат # БПЛА # призначений для ведення стратегічної, оперативної або тактичної повітряної розвідки на сухопутних та морських ТВД. БПЛА поділяються на малогабаритні і крупногабаритні, літакові або вертолітного компонування, ближньої або дальньої дії, багаторазового (більшість) і одноразового використання. БПЛА запускають різними способами: із спеціалізованих пускових установок, за допомогою літаків-носіїв, власними двигунами. Приземлювання БПЛА здійснюють за допомогою парашутів, гальмівних костилів і сіток-вловлювачів. В різних варіантах БПЛА оснащуються фото- і телевізійними камерами, інфрачервоними приладами, засобами радіо- і радіотехнічної розвідки, апаратурою радіоелектронною боротьби. Наведення і управління БПЛА здійснюють наземні центри.

reconnaissanceman – розвідник # див. intelligence agent, secret service man, spy, scout.

record – зафіксувати # зберегти у документованій формі опис процедур, подій, даних спостережень, припущень і результатів на рівні деталізації, достатньому для забезпечення відтворення в майбутньому процесі виконання оцінювання.

recording density – щільність запису # міра кількості бітів, записаних на одиницю довжини або площі.

recover – відновити # встановлення попереднього чи нового статус усієї чи частини системи, файлу, бази даних або іншого ресурсу чи виконання програми таким чином, щоб вона виконувала необхідні функції.

recovery – **1.** відновлення # *1.* повернення до вихідного значення або повернення до нормального функціонування системи після збою або відмови # *2.* процес, за допомогою якого станція передавання даних розв’язує конфлікт або виправляє помилки, що виникають при передаванні даних # **2.** відновлювання # *1.* відновлювання бази даних, наприклад, за допомогою файлів резервних копій та після-зображень # *2.* процес або результат відновлювання # *3.* процес для розв’язання конфліктуючих або помилкових умов, що виникають під час пересилання даних.

recovery function – функція відновлювання # здатність

функційного блока відновити нормальну роботові після відмови.

recovery log – журнал відновлення # журнал, що забезпечує можливість відновлення бази даних або файла. Містить інформацію про всі зміни в базі даних (файлі) з того моменту, коли було встановлено, що дані достовірні і була зроблена остання копія резервна. В загальному випадку ж. в. може бути використаний одним із двох способів: відтворенням усіх змін, зроблених з моменту одержання останньої резервної копії (якщо база даних або файл зруйновані); знищенням усіх неправильних змін (якщо джерело помилок – в самих цих змінах).

recovery time – час відновлювання # при відправленні чи прийманні імпульсів потрібен час між закінченням імпульсу та початком наступного імпульсу. Термін зазвичай застосовується до обладнання, яке надсилає чи отримує імпульси.

recruiting – вербування # залучення окремих осіб у якості агентів таємних.

recruiting online – вербування в Інтернеті # залучення окремих користувачів Інтернету в якості агентів таємних.

recruitment – вербування # див. recruiting.

redundancy – **1.** резервування # надлишковість. Наявність засобів на додаток до засобів, які були б достатні для виконання потрібної функції функційним блок або для даних, що представляють інформацію # наприклад використання копій функційних компонентів, додавання пари бітів. Резервування застосовується в основному для підвищення надійності чи доступності # **2.** надлишковість # сума R, за якої вміст рішення H[нижній індекс 0] перевищує ентропію H; у математичній нотації: R = H[нижній індекс 0] – H. Зазвичай, повідомлення можуть бути представлені меншою кількістю символів за допомогою відповідних кодів; надлишковість може розглядатися як показник зменшення середньої довжини повідомлень, здійснених відповідним кодуванням # наприклад: нехай {a, b, c} буде сукупністю трьох подій і нехай p(a) = 0,5, p(b) = 0,25, а p(c) = 0,25 бути ймовірностями їх виникнення. Надлишковість цього набору становить R = 1,58 Sh – 1,50 Sh = 0,08 Sh.

redundancy – надмірність # перевершеність міри, звичайної норми чого-небудь; надлишковість.

redundancy check – контроль за надмірністю # розпізнавання помилкових комбінацій кодових і виправлення даних за рахунок надмірності.

redundancy of language – надмірність мови # надмірність, зумовлена різними значеннями частоти використання у мові букв, а також суттєво меншою кількістю

дозволених граматикою складів, слів і фраз по відношенню до можливих комбінацій складів, слів і фраз, які теоретично можна скласти з букв алфавіту. У природних мовах наступні одне за другим слова, зв'язані між собою смислом і синтаксисом граматики, а послідовно розташовані букви в межах одного слова – правилами орфографії. Чим більше букв в алфавіті, менше словниковий склад мови і суворіші правила граматики, тим вища надмірність мови.

redundancy protection – захист резервуванням # метод відновлення даних, які зберігаються в зовнішній пам'яті, що полягає у копіюванні на додатковий носій тільки тих файлів, котрі були створені пізніше визначеного строку.

redundant code – надлишковий код # код, згідно з яким більше характеристик, символів або елементів сигналу, ніж строго потрібно, застосовуються для подання даних.

redundant code – надмірний код # 1. код, що має більшу кількість кодових комбінацій, ніж це потрібно для кодування символів повідомлень. Додаткові кодові комбінації можуть використовуватися для контролю правильності передавання даних або для кодування нової інформації # 2. код, комбінації якого містять більшу кількість розрядів, ніж це потрібно для кодування символів алфавіту. Надмірні розряди використовуються для виявлення (виправлення) помилок.

redundant coding – кодування з надмірністю # кодування з допомогою коду надмірного.

reference – характеристика # див. characteristic, description.

referential integrity – цілісність на рівні посилань # властивість набору відношень таких, що значення атрибутів зовнішніх ключів є нульовими значеннями чи ідентичними до значень первинних ключів інших відношень.

reflection surface – ефективна поверхня розсіювання # характеристика відбивної здатності цілі (об'єкта), що опромінюється хвилями електромагнітними Значення ефективної поверхні розсіювання визначається як відношення потоку (потужності) електромагнітної енергії, відбитої об'єктом в напрямку точки приймання, до поверхневої щільності потоку енергії, що падає на ціль. ЕПР об'єкта залежить в основному від розмірів та конфігурації цілі, властивостей її матеріалу, довжини і поляризації хвилі та напрямку опромінювання.

reflective-antenna grid shape – відбиваюча-антенна решітка # радіовідбивач, що має декілька горизонтальних і вертикальних рядів відбивачів дипольних, розташованих в одній площині на відстані чверті робочої довжини хвилі від відбиваючого екрана – металевої пластини. Дипольні пари розташовані дзеркально відносно

центра екрана, з'єднуються між собою відрізками кабелю коаксіального або радіохвилеводу. Відбивні властивості відбиваючої-антенної решітки максимальні в напрямку, перпендикулярному її площині. При орієнтуванні диполів у певному порядкові створюють можливість забезпечення відбивних властивостей решітки незалежно від поляризації радіохвиль, що падають на неї. В деяких конструкціях відбиваючої-антенної решітки замість диполів застосовуються плоскі спіралі, нанесення яких на діелектричний лист здійснюють методом друкованих плат.

reflector # пристрій або природна перепона, що змінює напрямок або інтенсивність світлових або теплових променів, електромагнітних хвиль, ядерних часток, а також твердих пружних тіл.

reflexive code – рефлексивний код # код двійковий, в якому комбінації, що відповідають сусіднім числам, відрізняються тільки в одному розряді.

register – регістр # 1. список, показник будь-чого, книга для записів # 2. ряд клавіш в друкувальних та обчислювальних машинках # 3. в обчислювальній техніці - внутрішній запам'ятовуючий пристрій процесора або адаптера для тимчасового збереження інформації та забезпечення швидкого доступу до неї.

registration – реєстрування # 1. взяття на облік, внесення до списку якихось даних, записів про певні факти # 2. послуга безпеки, що забезпечує збирання і і аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих комплексом засобів захисту # 3. запис інформації на паперовий або інший носій з метою її збереження і наступного використання.

registration authority – реєструючий орган # довірений учасник, який встановлює та/або гарантує ідентичність об'єкту CSP.

registration log – журнал реєстрації # упорядкована сукупність реєстраційних записів, кожний з яких заноситься комплексом засобів захисту за фактом здійснення контрольованої події.

regulation – регламентування # встановлення певних правил.

regulation of access to information – регламентування доступу до інформації # установлення часових, територіальних і режимних обмежень в діяльності співробітників організації і роботі технічних засобів, спрямовані на забезпечення безпеки інформації. Регламентація доступу передбачає: установлення меж зон контрольованих і охоронних; визначення рівнів захисту інформації в зонах; регламентацію діяльності співробітників і відвідувачів (розроблення розпорядку дня, правил поведінки співробітників в організації і поза нею і т. ін.); визначення режимів роботи технічних засобів, в тому числі

збирання, оброблення і зберігання інформації, що потребує захисту, на ПЕОМ, передавання документів, порядку складування продукції і т. ін.

regulations – регламент # звід, система правил, які визначають порядок організації і діяльності органів державної влади в цілому та їхніх складових частин.

relations – відносини # стосунки, зв'язки, взаємини між ким-небудь, контакти.

relative error – відносна похибка # співвідношення абсолютної похибки до істинної, визначеного чи теоретично правильного значення кількості, яка є похибкою.

relative redundancy – відносна надлишковість # співвідношення r надлишковість R до вмісту рішення H[нижній індекс 0]; у математичній нотації: r = R / H[нижній індекс 0]. Відносна надлишковість також дорівнює доповненню до однієї з відносної ентропії H[нижній індекс r]: r = 1 – H[нижній індекс r].

relay – ретрансляція # функція, за допомогою якої логічний об'єкт певного рівня передає отримані дані від одного однорангового логічного об'єкта до іншого однорангового логічного об'єкта.

relay line – радіорелейна лінія зв'язку # лінія зв'язку, що являє собою ланцюжок приймально-передавальних станцій, кожна з яких установлюється в межах прямої видимості іншої. Всі станції радіорелейної лінії зв'язку поділяють на кінцеві, проміжні і вузлові. Кінцеві станції розташовуються на початку і у кінці лінії. На цих станціях уводиться і виділяється інформація, забезпечується розподіл інформації між споживачами. Проміжні станції призначені для ретрансляції сигналів. Вузлові радіорелейні станції – це проміжні станції, на яких здійснюється розгалуження сигналів за різноманітними напрямками, виділення частини інформації, що передається, і введення нової інформації. Діапазон частот, призначений для передавання інформації одного виду, об'єднується в ствол радіочастотний. Для кожного ствола з метою виключення взаємного впливу виділяються дві робочі частоти – для передавання і приймання. Прийняті кожною станцією сигнали на частоті приймання, підсилюються і перетворюються на частоті передавання та випромінюються у напрямку наступної станції.

relaying – ретранслювання # приймання сигналів на проміжному пункті (ретрансляторі), їхнє підсилення і передавання на інший проміжний або кінцевий пункт. Використовується для збільшення дальності зв'язку. Розрізняють ретранслювання з підсиленням і передаванням сигналів у тому ж вигляді, в якому вони були прийняті, та регенеративну ретранслювання – з перетворенням сигналів і виправленням помилок, що

виникають при передаванні. Ретранслювання може здійснюватися із затримкою (сигнал запам’ятовується в спеціальному пристрої і передається в передбачений час).

reliability – надійність # властивість системи зберігати величини вихідних параметрів у межах установлених норм при заданих умовах (забезпечити нормальну роботу системи). Для надійність систем автоматизованих можна виділити окремо надійність апаратури і надійність програмного забезпечення комплексу засобів автоматизації. Проблема надійності для таких систем вирішується наступними шляхами: підвищенням надійності деталей і вузлів; побудовою надійних систем з менш надійних елементів за рахунок структурної надмірності (дублювання, потроєння елементів, пристроїв, підсистем і т. ін.); застосуванням контролю функціонального з діагностикою відмови, що збільшує надійність функціонування системи шляхом скорочення часу відновлення апаратури, що відмовила.

reliability – надійність # здатність функційного блока виконувати необхідну функцію в заданих умовах протягом певного інтервалу часу.

reliable source – надійне джерело # стандартне, активно використовуване джерело розвідувальних відомостей, надійність якого не потребує перевірки.

reliable transfer service element – сервісний елемент надійного пересилання # елемент обслуговування застосунків, який гарантує цілісність блоків протоколу, що обмінюються між парами об'єктів застосунків, які беруть участь в заданій асоціації, і забезпечують відновлювання від пошкоджень системи зв'язку та завершення відкриття системи з мінімальною кількістю повторних передач.

relying party – довіряюча сторона # учасник, який покладається на твердження або претензії ідентичності.

remark – примітка # мовна конструкція, що її застосовують винятково для вмісту тексту, який ніяк не впливає на виконання програми # наприклад пояснення для читачів; дані для автоматичної системи документації.

remote access – віддалений доступ # процес отримання доступу до мережних ресурсів з іншої мережі або з термінального пристрою, що не є постійно з'єднаним фізично або логічно з мережею, до якої він отримує доступ

remote attack – атака віддалена типова # віддалений інформаційний руйнівний вплив, програмно здійснюваний каналами зв’язку та характерний для будь-якої розподіленої обчислювальної системи. Віддаленою може бути будь-яка з типових атак, але характерними для розподілених обчислювальних систем є атака

аналізу трафіка та специфічні методи організації типових атак, наприклад, впровадження фальшивого об'єкта шляхом нав'язування фальшивого маршруту, недоліків алгоритму віддаленого пошуку. Специфічними атаками для мережі Інтернет є атаки шляхом упровадження фальшивих ARP та DNS серверів.

remote attack to network of exchange of information – атака на мережу обміну інформацією віддалена # процес впливу інформаційного (неенергетичного) на інформацію, що зберігають, обробляють й передають в мережі обміну інформацією (МОІ) з метою нанесення збитків і (або) забезпечення умов для нанесення збитків МОІ і (або) її користувачам, що здійснюють канали зв'язку. Виділяють два види віддалених атак – віддалені атаки на інфраструктуру мережі обміну інформацією і протоколи мережі, і віддалені атаки на телекомунікаційні служби. Віддалені атаки можна класифікувати за наступними ознаками: за характером впливу (атаки пасивні, активні і умовно-пасивні); за метою впливу (порушення конфіденційності інформації або інформаційних ресурсів МОІ, порушення цілісності інформації, порушення доступності [працездатності] об'єкта МОІ); за умови початку здійснення впливу (атака за умови запиту об'єкта, що атакується, атака за умови настання очікуваної події на об'єкті, що атакується, атака безумовна); за умови ситуації здійснення впливу (напад інформаційний,[зустрічний] вплив у відповідь на інформаційний напад); за наявністю зворотного зв'язку з об'єктом, що атакується (атака зі зворотним зв'язком, атака без зворотного зв'язку [атака односпрямована]); за розташуванням суб'єкта атаки відносно об'єкта, що атакується (атаки внутрішньосегментні і атаки міжсегментні); за тривалістю впливів (атаки разові, атаки довготривалі); за масштабом впливів (атаки локальні, атаки глобальні [широкомасштабні]); за рівнем моделі взаємодії відкритих систем, на якому здійснюється вплив (атака відповідно на фізичний, канальний, мережі ппї. транспортний, сеансовий, представницький або прикладний рівень). У зв'язку з тим, що віддалена атака реалізується мережною програмою, то найбільш логічно представляти віддалені атаки на МОІ у проекції їх на моделі взаємодії відкритих систем.

remote authentication dial-in user service – сервіс віддаленого автентифікування під'єднаного користувача # система забезпечення захисту мережі і мережних послуг від несанкціонованого віддаленого доступу, яка складається з сервера автентифікування та клієнтських протоколів доступу до нього.

remote data procuring – дистанційне добування інформації # одержання інформації з носіїв, що розповсюджуються за межі зони

контрольованої (приміщення, будівлі, території і т. ін.). Дистанційне добування інформації здійснюють в результаті спостереження, підслухування, перехоплення, збору носіїв інформації у вигляді матеріальних тіл (бракованих вузлів, деталей, демаскуючих речовин і т. ін.) за межами контрольованої

remote user – віддалений користувач # користувач, що перебуває на місці, відмінному від того, на якому розміщають ті мережні ресурси, які він використовує

remotely piloted vehicle – дистанційно пілотований літальний апарат # ДПЛА # апарат літальний безпілотний, політ якого здійснюють під безперервним контролем, а на певних етапах – під безпосереднім керуванням оператора, що знаходиться на наземному або повітряному пункті управління, з використанням двосторонніх каналів радіозв'язку. Встановлені на ДПЛА засоби огляду навколишнього середовища (телевізійні та інші) забезпечують ніби "ефект присутності" оператора-пілота на борті ЛА. Розрізняють ДПЛА літакової і вертолітної схем, одноразового та багаторазового використання, з наземним і повітряним стартом, посадкою "по літаковому" або на парашуті (у тому числі з підхопленням ДПЛА з повітря вертольотом), а за призначенням – для розвідки і цілевказу, радіоелектронної боротьби, нанесення ударів по наземних (морських) цілях, проведення льотних експериментальних досліджень і т. ін.

rename user – віддалений користувач # дистанційний користувач # користувач обчислювальної системи, який здійснює доступ до програм і даних з віддаленого термінала.

repeater – повторювач # пристрій рівня фізичного моделі ISO/OSI, призначений для підсилення сигналу з одного сегмента кабелю на інший сегмент без зміни змісту. Дозволяє збільшувати довжину магістралі мережі і кількість абонентів. Застосовується в мережах обчислювальних локальних.

repeater – ретранслятор # проміжна радіо, радіорелейна або телевізійна станція в мережі передавальних і приймальних станцій.

repeater line – радіорелейна лінія зв'язку # див. relay line.

report – ипривести у звіті [повідомленні] # включити результати оцінювання та допоміжні матеріали в технічний звіт про оцінювання або в повідомлення про проблему.

repudiation – відмова # самозаперечення одного з логічних об'єктів, задіяного в обмін даними, щодо участі повністю або частково в цьому обміні.

repudiation of origin – відмова від авторства # заперечення причетності до утворення або передавання якого-небудь документа чи повідомлення.

repudiation of receipt – відмова від одержання # заперечення причетності до одержання якого-небудь документа чи повідомлення.

requirement – вимога # встановлена, загально застосовувана чи обов'язкова потреба або очікування. «Загально застосовувана» означає, що це є клієнтською або загальною практикою для організації та зацікавлених сторін, що розглядувані потреби або очікування застосовують. Встановленою є така вимога, яку визначають, наприклад, у документованій інформації

requirements specifications – технічне завдання (ТЗ) # сукупність вимог до виробу, що визначаються його призначенням, галуззю застосування, умовами експлуатації, типом виробництва. ТЗ складають на основі документації нормативно-технічної, вимог замовника, а також за результатами вивчення ринку й аналізу кращих зразків конкурентної техніки (аналогів), наукового прогнозування. Відповідно до стандарту, ТЗ має такі розділи: назва і галузь застосування; джерело розробки; мета та призначення; технічні вимоги; економічні показники; етапи розроблення; порядок контролю і приймання; додатки.

resident – резидент # 1. за часів середньовіччя дипломатичний представник, що постійно перебуває в даній країні # 2. таємний уповноважений іноземної розвідки, який на території даної держави спрямовує діяльність своїх агентів; керівник мережі агентурної або групи за кордоном.

resident virus – резидентний вірус # вірус комп'ютерний, який залишає в оперативній пам'яті ЕОМ після завершення програми свою резидентну частину – переносника вірусу, який потім перехоплює звернення операційної системи до об'єктів зараження і впроваджується в них. Резидентний вірус знаходиться в пам'яті і є активним аж до виключення або перезавантаження комп'ютерної системи. Резидентний вірус активізують після кожного ввімкнення комп'ютера.

residential gateway – резидентний шлюз # вузол, розташований в приміщенні користувача, який забезпечує взаємодію існуючого обладнання користувача з пакетною мережею

residual data – залишкові дані # дані, що залишаються в носіях даних після видалення файлу чи частини файлу.

residual risk – залишковий ризик # ризик, що залишається після впровадження заходів забезпечення безпеки. Залишковий ризик або «збережений ризик» може містити неідентифікований ризик.

resilience – **1.** здатність системи до відновлювання функцій # здатність функційного блока продовжувати виконувати необхідну функцію за наявності несправностей або помилок # **2.** опірність # властивість чого-небудь протистояти певним

впливам, змінам, а також сила, ступінь такого протистояння.

resistance to cryptoanalysis – криптостійкість # див. cryptosecurity, cipher strength, cryptological hardness.

resistance to suggestion – опірність навіюванню # властивість об'єкта протистояти навіюючому впливу суб'єкта (контрсугестія). Здатність до опірності навіюванню залежить від особливостей інтелектуальної і емоційно-вольової сфери особистості. Опірність навіюванню поділяють на навмисну і ненавмисну, індивідуальну і групову, загальну і спеціальну. Опірність навіюванню мінлива. Один і той же об'єкт виявляє різну ступінь о. н. по відношенню до різних суб'єктів і різного змісту інформації, що навіюється. Опірність навіюванню також характеризують динамізмом. Величина реальної о. н. постійно коливається як у сторону зниження, так і в сторону підвищення. При зростанні вона може привести до такої величини, коли будь-який навіюючий вплив даремний. Так високу опірність навіюванню має солдат в атаці. В цей час будь-що йому навіювати не має ні найменшого сенсу.

resource reservation protocol – протокол резервування ресурсів # протокол, що дозволяє резервувати з'єднання та ресурси Інтернет і забезпечує обслуговування в реальному часі, обслуговування з негарантованою якістю та кероване спільне використання лінії.

resources – ресурси # 1. матеріальні засоби, цінності, запаси, кошти, що в разі потреби можна використати # 2. будь-які з компонентів (засобів) системи обчислювальної та можливості, які можуть бути надані нею для процесу оброблення даних на певний проміжок часу.

resources availability – доступність ресурсу # властивість ресурсу, що полягає у можливості його використання за вимогою користувача, який має відповідні повноваження.

responding-address – адреса відповідаючого # параметр, що може бути наявним у примітивах відповіді і підтвердження сервісу і який ідентифікує адресу у одержувача. У визначенні сервісу конкретного рівня такий параметр може називатися або «адреса викликаного», або «адресу відповідаючого».

response – реагування # виявлення свого ставлення до чогось, відповідь якимось чином на ту чи іншу дію, дія під впливом чого-небудь.

restricted data – закриті дані # захищені дані # дані, доступні обмеженому колу користувачів. Як правило, обмеження доступу досягається системою паролів.

retransmission– ретранслювання # див. relaying.

retransmitter – ретранслятор # див. repeater.

retrieval – пошук # 1. дії шукаючого, розшукування кого-, чого-небудь # 2. спосіб розвідки.

reverse LAN channel – резервний канал ЛМ # в широкосмуговій локальній мережі, канал, призначений для пересилання даних від станцій пересилання даних до головного вузла.

reversible code – оборотний код # код, в якому існує взаємно-однозначна відповідність між повідомленнями, що кодуються, і комбінаціями кодовими, що їх відображають.

review – **1.** перегляд # **2.** аналіз # діяльність, спрямована на визначення придатності, адекватності та ефективності дій для досягнення запланованих цілей # див. analysis.

review object – об'єкт перегляду [аналізу] # певний елемент, який переглядають [піддають аналізу].

review objective – **1.** ціль перегляду # **2.** мета аналізу # твердження, яке описує, чого саме має бути досягнуто в результаті перегляду [аналізу].

RFC IETF – request for comments – запит на коментар.

right – право # див. law, science of law, jurisprudence.

RIP – routing information protocol – протокол керування інформацією маршрутизації.

risk – ризик # *1.* можливість того, що певна загроза застосовуватиме особливу вразливість системи опрацювання даних # *2.* поєднання імовірності виникнення певної комбінації обставин та її наслідків # *3.* ефект невизначеності щодо досягнення цілей. Ефект відхилення від очікуваного — позитивне чи негативне. Невизначеність — це стан дефіциту, іноді часткового, відповідної інформації, розуміння або знань стосовно події, її наслідків або імовірності. Ризик часто характеризують з посиланням на потенційні події і наслідки або їх комбінацію. Ризик часто описують у термінах комбінації наслідків події (охоплюючи зміни в обставинах) і відповідної імовірності виникнення. У контексті систем керування інформаційною безпекою ризики інформаційної безпеки можна розглядати як ефект невизначеності щодо досягнення цілей інформаційної безпеки. Ризик інформаційної безпеки пов'язаний з можливістю того, що загрози будуть використовувати вразливості інформаційних ресурсів СУІБ або групи інформаційних ресурсів СУІБ і таким чином призводити до збитків організації.

risk acceptance – прийнятний [ступеня] ризику # організаційне рішення прийняття певного ризику, зазвичай, з технічних чи економічних причин.

risk analysis – **1.** аналіз ризиків # *1.* систематичний метод ідентифікації активів системи опрацювання даних, загрози для цих активів та вразливість системи до цих загроз # *2.* процес розуміння характеру ризику і визначення рівня ризику # аналіз ризиків забезпечує основу для визначення ступеня ризику і прийняття рішення про обробку ризику; аналіз ризиків охоплює прогнозну оцінку ризику **#** *3.* систематичне використання

інформації для визначення джерела й оцінювання ризику # **2.** аналізування ризику # процес осмислення природи ризику та визначення рівня ризику. Аналізування ризиків забезпечує основу зіставлення ризиків і прийняття рішень стосовно оброблення ризиків. Аналізування ризику охоплює оцінювання ризику.

risk analysis – аналіз ризику # процес визначення загроз безпеці інформації та їхніх характеристик, слабких сторін системи захисту інформації комплексної (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їхньої прийнятності для експлуатації автоматизованої системи.

risk assessment – оцінювання ризиків # *1.* систематичний метод ідентифікації активів системи опрацювання даних, загрози для цих активів та вразливість системи до цих загроз # *2.* загальний процес ідентифікації ризику, аналізування ризику та зіставлення ризику.

risk communication and consultation – обговорення ризиків і консультації # постійні та ітераційні процеси, які здійснює організація для того, щоб надавати, спільно використовувати чи отримувати інформацію, а також привертати увагу в діалозі з акціонерами до питання керування ризиками. Інформація може стосуватися існування, природи, форми, імовірності, значимості, зіставлення, прийняття та оброблення ризиків. Консультація є двостороннім процесом взаємного інформування між організацією та її акціонерами щодо спірних питань до прийняття рішення або визначення напрямків з цих питань. Консультації – це: процес, який діє на прийняття рішення скоріше через вплив, а не примусово; і вклад для прийняття рішення, а не прийняття спільного рішення.

risk criteria – критерії ризику # посилання, на основі яких можна оцінити важливість ризику. Критерії ризику базуються на цілях організації, а також зовнішніх та внутрішніх обставинах. Критерії ризику може бути отримано зі стандартів, законів, політик та інших вимог.

risk evaluation – **1.** зіставлення ризику # **2.** визначення ступеня ризику # процес порівняння результатів аналізування ризику з критеріями ризику для визначення, чи може ризик та/або його величина бути прийнятим або толерантним. Зіставлення ризику допомагає в прийнятті рішення стосовно оброблення ризику.

risk identification – ідентифікація ризику # процес виявлення, розпізнавання та описування ризику. Ідентифікація ризику охоплює ідентифікацію джерел ризику, подій, які його спричинили, та його потенційних наслідків. Ідентифікація ризику може охоплювати дані історії, теоретичний аналіз, неформальні та експертні висновки, а також потреби акціонерів

risk management – адміністративне керування ризиком # сукупність заходів, що проводяться протягом усього життєвого циклу системи автоматизованої щодо оцінки ризику, вибору, реалізації й упровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня ризику залишкового.

risk management – керування ризиком # скоординовані дії в організації щодо регулювання та контролю ризику.

risk management process – процес керування ризиком # систематичне застосування політик, процедур і практик керування до дій стосовно комунікації, консультацій, визначення обставин та ідентифікації, аналізування, зіставлення, оброблення, моніторингу та перегляду ризиків. Термін «процес» використовують для опису керування ризиками в цілому. Елементи в середині процесу керування ризиками описуються як «дії».

risk owner – власник ризику # особа чи організація, яка має повноваження та владу для керування ризиками.

risk treatment – оброблення ризику # процедура вибору й застосування варіантів коригування ризику. Оброблення ризику може охоплювати: усунення ризику за допомогою прийняття рішення не починати чи не продовжувати дії. які призводять до цього ризику; прийняття або посилення ризику з метою отримання нагоди для його вивчення; вилучення джерела ризику: зміни ймовірності виникнення ризику; зміни наслідків; розподіл ризику між іншими сторонами (охоплюючи контракти та фінансування ризиків); і утримання ризику як обізнаний вибір. Оброблення ризиків з негативними наслідками іноді називають «послаблення ризику», «усунення ризику», «попередження ризику» і «зменшення ризику». Оброблення ризиків може створювати нові ризики або модифікувати наявні ризики

risky information impact небезпечні інформаційні впливи # дії, спрямовані на зниження рівня безпеки інформаційної. Бони можуть бути засновані як на викраденні (втраті) цінної інформації з об’єктів інформаційної безпеки, так і на впровадженні негативної інформації на об’єкти інформаційної безпеки.

RNG random number generator – генератор випадкових чисел.

RO – remote operations – дистанційні операції.

roaming – роумінг # здатність користувача отримувати доступ до сервісів згідно зі своїм профілем протягом знаходження поза мережею прописки, тобто використовуючи пункт доступу візитної мережі.

rollback – відкат # послуга безпеки, що забезпечує повернення об’єкта системи комп’ютерної до відомого попереднього стану після виконання

над об’єктом певної операції або серії операцій.

ROSE – remote operations service element – елемент сервісу дистанційної операції.

rotational delay – затримка обертання # час, потрібний для головки зчитування/записування пристрою зберігання з прямим доступом для знаходження певного запису на доріжці, що відповідає заданій адресі чи клавіші.

round key – ітераційний ключ # ключ, який використовується на кожному циклі шифрування в симетричному блочному алгоритмі шифрування, побудованому за схемою Фейстела. Виробляється за певним правилом із ключа шифрування.

router – маршрутизатор # мережний пристрій, який використовують для встановлення і керування потоками даних між різними мережами за допомогою вибору трактів або маршрутів на основі механізмів і алгоритмів протоколів маршрутизації. Мережі самі можуть базуватися на різних протоколах. Інформація про маршрутизацію зберігається в таблиці маршрутизації

routing – маршрутизація # процес визначення шляху для передавання даних від відправника до одержувача. Алгоритми м., необхідні для оновлення таблиці маршрутизації, яка би відповідала потоковій топології мережі, реалізуються в протоколах маршрутизації. Виходячи з різних критеріїв оцінки алгоритмів м., можна виділити наступні види м.: статична, динамічна, внутрішньодоменна, між-доменна, однорівнева, ієрархічна, централізована, розподілена, одношляхова, багатошляхова, м. хостом, м. маршрутизатором, канальна (маршрутизація за станом каналу), векторна і примусова.

routing control – контроль маршрутизації # застосування правил у процесі маршрутизації до вибору чи виключення конкретних мереж, ланок даних або ретрансляторів.

routing domain – домен маршрутизації # сукупність маршрутизаторів, які обмінюються інформацією маршрутування пакетів в межах адміністративного домену.

routing information protocol – протокол керування інформацією маршрутизації # протокол забезпечує це керування в самодостатніх мережах (корпоративних комп’ютерних) чи у взаємодіючих групах таких мереж і є одним з протоколів внутрішнього шлюзу IGP.

routing table – таблиця маршрутизації # список діючих шляхів передавання даних.

RPV – remotely piloted vehicle – дистанційно пілотований літальний апарат.

RSA[1] – Rivest-Shamir-Adleman – шифрування Ривеста-Шаміра-Адлемана.

RSA[2] – ron rivest, adi shamir, and leonard adleman cryptography algorithm – алгоритм асиметричного шифрування з відкритим ключем.

RSA encipherement – шифрування методом RSA # метод шифрування, запропонований Рівестом, Шаміром і Адлеманом, при якому ключ, що використовується для зашифровування, не збігається з ключем для розшифровування (останній повинен бути відомим одержувачу); відноситься до методів шифрування з відкритим ключем.

RSVP – resource reservation protocol – протокол резервування ресурсів.

RTCP – real time transport control protocol – протокол керування транспортуванням у реальному часі.

RTP – **1.** real time protocol – протокол реального часу # **2.** real time transport protocol – транспортний протокол реального часу.

RTSE – reliable transfer service element – сервісний елемент надійного пересилання.

rule – правило # 1. положення, яким передається якась закономірність, стале співвідношення певних явищ; припис, норма # 2. зібрання якихось положень, що визначають порядок ведення або дотого-небудь.

rule-based security policy – уніфікована стратегія захисту # стратегія захисту, заснована на загальних правилах, пропонованих для всіх користувачів. Ці правила, зазвичай, ґрунтуються на порівнянні чутливості доступних ресурсів і володінні відповідними атрибутами користувачів, груп користувачів або логічних об'єктів, що діють від імені користувачів.

running – запуск # стосується стану задачі виконуваного завдання, у якому завдання на заданий момент призначено процесору.

S

safeguards measure – заходи убезпечення # послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

safety – безпека # див. security.

safety ring – кільце безпеки # знімне пластикове чи металеве кільце, наявність або відсутність якого на магнітній стрічці котушки заважає писати на магнітній стрічці і тим самим запобігає випадкове стирання файлу.

salt – **1.** «сіль» # **2.** «пісок» # несекретні, зазвичай випадкові, значення, які використовуються в процесі хешування.

sample – вибірка # вибір елементів із деякої сукупності для дослідження таким чином, щоб його результати дали інформацію про аналогічні елементи, які не увійшли до вибірки.

sanitizing – очищення # видалення конфіденційної інформації з документа, щоб зменшити його вразливість.

SAP – service access point – точка доступу до сервісу.

SAP-address – service access point address – SAP-адреса # див. service access point address.

SASL – simple authentication and security layer – рівень простої аутентифікації та безпеки.

save – збереження # функція чи режим, що дає змогу користувачеві зберігати

файл на носії даних, щоб постійно змінювати вміст файлу.

scaffolding – кодогенерування # програми та дані, призначені для підтримки розробляння та тестування програмного забезпечення, але не передбачені для долучення до кінцевого продукту # наприклад фіктивні програми чи файли, тестові генератори, монітори програмного забезпечення, заглушки.

scale – **1.** масштаб # упорядкований набір значень, безперервний або дискретний, або набір категорій для відображення атрибутів. Тип масштабу залежить від природи взаємозв'язків між значеннями на масштабі. Зазвичай визначають чотири типи масштабів: номінальний: значення вимірювань категоризовані; порядковий: значення вимірювань класифіковані; інтервальний: значення вимірювань порівнюють з дистанціями, які відповідають однаковим кількостям атрибутів; з коефіцієнтами: значення вимірювань порівнюють з дистанціями, які відповідають однаковим кількостям атрибутів, де значення нуль відповідає відсутності атрибутів # **2.** масштабування зміна подання кількості, вираженням її в інших одиницях, так щоб її діапазон був уведений в границях заданого інтервалу.

scare – паніка # див. panic.

scavenge – збиратия # пошук без авторизації через залишкові дані для отримання конфіденційної інформації.

scenario – сценарій # подання знань, яке застосовує заздалегідь визначені послідовності подій для визначення результатів взаємодії між відомими об'єктами. Подія представлена за допомогою сцен, параметрів, тематичних ролей та реквізитів. Скрипт орієнтований на події в протилежність кадрум, які орієнтовані на дані, і які стосуються моменту часу.

schema – схема # *1.* графічне зображення умовними символами структури якого-небудь об'єкта # *2.* опис складу і властивостей об'єкта # *3.* визначення контенту, структури та обмежень, що використовуються для створення та підтримки бази даних

scheme – система оцінювання # сукупність правил, що встановлені органом оцінювання та визначають середовище оцінювання, включаючи критерії і методологію, що необхідні для проведення оцінювання безпеки інформаційних технологій # див. schema, circuit.

science of law – право # див. law, right, jurisprudence.

scientific informatics – теоретична інформатика # напрямок інформатики, що використовує методи математики для побудови і вивчення моделей обробки, передавання та використання інформації, створює той теоретичний фундамент, на якому будується вся інформатика.

scientific information activity – науково-інформаційна діяльність # галузь діяльності щодо задоволення

потреб суспільства у науково-технічній інформації. До поняття д. н. і. входять збирання, перероблення аііалітіїко-сіппетичне, зберігання, пошук, розповсюдження науково-технічної інформації.

scout – розвідник # див. intelligence agent, secret service man, spy, reconnaissanceman.

scout pilotless vehicle – розвідувальний безпілотний апарат літальний # див. reconnaissance pilotless vehicle.

scouting – розвідка # див. intelligence, reconnaissance, surveillance, secret service.

scramble – скремблювання # 1. перетворення інформаційного двійкового сигналу з будь-якими статистичними властивостями у двійковий сигнал, в якому послідовність одиниць і нулів змінюється по випадковому або псевдовппилковому закону. Скремблювання можна розглядати як вторинне кодування без внесення надмірності. Воно здійснюється на передавальній стороні за допомогою пристрою, що називається скремблером. На приймальній стороні здійснюється зворотна операція – дескремблювання – пристроями, що називаються дескремблерами # 2. спрощений метод захисту інформації, заснований, як правило, на перестановці (змішуванні) окремих елементів повідомлення без використання ключа.

scramble – шифрувати # перетворення цифрового сигналу на псевдовипадковий цифровий сигнал, що має таке ж значення й таку ж швидкість пересилання, щоб полегшити пересилання чи записування. Шифрування уникає проблем, які можуть виникнути внаслідок пересилання довгих послідовностей «1» або «0».

scrambler – скремблер # кодувальний пристрій, який видає випадкову послідовність бітів, забезпечуючи постійність спектральної густини модульованих сигналів незалежно від змісту інформації, що передається. В найбільш загальному випадку с. реалізує логічну операцію підсумовування за модулем два вихідного і перетворюючого випадкового двійкового сигналу. Обернена операція здійснюється пристроєм, що називаються дескремблером. Скремблер і дескремблери реалізуються за допомогою регістрів зсуву.

scrambling – засекречування # див. classifying, classification, cryptment, security.

scrambling – скремблювання # див. scramble.

screening– екранування # див. shielding.

script – скрипт # подання знань, яке застосовує заздалегідь визначені послідовності подій для визначення результатів взаємодії між відомими об’єктами. Подію представляють за допомогою сцен, параметрів, тематичних ролей та реквізитів. Скрипт орієнтований на події в протилежність кадрум, які

орієнтовані на дані, і які стосуються моменту часу.

SD system – система SD # система розпізнавання мови, обмежене зареєстрованим користувачем або групою користувачів, яка потребує попередньої підготовки до їхніх моделей мови # наприклад одноголосна система, мультиголосна система.

SDSL – symmetric digital subscriber line – симетрична цифрова абонентська лінія.

SDU – service data unit – сервісний блок даних.

seal – печатка # значення криптографічного контролю, яке підтримує цілісність, але не захищає від підробки одержувачем (тобто він не підтримує неможливості відмови).

seamless service – **1.** цільний сервіс # **2.** неперервний сервіс # сервіс, який запобігає тому, щоб користувачі відчували будь-які переривання обслуговування у стані рухомості чи переносності.

search – пошук # перевірка одного чи кількох елементів даних набору для пошуку тих елементів, які мають певні властивісті.

search cycle – цикл пошуку # послідовність подій пошуку, яка повторюється для кожного елемента даних.

search key – ключ пошуку # ключ для опрацювання даних.

search space – простір пошуку # при вирішенні проблем, набір можливих кроків, що ведуть від початкових станів до цільових станів.

search time – час пошуку # час, потрібний для головки зчитування/записування пристрою зберігання з прямим доступом для знаходження певного запису на доріжці, що відповідає заданій адресі чи клавіші.

search tree – дерево пошуку # деревоподібний граф, який відповідає різним правилам, застосованим у пошуку, для вивчених вузлів та отриманих результатів.

search(ing) – пошук # див. retrieval.

secondary key – вторинний ключ # ключ, який не є первинним ключем, але для якого підтримується індекс, і він може позначати більше одного запису.

SecOPs – security operating procedures – робочі процедури безпеки.

secrecy – скритність # таємниця # 1. дещо ще не розгадане, не пізнане # 2. дещо, що старанно приховується від інших, відоме тільки обмеженому колу осіб, інформація, що не підлягає розголошенню, секрет # 3. таємна або конфіденційна інформація (відомості), що відома вузькому колу суб’єктів унаслідок виконання службових, професійних обов’язків або окремих доручень, яка охороняється особливим чином, а розголошення її може спричинити юридичну відповідальність. Причому юридична відповідальність наступає не тільки за розголошення таємниці, але й і за її незаконне одержання та використання. В законодавствах розвинених країн звичайно

виділяють наступні види таємниць: таємницю приватного життя, професійну, комерційну, службову, державну таємницю # див. confidentiality.

secret – секрет # таємниця # 1. таємниця (у тому числі державна); те, що старанно охороняється і приховується (інформація, винаходи, прилади і т. ін.) # 2. потайний пристрій в механізмі # див. confidentiality. див. secrecy, mystery.

secret [top-secret] clearance – допуск до державної таємниці # процедура оформлення права громадян на доступ до відомостей, що складають таємницю державну, підприємств, закладів і організацій – на проведення робіт з використанням таких відомостей. Допуск посадових осіб і громадян до державної таємниці здійснюється у добровільному порядку і передбачає відповідну процедуру допуску до державної таємниці. При цьому встановлюються три форми допуску, які відповідають ступеням секретності відомостей, що складають державну таємницю: до відомостей державної важливості, цілком секретних і секретних.

secret information – відомості таємні # відомості, що складають державну таємницю, за виключенням відмомостей особливої ваги та цілком таємних, розповсюдження яких може нанести шкоду підприємства, закладу або організації.

secret information – таємна інформація # інформація з обмеженім доступом, яка містить відомості що становлять державну або іншу передбачену законом таємницю.

secret intelligence device – закладний пристрій # потай встановлений технічний засіб, який створює загрозу для інформації.

secret key – секретний ключ # ключ, який призначений для використання обмеженою кількістю кореспондентів для шифрування та дешифрування.

secret operation – таємна операція # сукупність заходів, що проводяться розвідувальною організацією в скритій або замаскованій формі, головним чином, із тим, щоб утрудняти (або зробити неможливим) процес доказу причетності до них їхніх організаторів.

secret service – розвідка # див. intelligence, scouting, surveillance, reconnaissance.

secret service man – розвідник # див. intelligence agent, scout, spy, reconnaissanceman.

secret-key cryptosystem – симетрична криптосистема # див. symmetric cryptosystem, classical cryptosystem, one-key cryptosystem.

secret-service network – агентурна мережа # група агентів, зв’язаних між собою і підпорядкованих агенту-груповоду, який, у свою чергу, підзвітний співробітнику розвідки (резиденту) держави, на яку працює мережа.

sector – сектор # заздалегідь визначена кутова частина доріжки чи смуги на магнітному барабані чи магнітному диску, що може адресуватися.

sector alignment – вирівнювання секторів # методика захисту від копіювання, яка визначає, чи є диск неавторизованою копією, перевіряючи доріжку за доріжкою на правильність розташування секторів.

secunty gateway – шлюз безпеки # точка з'єднання між мережами, між сегментами мереж або між програмними застосунками в різних доменах безпеки, призначена для захисту мережі відповідно до наявної політики безпеки

secure access management service – сервіс керування захищеним доступом # сервіс, який забезпечує захист ресурсів системи опрацювання повідомлень від їх несанкціонованого використання.

secure device identifier – ідентифікатор захищеного пристрою # ідентифікатор пристрою, який криптографічно прив'язаний до пристрою і складається із ключа ідентифікатора захищеного пристрою (Secure Device Identifier Secret) та повноваження ідентифікатора захищеного пристрою (Secure Device Identifier Credential).

secure device identifier certificate – сертифікат ідентифікатора захищеного пристрою, сертифікат DevID # синоніми для об'єкта даних побудованого з використанням криптографічних операцій, щоб зв'язати ім'я DevID з іншими даними для криптографічних даних про ключ, які має пристрій.

secure device identifier credential – **1.** повноваження ідентифікатора захищеного пристрою # **2.** повноваження DevID # синоніми для об'єкта даних побудованого з використанням криптографічних операцій, щоб зв'язати ім'я DevID з іншими даними для криптографічних даних про ключ, які має пристрій.

secure device identifier module – **1.** модуль ідентифікатора захищеного пристрою # **2.** модуль DevID # логічний компонент безпеки, який буде надійно зберігати і працювати з одним чи декількома ключами DevID і пов'язаних з ними DevID повноваженнями.

secure device identifier root credential store – база корневих повноважень ідентифікатора захищеного пристрою # база даних кореневих повноважень для IDevID і LDevID повноважень, які зберігаються і використовуються DevID за сумісними рішеннями. Це еквівалентно звичайному кореневому сховищу веб-браузера і може бути відправлене як закінчене рішення.

secure device identifier secret – ключ ідентифікатора захищеного пристрою # приватна частина ключа, публічно-приватного ключа парно пов'язаного з повноваженнями DevID.

secure interaction rules – правила захищеної взаємодії # загальні

аспекти правил, необхідних для взаємодії між доменами захисту.

security – **1.** засекречування # див. classifying, classification, cryptment, scrambling # **2.** захист # див. protection, lock out # **3.** безпека # стан, при якому кому-небудь, чому-небудь не загрожує небезпека (будь-якого виду), існує захист від небезпеки. Виділяють три рівні безпеки: особистості, суспільства, держави і розрізняють зовнішню, міжнародну, внутрішню, національну, політичну, державну, інформаційну, особисту, воєнну, суспільну, регіональну, господарську, економічну, продовольчу, екологічну безпеку. В державній практиці різних країн створюються міністерства, комітети, ради національної (державної) безпеки, відповідні органи, структури і служби.

security administrator – адміністратор безпеки # *1.* особа або група осіб, відповідальних за забезпечення безпеки системи, за реалізацію і безперервність дотримання адміністративних заходів захисту і здійснюючих постійну організаційну підтримку функціонування фізичних і технічних засобів захисту, що застосовуються # *2.* адміністратор, відповідальний за дотримання політики безпеки.

security administrator – адміністратор захисту # суб'єкт доступу, який є відповідальним за захист від несанкціонованого доступу системи інформаційної.

security analysis – аналіз захищеності # *1.* перевірка відповідності якісних і кількісних характеристик показників ефективності заходів із захисту інформації вимогам із безпеки інформації # *2.* процес виявлення уразливостей ресурсів автоматизованої системи, а також вироблення рекомендацій з їхнього усунення.

security association – захист асоціації # відносини між двома або більше об'єктами, для яких існують атрибути (стан інформації та правила), що регулюють надання послуг захисту, які стосуються цих об'єктів.

security attestation– атестація засобів захисту # засвідчення ступеня відповідності вимогам доданого класу засобів захисту.

security audit – **1.** перевірка [стану] безпеки # **2.** аудит [стану] безпеки # **3.** перевірка засобів захисту # **4.** аналіз процедур захисту # незалежний огляд та перевірка записів та операцій системи опрацювання даних для перевірки адекватності системного контролю, забезпечення відповідності встановленої політики безпеки та операційних процедур, виявлення порушень безпеки та рекомендації щодо будь-яких зазначених змін у керуванні, політиці безпеки та процедурах.

security audit trail – **1.** дані трасування захисту # накопичені і готові до використання дані, призначені для докладнішого аналізу процедур

захисту скритність # **2.** фіксування контролю засобів захисту # сукупність відомостей про стан засобів захисту, що накопичуються з часом і призначені для спрощення керування засобами захисту.

security avaluation criterion – критерій оцінки захищеності # сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їхньої реалізації.

security category – категорії безпеки # неєрархічна група конфіденційної інформації, що її застосовують для більш точного керування доступу до даних, ніж з єрархічною класифікацією безпеки.

security certification – **1.** атестація захисту # підтвердження уповноваженою компетентною особою того, що оцінка захисту була зроблена кваліфіковано і відповідно до встановлених правил # **2.** сертифікація засобів захисту інформації # процес встановлення відповідності засобів захисту інформації до вимог захисту відомостей відповідного ступеня секретності.

security classification – класифікація безпеки # – категорія захисту #визначення того, який конкретний ступінь захисту від доступу до даних або інформації вимагається, разом із зазначенням цього ступеня захисту # наприклад «найпотаємніші», «секретні», «конфіденційні» # див. security classification label.

security classification label – гриф секретності # реквізити, що свідчать про ступінь секретності відомостей, що містяться в їхньому носієві, і проставляються на самому носієві і (або) супроводжувальній документації на нього. Установлюється на основі відповідних законів та відомчих переліків відомостей, що складають таємницю державну. Для інформації секретної, цілком секретної інформації та особливої важливості вводяться грифи «секретно», «цілком секретно» та «особливої важливості», для несе- кретної інформації, що містить службову таємницю, вводять гриф «для службового використання».

security clearance – категорія допуску # рівень захисту # категорія, що пов’язана з суб’єктом доступу і визначає категорію захисту інформації, до якої цьому суб’єктові надане право доступу.

security communication function – функція захисту обміну данимии # функція, що підтримує передавання інформації, яка стосується захисту, між відкритими системами.

security controls – контроль безпеки # керування, операційний і технічний контроль (тобто засоби захисту і заходи протидії), заздалегідь описані для інформаційної системи з метою захисту конфіденційності, цілісності й доступності системи та її інформації. Мається на увазі засоби керування, що забезпечують відстежуваність, автентичність,

неспростовність, захист персональної інформації і надійність, які часом розглядаються окремо від конфіденційності, цілісності й доступності.

security domain – **1.** домен захисту # домен безпеки # набір елементів, політика захисту, орган захисту та набір заходів, пов'язаних із безпекою, в яких набір елементів підпорядковується політиці захисту, яку веде служба захисту, для зазначених видів діяльності # **2.** захищена зона # частина операційної системи яка виконує функції політики забезпечення захисту.

security evaluation – оцінювання захисту # визначення ступеня відповідності системи захисту встановленій моделі механізму захисту, стандарту забезпечення захисту і технічним умовам. Оцінювання захисту може бути зроблена шляхом: спостереження за поведінкою системи при виконанні її функцій; спроб упровадитися до системи з використанням методів зловмисника; аналізу подробиць побудови системи, особливо програмного забезпечення, який часто проводиться з використанням верифікації і атестації.

security exchange – захист обміну # передача або послідовність передавання інформації-керування-протоколу-прикладного-рівня між відкритими системами як частина роботи одного або декількох механізмів захисту.

security exchange function – функція захисту обміну # функція захисту обміну даними, що розташована на прикладному рівні, яка забезпечує засоби для передавання інформації про безпеку між АЕ-зверненнями.

security exchange item – елемент захисту обміну # логічно виразний фрагмент інформації, що відповідає одиничній передавання (у послідовності передавання) обміну захисту.

security filter – фільтр безпеки # надійна комп'ютерна система, яка забезпечує дотримання політики безпеки даних, що проходять через систему.

security implementation standard – стандарт впровадження безпеки # документ, який визначає санкціоновані шляхи реалізації безпеки.

security label – мітка грифа # позначка захисту # гранична позначка, надана ресурсу (наприклад, блоку даних), що іменує або позначає атрибути захисту цього ресурсу. Позначка та/або надане значення можуть бути явними або неявними.

security level – рівень безпеки # комбінація єрархічної класифікації безпеки та категорій безпеки, що відображають вразливість об'єкта чи рівень безпеки особи.

security level of language information – рівень захисту мовної інформації # поняття, що використовується для визначення можливостей різноманітних методів закриття мови. Основні рівні захисту

визначаються як тактичний та стратегічний, що в деякій мірі перекликається з поняттями практичної та теоретичної стійкості криптографічних систем закриття даних. Засоби з тактичним, або низьким, рівнем використовується для захисту інформації від підслухування сторонніми особами на період часу, що вимірюється хвилинами або днями. Існує велика кількість простих методів, здатних забезпечити такий рівень захисту при прийнятній вартості. Засоби зі стратегічним, або високим, рівнем захисту інформації від перехоплення використовується у випадках, коли високо кваліфікованому, технічно добре озброєному фахівцеві потрібно буде для дешифрування перехопленого повідомлення період часу від декількох місяців до багатьох років. Часто використовується і поняття середнього ступеня захисту, що займає проміжне положення між тактичним та стратегічним рівнем закриття.

security management information base – інформаційна база керування безпекою.

security mechanism – механізм захисту # 1. конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки # 2. сукупність засобів захисту, що функціонують разом для виконання поставленого завдання з захисту даних.

security mechanism model – модель механізму захисту # формальне визначення внутрішніх характеристик захисту, що забезпечуються певним механізмом захисту. Як правило, містить докладну специфікацію дозволених і заборонених відносин між суб'єктами і об'єктами доступу згідно з відповідними категоріями доступу та грифом секретності, а також визначає події, які повинні фіксуватися у журналі контрольному.

security model – модель безпеки # формальне подання політики безпеки, що розроблена для системи. М. б. містить формальний опис факторів та правил, що визначають управління, розподіл і захист інформації критичної.

security of automated system – бзпека автоматизованої системи # захищеність системи автоматизованої від несанкціонованого втручання в нормальний процес її функціонування, а також від спроб розкрадання, незаконної модифікації або руйнування її компонентів.

security of banking information – безпека банківської інформації # безпека інформації, яку обробляють в банківських системах. Основним фактором, за яким убезпечення банківської інформації виділяють в окреме завдання є те, що банківські системи автоматизовані є платіжними системами, які використовуються багатьма

організаціями та приватними особами.

security of information – безпека інформації # стан інформації, в якому забезпечують збереження визначених політикою безпеки властивостей інформації.

security of information and their carriers – засекречування відомостей і їхніх носіїв # уведення в передбаченому законом порядку для відомостей, що складають державну таємницю, обмежень на їхнє розповсюдження і доступ до їхніх носіїв. Обґрунтованість засекречування полягає у встановленні шляхом експертної оцінки доцільності засекречування конкретних відомостей, ймовірних економічних і інших наслідків цього акту, виходячи з балансу інтересів життєво важливих держави, суспільства і громадян.

security of resources automated system – безпека ресурсів автоматизованої системи # стан системи автоматизованої, при якому забезпечують конфіденційність, цілісність і доступність компонентів системи. Конфіденційність компонента системи полягає у тому, що він доступний тільки тим суб'єктам доступу (користувачам, програмам, процесам), яким надані на це відповідні повноваження. Цілісність компонента передбачає, що він може бути модифікований тільки суб'єктом, що має на це відповідні права. Цілісність є гарантією коректності (незмінності, працездатності) компонента в будь-який момент часу. Доступність компонента означає, що суб'єкт, який має відповідні повноваження, може і будь-який час без особливих проблем одержати доступ до необхідного компонента (ресурсу).

security of subjects information relations – безпека суб'єктів інформаційних відносин # захищеність суб'єктів відносин інформаційних від нанесення їм матеріальних, моральних або інших збитків шляхом впливу на інформацію і (або) засоби її оброблення та передавання.

security policy – **1.** політика безпеки # сукупність законів, правил та практичного досвіду, на основі яких будується керування, захист і розподіл інформації конфіденційної.# **2.** стратегія захисту # набір критеріїв для забезпечення послуг захисту. Повна стратегія захисту неминуче буде пов'язана з вирішенням багатьох питань, що не входять у сферу ВВС # див. identity-based security policy та rule-based security policy.

security policy violator – порушник правил розмежування доступу # суб'єкт доступу, що здійснює доступ несанкціонований до інформації.

security processing mode – режим забезпечення безпеки # опис усіх категорій допуску усіх користувачів у відповідності до всіх категорій захисту інформації, що повинна зберігатися і оброблятися в системі.

security service – сервіс захисту # сервіс, наданий яким-небудь рівнем

взаємозв`язку відкритих систем, що забезпечує відповідний захист систем або процедур передавання даних.

security state – стан захисту # стан інформації, що зберігається у відкритій системі, і яка необхідна для надання послуг захисту.

security strategy – стратегія захисту # формальне визначення критеріїв, якими слід керуватися при забезпеченні захисту системи від відомих загроз.

security subject – суб'єкт безпеки #активна складова системи, до якої застосовується методика безпеки.

security system attack – атака на систему захисту # спроба подолання системи захисту. Атака може бути активною, тобто такою, що веде до зміни даних, і пасивною. Той факт, що атака була проведена, ще не означає, що вона була успішною. Міра "успіху" атаки залежить від уразливості системи захисту та ефективності захисних заходів.

security system project algorithm – алгоритм проектування системи захисту інформації # розроблення варіанта потрібної системи захисту інформації, засноване на результатах аналізу системного існуючої інформаційної системи. Охоплює наступні етапи: визначення переліку інформації, що належить захисту, цілей, завдань, обмежень і показників ефективності системи захисту; моделювання існуючої системи і виявлення її недоліків із позицій поставлених цілей і завдань; визначення і моделювання загроз безпеці інформації; розроблення варіантів (алгоритмів функціонування) системи, яку проектують; порівняння варіантів за критерієм глобальним і показниками частковими, вибір найкращих варіантів; обґрунтування обраних варіантів перед керівництвом організації; доопрацювання варіантів або проекту з врахуванням зауважень. У зв'язку з відсутністю формальних способів синтезу системи захисту, її оптимізація при проектуванні можлива шляхом поступового наближення до раціонального варіанта в результаті декількох ітерацій.

security threat – загроза безпеці # сукупність умов і факторів, що створюють небезпеку інтересам життєво важливим особистості, суспільства і держави.

security time-lag – час безпечний # математичне сподівання часу розкриття системи захисту статистичним апробуванням можливих варіантів доступу до даних.

security transformation – перетворення захисту # набір функцій (функції захисту системи та функції захисту обміну даними), які в комбінації працюють з елементами даних користувача, з метою захисту цих елементів даних певним способом під час передавання чи зберігання. Специфікації функцій захисту системи та функцій захисту звязку не

є частиною визначень рівнів послуг ВВС або специфікації протоколів.

security zone – зона безпеки інформації # простір, в межах якого забезпечується безпека інформації.

seek time – час пошуку доріжки # час, потрібний важілю доступу у пристрої зберігання з прямим доступом, для розташування на відповідній доріжці.

segment – сегмент # частина програми, яка може бути виконана без усієї резидентної програми в оперативній пам’яті # див. infiltration.

segmentation – сегментація # метод для виділення пам’яті, в якому частини програми завантажуються з допоміжної пам’яті в оперативну пам'ять за потрібності.

selective field protection – вибірковий захист поля # захист конкретних полів усередині повідомлення, що підлягає передачі.

selectivity – вибірковість # здатність здійснювати відбір.

selfcheching code – самоконтролюючий код # надмірний код, декодування якого автоматично приводить до виявлення помилок.

self-checking code – код з виявленням помилок # див. binary error-detecting code, error-detecting code, error-checking code.

self-descriptiveness – інформативність # інтенсивність потоку інформації # якісний показник кількості інформації в джерелі інформації.

semantic check – контроль семантичний # контроль програми на наявність семантичних (смислових) помилок. Здійснюється програмістом до виконання програми або автоматично під час її виконання. Якщо в програмі не передбачені спеціальні засоби, семантичні помилки можуть призвести до аварійного завершення завдання.

semantic code – семантичний код # складна семантична система, яка з достатньо великим наближенням моделює зміст мови природної.

semantic integrity – семантична цілісність # стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

semantic net – семантична мережа # подання знань на основі концепції, в якій об'єкти чи стан виступають як вузли, пов'язані з посиланнями, які вказують на зв'язок між різними вузлами.

semantic network – семантична мережа # подання знань на основі концепції, в якій об'єкти чи стан виступають як вузли, пов'язані з посиланнями, які вказують на зв'язок між різними вузлами.

semantic network transparency – семантична прозорість мережі # здатність мережі доставляти інформацію від джерела до адресата з прийнятним рівнем помилок.

sender – передавач # див. transmitter.

senses – орган чуття # див. organs of sense.

sensibility – чутливість # величина, що характеризує здатність відображати, фіксувати зовнішні впливи, зміни, прояви певного рівня.

sensitive information – конфіденційна інформація # інформація, яка, як визначається компетентним органом, має бути захищена, оскільки її розкриття, модифікація, знищення чи втрата приведуть до відчутних збитків комусь або чомучь.

sensitive material – світлочутливі матеріали # див. light-sensitive material.

sensitiveness – чутливість # див. sensibility, sensitivity.

sensitivity – **1.** вразливість # міра важливості, призначена інформації власником інформації, для позначення потрібності її захисту # **2.** чутливість # характеристика ресурсу, що визначає його цінність чи важливість і може враховувати його уразливість.

sensitivity – чутливість # див. sensibility, sensitiveness.

sequence – послідовність # певна черговість подій, явищ, етапів роботи, порядок розташування чогось.

sequential access – послідовний доступ # здатність вводити дані в пристрій зберігання даних або носій даних у тій самій послідовності в якій вони були задані, чи для отримання даних у тому ж порядку, у якому вони були введені.

sequential circuit – послідовна схема # логіковий пристрій, вихідні значення якого в заданий момент часу залежать від його вхідних значень та внутрішнього стану в той момент, і внутрішній стан якого залежить від безпосередньо попередніх вхідних значень і попереднього внутрішнього стану. Послідовна схема може приймати обмежене число внутрішніх станів і тому може розглядатися з абстрактної точки зору як кінцевий автомат.

serial access – послідовний доступ # здатність вводити дані в пристрій зберігання даних або носій даних у тій самій послідовності в якій вони були задані, чи для отримання даних у тому ж порядку, у якому вони були введені.

series – послідовність # див. sequence.

servability – див. serveability.

serveability – працездатність # можливість отримання сервісу на вимогу користувача та продовжувати надавати сервіс потрібної тривалості з допустимими відхиленнями та за певних умов.

server – сервер # *1.* у комп'ютерній мережі функційний блок, який надає сервіси робочим станціям, персональним комп'ютерам або іншим функційним блокам # наприклад файловий сервер, сервер друку, поштовий сервер # *2.* роль, яку виконує процесор, коли надає послуги іншому процесору.

server registration in the search engine – реєстрування сервера в пошуковій системі # процедура внесення адреси сервера в базу даних, що індексуються, серверів системи пошукової. Якщо необхідно, щоб інформацією, розташованою на сайтах, познайомилася достатня кількість користувачів мережі, необхідно зареєструвати покажчик

URL сервера в пошуковій системі. Для проведення реєстрації досить звернутися по посиланню Add URL на першій сторінці пошукової системи.

service – сервіс # послуга # служба #*1.* здатність заданого рівня та рівнів, розташованих нижче за нього, надаваних логіковим об'єктам наступного більш вищого рівня. Сервіс заданого рівня надають на межі між цим рівнем й наступним вищим рівнем # *2.* здатність заданого рівня та рівнів, що знаходяться нижче його, яка надається логіковим об'єктам наступного більш високого рівня. Сервіс заданого рівня надається на межі між цим рівнем й наступним вищим рівнем.

service access point – точка доступу до сервісу # точка, у якій сервіс заданого рівня надається логіковим об'єктом цього рівня логіковому об'єкту наступного вищого рівня.

service access point address – адреса точки доступу до сервісу # адреса, яка використовується для визначення однієї SAP.

service attribute – атрибут сервісу # параметр, який визначає певну технічну характеристику сервісу # наприклад тип інформації користувача, швидкість переносу інформації тощо.

service component – компонент послуги # частина мультимедійного сервісу, відповідний за обмін даними, пов’язаний з передаванням інформації одного типу.

service content – **1.** інформаційний вміст сервісу # **2.** сервісний контент # корисна інформація, що передається користувачу в процесі реалізації послуги: текстове чи мультимедійне повідомлення, відеофільм тощо.

service continuity – неперервність обслуговування # здатність мережі підтримувати поточний сервіс протягом мобільності користувача.

service data unit – сервісний блок даних # набір даних, який пересилається користувачем сервісу заданого рівня і який має бути переданим рівноправному користувачеві сервісу без семантичних змін.

service documentation– експлуатаційна документація # див. maintenance documentation.

service feature – елемент сервісу # специфічна властивість телекомунікаційного сервісу, яка може використовуватись у поєднанні з іншими сервісами (елементами сервісів) як частина комерційної пропозиції – це може бути основний елемент сервісу або його додаткова функція.

service level agreement – угода про рівень обслуговування # письмова угода між постачальником і замовником, в якому задокументовані послуги та узгоджені рівні послуг. Угоду про рівень обслуговування також може бути встановлено між постачальником послуг і продавцем, внутрішньої групою або споживачем, що діє як продавець.

Угоду про рівень обслуговування може бути включено в контракт або інший тип документованого угоди.

service level agreement – угода про рівень обслуговування # угода між постачальником сервісу та його абонентом (або оператором мережі доступу), яка характеризує вибір певної можливості передавання даних та відповідний атрибут виділення ресурсів.

service node – сервісний вузол # елемент мережі, який підтримує одну чи кілька функцій керування сервісами, функцій даних сервісу, функцій спеціалізованих ресурсів та функцій комутації сервісів для надання послуг у контексті глобальної інформаційної інфраструктури.

service profile – профіль обслуговування # підтримувана мережею сукупність інформації, яка визначає набір послуг, що надається користувачу.

service provider – постачальник сервісу # абстрактне подання всіх логікових об'єктів, які забезпечують сервіси рівноправним користувачам сервісу.

service security policy – політика безпеки сервісу # правила, згідно якими функціонують механізми, що реалізують послугу безпеки.

service user – користувач сервісу # логіковий об'єкт у єдиній відкритій системі, який застосовує сервіс через точки доступу до сервісу.

serviceability – обслуговність # працездатність # можливість отримання сервісу на вимогу користувача та продовжувати надавати сервіс потрібної тривалості з допустимими відхиленнями та за певних умов.

service-oriented interconnection – сервіс-орієнтоване взаємоз'єднання # фізичне та логічне зв'язування доменів мереж, яке дозволяє операторам і постачальникам сервісів пропонувати сервіси через платформи мереж з керуванням і сигналізацією, що забезпечують визначені рівні взаємодії.

services interface – інтерфейс послуг # визначений набір послуг, які доступні процесу або процесору.

session – **1.** сеанс # **2.** сесія # певний інтервал часу, протягом якого клієнт може багато разів взаємодіяти з сервером, причому і клієнт, і сервер підтримують дані один про одного.

session initiation protocol – протокол ініціювання сеансу # протокол рівня застосувань для ініціювання та керування сеансами мультимедійного зв'язку, конференц-зв'язку, телефонного зв'язку, сповіщень про події тощо, який підтримує можливості рухомості користувачів. Різновид протоколу для телефонного зв'язку SIP-T (SIP for Telephones) забезпечує інкапсуляцію повідомлень ISUP в запити SIP і транслювання інформації цих повідомлень, важливої для маршрутування, в заголовки запитів SIP, що дозволяє їх належним чином маршрутувати.

session key – сеансовий ключ # криптографічний ключ, який

використовується тільки під час одного сеансу зв’язку. Після закінчення сеансу зв’язку знищується або виводиться з використання.

session node – вузол мережного з’єднання # набір розташованих поряд станцій робочих, скриньок поштових і кінцевих точок мережі транспортної.

session-based services – сеансовий сервіс # сервіс, надання якого потребує одного чи кількох сеансів обміну даними.

set – **1.** комплект # 1. повний набір інструментів, інших предметів, що мають певне призначення # 2. комплекс, але для виробів, що мають експлуатаційне призначення допоміжного характеру # **2.** набір # поіменована колекція записів, що мають загальну властивість або властивості.

set type – тип набору # тип «множина» # поіменована колекція типів записів, яка складено з одного типу запису облікового запису власника і одного чи кількох типів запису записів про членство, а також єрархічного відношення між типом запису облікового запису власника та іншими типами записів.

SHA – secure hash algorithm – алгоритм криптографічного хешування.

share – частина # див. parts.

shared access – колективний доступ # спільне використання системи обчислювальної двома або більше користувачами в пакетному чи інтерактивному режимах.

shared object – поділюваний об’єкт # спільно використовуваний об'єкт # об’єкт комп’ютерної системи, який одночасно або почергово використовується різними користувачами і (або) процесами.

shared secret – секрет сумісного використання # секрет, який використовується при перевірці автентичності, який відомий тільки об'єкту і перевіряючому.

shattered virus – роздроблений вірус # вірус комп’ютерний, програма якого розділена на частини, які на перший погляд не мають між собою логічного зв’язку. Ці частини містять інструкції, які вказують комп’ютерові, як їх зібрати разом, в якій послідовності і якому випадку або в який час відтворити вірус і коли розмножити його (принцип “Троянського коня”).

shell site – 'холодне' резервне виробниче чи офісне приміщення # технічні засоби, принаймні з обладнанням, необхідним для підтримки встановлення і експлуатації альтернативної системи опрацювання даних.

shielding – екранування # дія, спрямована на реалізацію захисту кого-, що-небудь екраном від зовнішнього впливу, шкідливого діяння і т. ін.

shielding sideways fields – екранування побічних полів # локалізація побічних полів, що породжуються при роботі радіоелектронних засобів, в межах зони контрольованої шляхом екранування джерел поля.

Розрізняють наступні способи екранування: екранування електричного поля; екранування магнітного поля; екранування електромагнітне.

short-term key – короткостроковий ключ # ключ, криптоперіод якого має відносно невелике значення.

SI system – система SI # розпізнавач мови відкритий для незареєстрованих користувачів, який може надійно працювати з користувачами, які рідко чи ніколи його не застосовували.

SIEM - security information and event management – технологія керування інформаційною безпекою та подіями безпеки.

side effect – побічний результат # будь-які непрямі наслідки, викликані виконанням виразу, оператора чи підпрограми. Побічні результати можуть бути застосовані, наприклад, для зміни значення даних параметра, переданого функцією.

sign – ознака # 1. показник, прикмета, знак, за якими можна упізнати, визначити будь-що # 2. в обчислювальних системах – значення, що задаються при пошуку даних.

signal – сигнал # зміна фізичної величини, яка застосовується для подання даних.

signal dynamic range – динамічний діапазон # відношення найбільшого і найменшого миттєвих значень потужності або напруги сигналу, яких він реально може набувати в процесі вимірювання. Як правило, використовують логарифм цього відношення.

signal element – елемент сигналу # кожна з частин, що складають дискретний сигнал і відрізняється від інших одним або кількома характерними величинами # наприклад амплітуда, форма сигналу, тривалість та положення за визначений час.

signal feature – ознаки сигналів # ознаки, що описують параметри полів і сигналів, що генеруються об’єктом: їхні потужність, частота, вид (аналоговий, імпульсний), ширина спектра і т.ін. Зумовлені тим, що будь-яке матеріальне тіло з температурою, вищою абсолютного нуля випромінює електромагнітні поля, створювані тепловим рухом електронів атомів речовини. Крім того, об’єкт може містити створені штучно джерела полів або електричного струму. У складі об’єкта можуть знаходитися радіоактивні речовини. Радіоелектронні засоби випромінюють функціональні та побічні електромагнітні поля, механічні рухи частин приладів і машин створюють акустичні поля.

signal regeneration – відновлювання сигналу # трансформація сигналу, яка відновлює сигнал до його відповідних вихідних характеристик.

signal shaping – формування сигналу # дія, що змінює одну чи кілька характеристик сигналу, наприклад максимальне значення, форму чи час.

signal source – джерело сигналу # складова частина об'єкта, що випромінює сигнал. Джерело сигналу містить інформацію про ознаки сигналу. Якщо об'єкт відбиває поля зовнішніх джерел, то він одночасно стає джерелом інформації про об'єкт і джерело сигналу. В цьому випадку сигнал містить інформацію про ознаки об'єкта видові або сигнальні.

signal spectrum – спектр сигналу # сукупність гармонічних складових сигналу. Для періодичного сигналу будь-якої форми амплітуда кожної спектральної складової характеризує енергію відповідної гармоніки основної частоти сигналу. Чим більша швидкість зміни амплітуди сигналу, тим більше у його спектрі високочастотних складових. Різниця між максимальною і мінімальною частотами спектру сигналу, між якими зосереджена основна частина енергії сигналу, називається шириною спектра сигналу. Частоти складових спектра неперіодичного сигналу безперервно змінюються. Тому при спостереженні спектра такого сигналу положення і рівень різноманітних спектральних складових безперервно змінюються і спектр виглядає як суцільний.

signal transformation – трансформація сигналу # дія, що змінює одну чи кілька характеристик сигналу, наприклад максимальне значення, форму чи час.

signal(l)ing – сигналізація # подавання сигналу попередження про будь-що, наприклад, застереження про небезпеку.

signalling gateway – шлюз сигналізації # перетворювач форматів сигналізації на межі пакетної мережі і мережі з комутацією каналів, функції якого можуть бути інтегровані у медіа шлюзі.

signature – підпис # конкретний фрагмент тексту, в кінці тіла, розроблений ініціатором для індивідуальної ідентифікації. Підпис зазвичай містить назву, адресу та може також містити номери телефону та факсу. Підпис може містити цифровий підпис або інші дані, що автентифікують повідомлення # див. digital signature.

signature code – підпис коду # механізм, що дозволяє підписувати програмне забезпечення, що розповсюджується мережами загального користування. Підпис коду дозволяє автентифікувати автора програмного забезпечення і гарантувати, що у процесі передавання код не модифікувався.

signs of preparation for armed struggle in psychological warfare field – ознаки підготовки до збройної боротьби в галузі психологічної війни # значне підсилення протиборства між імовірними противниками в сфері інформаційній; бойове розгортання органів психологічної боротьби; початок здійснення операцій психологічних.

signs of substances – ознаки речовин # ознаки, що визначають фізичний і

хімічний склад, структуру і властивості речовин матеріального об'єкта. Демаскуючі ознаки речовин. містяться не тільки в кінцевому продукті, але і в тих вихідних та проміжних продуктах технологічного процесу одержання цієї речовини. Ознаки речовин можуть поділятися на ознаки складу речовини, ознаки побудови речовини та ознаки властивостей речовини.

SIM – subscriber identity module – модуль ідентифікації абонента.

simple buffering – проста буферизація # техніка присвоєння буферного сховища на час виконання комп'ютерної програми.

simple mail transfer protocol – протокол простого перенесення пошти # протокол з протокольного стеку TCP/IP, який визначає правила переносу повідомлень електронної пошти і формати повідомлень керування цим переносом.

simple network management protocol – протокол простого керування мережею # протокол з протокольного стеку TCP/IP, який забезпечує контроль і керування IP-шлюзами та іншими мережними елементами.

simple response – просте реагування # реакція системи захисту інформації на несанкціоновані дії в інформаційно-обчислювальній мережі (ІОМ). Просте реагування може включати наступні дії: сигналізацію про доступ несанкціонований; блокування (вимкнення термінала, групи терміналів, елементів 10М і т. ін.); відмову в запиті.

simplex transmission – симплексне пересилання # пересилання даних тільки в одному попередньо визначеному напрямку.

simulation – імітаційне моделювання # використання системи опрацювання даних для подання вибраних поведінкових характеристик фізичної чи абстрактної системи # наприклад подання повітряних потоків навколо деталей з аеродинамічним профілем при різних швидкостях, температурах та тиску повітря.

single attack – разова атака # атака на мережу обміну інформацією віддалена, що полягає в проведенні обмежених у часі цілеспрямованих впливів на об'єкти мережі обміну інформацією.

single information space of state – єдиний інформаційний простір держави # сукупність баз і банків даних, технологій їхнього ведення і використання, інформаційно-телекомунікаційнихмереж і систем, які функціонують на основі єдиних принципів і за загальними правилами, що забезпечують інформаційну взаємодію організацій і громадян, а також задоволення їхніх інформаційних потреб. Єдиний інформаційний простір держави формують з наступних головних компонентів: ресурсів інформаційних, що містять дані, відомості і знання, зафіксовані на відповідних носіях інформації; організаційні структури, що

забезпечують функціонування і розвиток єдиного інформаційного простору, тобто збирання, оброблення, зберігання, розповсюдження, пошук і передачу інформації; засоби інформаційної взаємодії громадян і організацій, які забезпечують їм доступ до інформаційних ресурсів на основі відповідних інформаційних технологій, включаючи програмно-технічні засоби і організаційно-нормативні документи. Організаційні структури та засоби інформаційної взаємодії утворюють інфраструктуру інформаційну.

single-level device – однорівневий пристрій # функційний блок, який в певний час може обробляти дані лише одного рівня безпеки.

SIP – session initiation protocol – протокол ініціювання сеансу.

situational center – ситуаційний центр # постійний чи тимчасово діючий орган, призначений для колективного прийняття рішень, як правило, в надзвичайних ситуаціях.

SLA – service level agreement – угода про рівень обслуговування.

SMAE – systems management application-entity – сутність-прикладна задача системного адміністрування.

smart card – смарт-картка # інтелектуальна картка # картка з мікросхемою, що являє собою повний мікрокомп'ютер (мікроконтролер) з операційною системою, програмним забезпеченням і системою захисту даних.

SMI – structure of management information – структура інформації керування.

SMTP simple mail transfer protocol – протокол простого перенесення пошти.

snapshot dump – миттєвий знімок # копія всіх або частини даних, що містяться в пам'яті чи в базі даних у певний момент часу.

sniffing – аналіз трафіка # див. traffic analysis.

SNMP – simple network management protocol – простий протокол керування мережею.

social stereotype – соціальний стереотип # звичний, усталений спосіб духовної діяльності, стійкі форми й оцінки соціальних об'єктів та явищ, нормативні утворення групової і суспільної свідомості.

society safety – безпека суспільства # наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи усіх груп населення і протистояти діям, що ведуть до розколу суспільства (у тому числі і зі сторони держави).

soft copy – недокументальна копія # тимчасове виведення інформації в аудіо чи візуальному форматі # наприклад дисплей з катодним променем.

soft error – випадковий збій # помилка, яка зустрічається час від часу й може не з'являтися при послідовних спробах зчитування даних.

soft sectoring – гнучке розбиття на сектори # визначення границь сектору на магнітному диску за допомогою записаних даних.

softswitch – софтсвіч # об'єкт мережі, який виконує функції керування викликами у розподіленій пакетній системі комутації.

software documentation – програмна документація # документація програмного забезпечення # частина документації проектної, яка містить рішення із застосування програм і забезпечення програмного в цілому. Призначена для користувачів # див. software documentation.

software environment – програмне середовище # програмні засоби, з якими взаємодіє програма або система.

software library – бібліотека програм # керована колекція програмного забезпечення та відповідної документації, призначених для розробляння, використання чи технічного обслуговування програмного забезпечення.

software lock – захист програми # сукупність умов, що запобігають запуску програми на виконання.

software package – програмний пакет # повний та документально підтверджений набір програм, що поставляють кільком користувачам для загального застосування чи призначення. Деякі програмні пакети можуть змінюватися для певної програми.

software piracy – незаконне використання програмного забезпечення # незаконне використання чи копіювання програмних продуктів.

software piracy – програмне піратство # несанкціоноване використання, копіювання чи розповсюдження програмних продуктів.

software trap – програмна пастка # програмна закладка, що використовує помилки або неоднозначність у програмному забезпеченні.

sonar intelligence – гідроакустична розвідка # hydroacoustic intelligence.

sound insulator – звукоізоляційні матеріали # матеріали акустичні, призначені для використання в конструкціях міжповерхових перекриттів, у внутрішніх стінах і перегородках, а також у вигляді віброізоляційних прокладок під машини та обладнання. Звукоізоляційні матеріали виготовляють з штучних волокон (мінераловатні і скловолокнисті мати і плати), а також з еластичних газонаповнених пластмас (пінополіуретан, пінополівінілхлорид і т. ін.). Для звукоізоляції застосовують також штучні прокладки з литої або губчастої гуми.

sound location – шумопеленгування # виявлення та визначення координат плаваючих засобів за їхніми шумами. Інша назва – пасивна гідролокація.

sound record – аудіальний документ # див. audio document.

sound spectrum – спектр звуку # сукупність гармонічних складових

звукових хвиль. Основна частота спектра визначає при цьому сприйняту на слух висоту звуку, а набір гармонічних складових – тембр звуку. В спектрі звуку мови наявні форманти — стійкі групи частотних складових, що відповідають певним фонетичним елементам.

sound-absorbing material – звукопоглинальні матеріали #матеріали, що використовуються для перетворення кінетичної енергії звукової хвилі в теплову енергію. Звукопоглинальні властивості матеріалів оцінюються коефіцієнтом звукопоглинання. Використовуються для створення засобів звукопоглинання хвилі акустичної. За конструктивними властивостями розрізняють рихлі акустичні матеріали, плитні матеріали, акустичну штукатурку і резонансні поглиначі у вигляді панелей і щитів з дерева та інших матеріалів.

sounding – зондування # див. probe, reconnaissance.

soundproofing criterion – показник звукоізоляції # показник, що характеризує величину ослаблення *R* в дБ акустичної хвилі засобами звукоізоляції акустичного сигналу: $R = 10 \cdot lg(P_1/P_2)$, де P_1 – потужність падаючої на засіб звукоізоляції акустичної хвилі, P_2 – потужність акустичної хвилі, що пройшла через цей засіб.

source – джерело # те, що дає початок чому-небудь, звідки виходить що-небудь.

source environment – інструментальне середовище # сукупність інструментальних засобів, що охоплюють весь цикл розробки програми або системи.

source of information impact – вплив джерела інформації # складова частина впливу переконуючого. Ефективність такого впливу залежить від того, як люди, що його сприймають, відносяться до джерела інформації. В ході війни психологічної джерелами інформації можуть бути: уряд і керівництво збройних сил своєї країни; особи, авторитетні для об’єкта переконуючого впливу; органи психологічної війни. Власний уряд і воєнне керівництво використовуються як джерела інформації тоді, коли треба повідомити населенню і військам противника урядові заяви, ультиматуми або іншу важливу офіційну інформацію. Вплив таких джерел ефективний у випадку, коли інформаційно-пропагандистські матеріали доставляються вчасно. Крім того, заяви й заклики офіційних джерел найбільш дійові тоді, коли загальна політична ситуація заплутана, або противник не впевнений у сприятливому для нього закінчення війни. Авторитетними джерелами інформації можуть найрізноманітніші люди, наприклад, церковні діячі, популярні журналісти, військовополонені і т. ін. Представники органів психологічної війни як джерела інформації

використовуються доволі рідко, за виключенням випадків, коли психологічний вплив здійснюється на населення союзних країн або в ході миротворчих операцій.

source of information reliability assessment – оцінка надійності джерела інформації # показник достовірності інформації, що характеризує відсутність в ній елементів дезінформації. В першому наближенні джерело інформації оцінюється за багаторівневою шкалою, наприклад: цілком надійне; звичайно надійне; доволі надійне; не завжди надійне; ненадійне; надійність не може бути визначена.

source schema – схема джерела # визначення даних або набір визначень даних перед трансформацією у схему.

space – простір # протяжність, місце, не обмежене видимими краями.

spam – спам # незапитувані листи електронної пошти, вміст яких може бути деструктивним та/або шахрайським

span – інтервал # різниця між найвищим та найнижчим значенням, яке може приймати величина чи функція.

spatial condition of reconnaissance contact – просторова умова розвідувального контакту # умова, що передбачає таке просторове розташування розвідника відносно джерела інформації, при якому розвідник «бачить» джерело інформації.

speaker-adaptive system – система, адаптована до голосу # незалежна від спікера система, здатна модифікувати та оновлювати свій шаблон мови, для відстеження відмінностей між зразками мови, та підвищення своєї продуктивності. Можливість покращення продуктивності є своєрідним навчанням.

speaker-dependent recognition – розпізнавання, залежне від голосу # розпізнавання зразків мови зареєстрованого користувача чи групи користувачів, засноване на попередньому навчанні на своїх моделях мови.

speaker-dependent system – система, залежна від голосу # система розпізнавання мови, обмежене зареєстрованим користувачем або групою користувачів, яка потребує попередньої підготовки до їхніх моделей мови # наприклад одноголосна система, мультиголосна система.

speaker-independent recognition – розпізнавання, незалежне від голосу # розпізнавання зразків мови від будь-якого користувача без попередньої підготовки до його чи її моделей мови.

speaker-independent system – система, незалежна від голосу # розпізнавач мови відкритий для незареєстрованих користувачів, який може надійно працювати з користувачами, які рідко чи ніколи його не застосовували.

speaker-trained system – система з голосовим навчанням # система розпізнавання мови, обмежене зареєстрованим користувачем або групою користувачів, яка потребує попередньої підготовки до їхніх моделей мови # наприклад одноголосна система, мультиголосна система.

speaking mode – розмовний режим # будь-який з трьох способів розмови для розпізнавання мови, а саме: режим ізольованих слів, режим суміжних слів або режим неперервного мови.

special importance information – відомості особливої важливості # відомості у галузі воєнної, зовнішньополітичної, економічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, розповсюдження яких може нанести шкоду державі в одній або декількох із перелічених галузей.

special influence – спеціальний вплив # вплив на технічні засоби, що призводить до здійснення загрози для інформації.

special operation – спеціальна операція # термін для позначення підривних і диверсійних операцій.

special resistance – спеціальна опірність # опірність навіюванню, що має більш вузьку сферу дії, аж до відношення до конкретної людини або до конкретної інформації. Наприклад, людина, вихована на певних принципах, не буде сприймати інформацію, що суперечить їм.

specific characteristics of information – специфічні характеристики інформації # інформація існує віртуально, а не фізично; вона є нескінченним ресурсом, може знаходитися одночасно в декількох місцях і використовуватися декількома її власниками; інформація, що являє сама по собі тільки масив фактів, зібраних різними способами, і які не відрізняються точністю і вірогідністю, повинна бути перетворена в знання; при правильному обробленні, аналізі і узагальненні інформація перетворюється в засіб швидкого і адекватного реагування на обстановку, що змінюється; інформація нелінійна за своїм характером: великий обсяг даних може не дати ніякого ефекту, тоді як коротке повідомлення, представлене невеликою кількістю даних, може змінити хід історії; інформація не визнає міжнародних кордонів і не має формальних границь; одна і та ж інформація або одне і те ж її джерело часто може використовуватися будь-якою з конфліктуючих сторін.

specific indication object – видові ознаки об’єкта # форма об’єкта, його розміри, деталі об’єкта, тон, колір і структура його поверхні і т.ін. Видові ознаки об’єкта описують зовнішній вигляд об’єкта. Вони об’єктивно йому властиві, але виявляються в результаті аналізу

зовнішнього вигляду моделі об’єкта – зображення його на екрані оптичного приймача (сітківки ока людини, фотознімкові, екрані телевізійного приймача, приладу нічного бачення і т. д.). Так як модель в загальному випадку відрізняється від оригіналу, то склад і значення видових ознак залежить не тільки від об’єкта, але і від умов спостереження і характеристик оптичного приймача. У зв’язку з цим розрізняють ознаки об’єкта видові у діапазоні випромінювання оптичного (видимого та інфрачервоного) і діапазоні радіовипромінювання.

specification – **1.** специфікація # *1.* детальне формулювання, у формі документа, яке забезпечує остаточний опис системи для її розробляння чи перевірки # *2.* формалізований опис властивостей, характеристик і функцій об’єкта # **2.** умова # див. condition.

specification language – мова специфікацій # проблемнозорієнтована мова, найчастіше комп'ютерно-оброблюване поєднання природної мови та штучної мов, яке застосовується для вираження вимог, архітектури, поведінки чи інших характеристик системи чи компоненти, і яка забезпечує спеціальні мовні конструкції та, іноді, протоколи верифікації, застосовувані для розробляння, аналізу та документавання перерахованих логікових об'єктів.

specification of guarantees level – специфікація рівня гарантій # специфікації, що визначають заявлений рівень гарантій захисту продукту інформаційних технологій і його відповідність вимогам гарантій безпеки у вигляді подання параметрів технології проектування й створення ІТ-продукту. Ці параметри повинні бути представлені у форматі, що дозволяє визначити їхню відповідність стандартним вимогам гарантій «загальних критеріїв».

specification of security features – специфікація функцій захисту # специфікації, що описують функціональні можливості засобів захисту продукту інформаційних технологій та заявлені його розробником як такі, що реалізують декларовані вимоги безпеки. Форма подання специфікацій повинна дозволяти визначити відповідність між функціями захисту і і вимогами безпеки.

spectrum – спектр # 1. сукупність всіх значень будь-якої величини, що характеризує систему або процес # наприклад: оптичний спектр, акустичний спектр, спектр електромагнітних хвиль, спектр радіочастот # 2. кольорова смуга, що утворюється від розкладу білого світла.

spectrum analyzer – аналізатор спектру # прилад для візуального спостереження і вимірювання параметрів амплітудних, середніх за потужністю та фазових спектрів

сигналів. За методом апаратурного спектрального аналізу розрізняють аналізатор спектру паралельного (одночасного), послідовного та змішаного аналізу, а за принципом дії – аналогові та цифрові аналізатори спектру. Основними характеристиками аналізатор спектру є: діапазон частот, смуга огляду, роздільна здатність, чутливість, динамічний діапазон вхідних сигналів, час аналізу, основні похибки вимірювання частотних інтервалів і вимірювань амплітуд (потужностей) спектральних компонентів тощо. Аналогові аналізатори спектру можуть бути реалізовані на різних принципах (дисперсійному, рециркуляційному, акустооптичному тощо), хоча на практиці найпоширенішими є фільтрові методи паралельного і послідовного аналізу.

speech – мовлення # голосові зразки в заданій природній мові чи акустичних сигналах, що імітують такі зразки.

speech processing – опрацювання мовлення # опрацювання мовних сигналів, таке як аналіз мови, стиснення мовної інформації, розпізнавання мови та синтез мови.

speech recognition – розпізнавання мовлення # перетворення, функційним модулем, мовленевого сигналу в подання контенту мови.

speech recognition – розпізнавання мовлення # сприйняття та аналіз, функційним модулем, інформації, пересланої людським голосом.

speech recognition system – система розпізнавання мовлення # функційний модуль для розпізнавання мовлення. Розпізнавач мови містить аналізатор мови серед своїх компонентів і зазвичай відповідає введенню голосу з характеристичними параметрами зразків мови.

speech recognizer – розпізнавач мовлення # функційний модуль для розпізнавання мовлення.

speech synthesis – синтез мовлення # генерування штучного мовлення.

speech synthesis system – системи синтезу мовлення # функційний блок для синтезу мовлення.

speech synthesizer – синтезатор мовлення # функційний блок для синтезу мовлення.

speech template – шаблон мовлення # набір попередньо записаних або заснованих на правилах голосових характеристик, що зберігаються у функційному блоці для майбутніх довідкових або узгоджувальних цілей.

speech-pattern matching – збіг шаблонів мовлення # збіг зразків мовлення # співставлення характеристичних параметрів, видобутих з пробного мовного зразка з шаблонамии мовлення, попередньо записаними в словник розпізнавання.

sphere – сфера # 1. область фізичного або духовного життя, діяльності людини або суспільства # 2. сукупність точок, рівновіддалених від даної точки (центра сфери).

spiral track – спіральна доріжка # доріжка на диску спіральної форми, що є частиною методу захисту від копіювання.

SPIT – spam over IP telephony – спам через IP-телефонію.

spoken-language identification – розпізнавання розмовної мови # розпізнавання мови чи діалекту, що вимовляє людина, з використанням мовних зразків цієї особи.

spoof – фальсифікувати # вживання заходів для того, щоб увести в оману користувача, спостерігача (наприклад, підслуховувача) або ресурс.

spoofing – спуфінг # підробка # процес, в ході якого відправник підроблює свої початкові дані, щоб можна було подумати, що пакет приходить з будь-якого іншого місця. Також називається підробка адреси.

sprout – паросток # в криптології – випадкова послідовність x, що подається на вхід псевдовипадкового генератора. Під «випадковістю» розуміється, що x є реалізацією випадкової величини X рівномірно розподіленої на множині $/0,1/^{\infty}$. Звичайно, паросток – це теоретичне поняття. За добре наглих який задовольняє певним вимогам. Інша назва зерно.

spurious aiming – паразитне наведення # передача електричних сигналів з одного елемента радіопристрою в інший, не передбачена його схемою і конструкцією. Паразитні наведення виникають через індуктивні і ємнісні паразитні зв'язки. Паразитні наведення створюють загрозу безпеці інформації у випадку наведень на кола, що мають вихід сигналів з інформацією, що належить захисту, за межі зони контрольованої. Найбільшу загрозу створюють наведення в проводах кабелів телефонної мережі, радіотрансляції, електроживлення від сигналів розташованих поряд кабелів, по яких передається конфіденційна інформація. Крім того, наведення дуже малого рівня можуть модулювати високочастотний сигнал, що розповсюджується за межі контрольованої

spurious electromagnetic emission and breakthrough – випромінювання і наведення електромагнітні побічні # *1.* Випромінювання електромагнітне і наведення паразитні, що виникають при функціонуванні будь-яких радіоелектронних і електричних пристроїв та приладів і утворюють джерела небезпечних сигналів, які можуть містити інформацію, що потребує захисту # *2.* в обчислювальних мережах – електромагнітне випромінювання засобів мікропроцесорної та обчислювальної техніки, створення якого не є призначенням цих засобів, але яке має місце в процесі їхнього функціонування і може бути носієм інформації, зокрема, про процес оброблення даних. Здійснення реєстрації цієї інформації розглядають як загрозу.

spy – шпигун # розвідник # 1. таємний агент, що займається шпіонажем # 2.

особа, що таємно слідкує за будь-ким, вистежує будь-кого # див. intelligence agent, secret service man, scout, reconnaissanceman.

SSH – secure shell – безпечна оболонка.

stability – стійкість # здатність витримати зовнішній вплив, протидіяти чомусь.

stakeholder – акціонер # особа чи організація, яка на прийняття рішень або виконання дій може впливати, на яку можуть впливати або яка відчуває можливість впливу на неї.

standard – стандарт # 1. норма, зразок, мірило # 2. прийнятий організацією відповідної компетенції тип виробів, що відповідає певним вимогам за якістю, хімічним складом, фізичними властивостями, вагою, розміром, об'ємом тощо # 3. нормативно-технічний документ, який регламентує вимоги і правила до виробів, технологічних процесів і прийнятий відповідної компетенції організацією як офіційний документ.

state administration – державне адміністративне керування # див. government management.

state information security – інформаційна безпека держави (суспільства) # ступінь захищеності держави (суспільства) та стійкість основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т. ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т. ін.) впливів інформаційних, причому як з упровадження, так і добування інформації. Інформаційну безпеку держави визначають здатністю нейтралізувати такі впливи. В основу забезпечення інформаційної безпеки держави повинні бути покладені наступні принципи: законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки.

state intelligence – державна розвідка # розвідка, яка ведеться з метою забезпечення керівництва країни інформацією, необхідною для прийняття ним політичних, економічних, воєнних, науково-технічних рішень в умовах жорсткої міждержавної конкуренції. Основними сферами інтересів державної розвідки є: стан воєнно-економічних і науково-технічних потенціалів інших держав, насамперед, потенційних противників, і прогнозування їхнього розвитку; розташування воєнно-технічних об'єктів, їхні виробничі потужності, характер і розподіл продукції, що випускається; зміст і характер робіт, що ведуться в галузі створення нових видів озброєння і військової техніки; склад і дислокація угруповань військ і сил флоту; ефективність озброєння і військової техніки, їхні тактико-технічні характеристики; масштаб навчань, що проводяться, склад сил та засобів, що залучаються до них, зміст завдань, що вирішуються на

навчаннях; принципи побудови і технічного оснащення систем державного і воєнного управління; інженерне обладнання континентальних і навігаційно-гідрографічне забезпечення морських і океанських театрів воєнних дій; наявність паливо- енергетичних, рудних, водних, рослинних та інших природних ресурсів; метеорологічні умови на території держав, що розвідуються; виконання умов міжнародних договорів, насамперед, про обмеження озброєнь. Крім того, органи державної розвідки добувають великі об'єми різноманітної інформації, аж до стану здоров'я, характеру, звичок, стилю мислення політичних і військових керівників іноземних держав.

state intelligence agency – орган державної розвідки # органи розвідки, створені державою для забезпечення керівництва країни інформацією, необхідною для прийняття ним політичних, економічних, воєнних, науково-технічних рішень в умовах жорсткої міждержавної конкуренції. Структура органів державної розвідки залежить від цілей держави, її зовнішньої політики та можливостей.

state secrets protection agency – орган захисту державної таємниці # органи державної влади, підприємства, заклади і організації та їхні структурні підрозділи, які взяли на себе зобов'язання або зобов'язані відповідно до свого статусу виконувати вимоги законодавства держави про державну таємницю.

state security – безпека держави # положення, при якому державі не загрожує небезпека. Досягають наявністю ефективного механізму управління і координації діяльності політичних сил та суспільних груп, а також активних інститутів (органів) їхнього захисту.

stationary random process – випадковий стаціонарний # процес випадковий, властивості якого не залежать від часу.

stealth virus – вірус-невидимка # комп'ютерний вірус , що використовує спеціальні алгоритми, які маскують його присутність на диску (у деяких випадках і в оперативній пам'яті).

steganalytic attack – стегоаналітична атака # загальна назва методу, яким стегоаналітик намагається зламати стеганографічну систему. Стегоаналітичну атаку поділяються за критерієм інформації, яка відома противникові з відомим контейнером, з вибором контейнера, з відомою стеганограмою (стего), з обраною стеганогра- мою, з відомим прихованим повідомленням, з обраним прихованим повідомленням; за метою порушника виявлення прихованих повідомлень стегоключів), руйнування прихованих повідомлень, які поділяються на стиск стеганограми з утратою даних, геометричні

перетворення стеганограми, зашумлення контейнера, фільтрація.

stegoanalysis – стегоаналіз # наука про вивчення методів виявлення існування секретної інформації у відкритих повідомленнях. В с. розрізняють дві основних стратегії дій противника (стегоаналітика): пасивну та активну. При пасивній стратегії противника намагається тільки виявити факт існування і власне секретну інформацію, при активній – знищити таку секретну інформацію у відкритому повідомленні.

stereotype – стереотип # 1. те, що часто повторюється, стало звичайним, загальноприйнятим і чого дотримуються, що наслідують у своїй діяльності; стандарт, трафарет, догма, норма, канон # 2. розповсюджені в певних соціальних і етнічних групах схематизовані уявлення про факти дійсності, що обумовлюють надто спрощені (як правило – неадекватні реальності) оцінки й судження представниками цих груп. Вони формуються в результаті неодноразового смислового й емоційного акцентування свідомості людей на цих або інших явищах і подіях, багаторазового їхнього сприйняття і закарбовування у пам'яті. Стереотип найчастіше відображає не суттєві, а зовнішні, найбільш помітні, найбільш яскраві риси явищ або подій. Будь-яка оцінка останніх, відповідно до с., приймається без доказів і вважається правильною, тоді як всяка інша піддається сумніву. Стереотипи виникають в індивідуальній, груповій і суспільній свідомості в результаті впливу не тільки навколишнього середовища, але і внаслідок сприйняття досвіду, поглядів, суджень інших людей. Стереотипи можуть стати об'єктами впливу психологічного. їхня трансформація є одночасно і передумовою дії такого впливу, і умовою, дотримання якої дозволяє змінювати поведінку людей.

stereotyped thinking effect – ефект стереотипності # психологічний ефект, що виражається у спрощеному й схематичному, але стійкому уявленні про будь-що (або будь-кого). Стереотипи стихійно формуються в умовах дефіциту інформації, або нездатності індивіда інтерпретувати її адекватно. Стереотип ніколи не буває істинним, він завжди містить тенденційні, наперед задані характеристики явища, тому завжди неадекватний йому. Стереотип узагальнює явища за принципом зовнішньої подібності або випадкового збігу, проте не аналізує його глибинну сутність.

stethoscope – стетоскоп # пристрій для прослухування розмов через стіни. Стетоскоп являє собою вібродатчик, підсилювач та головні телефони. Може оснащуватися проводовим, радіо або іншим каналом передавання інформації.

stochastic process – стохастичний процес # випадковий процес # див. random process, probability process.

stolen phone fraud – шахрайство з украденим телефоном # несанкціоноване використання вкраденого або загубленого апарата стільникового зв'язку.

storage – накопичувач # див. accumulator.

storage image – дублювання вмісту пам'яті # представлення комп'ютерної програми та пов'язаних з нею даних, які існують на той час, коли вони знаходяться в оперативній пам'яті.

storage medium – запам'ятовуюче середовище # див. environment.

storage protection – захист [зовнішньої] пам'яті # захист запам'ятовувача # обмеження доступу до пристрою зберігання даних або до одного чи кількох місць зберігання, запобігаючи записуванню чи зчитуванню чи і тому і іншому.

storage protection key – ключ захисту пам'яті # код, який присвоюється блоку пам'яті, що виділений програмі, і використовується при зверненні програми до пам'яті з метою її захисту. Ключ захисту пам'яті повинен збігатися з ключем захисту; у противному випадку завдання завершується в аварійному режимі.

stored data – дані, що зберігаються # дані, розташовані на зовнішньому носії або в постійно-запам'ятовуючому пристрої.

strategy – стратегія # 1. мистецтво підготовки і ведення великих воєнних операцій # 2. мистецтво суспільного і політичного керівництва масами, яке має визначити головний напрям їхніх дій, вчинків # 3. спосіб дій, лінії поведінки кого-небудь.

stream encipherement – шифрування потокове # спосіб шифрування даних, при якому кожний знак шифрується незалежно.

stress analyzer – детектор брехні # *1.* засіб, призначений для перевірки правдивості людей. Визначення брехні засновується на тому факті, що людина, яка говорить неправду, відчуває в цей момент деякий психологічний стрес, що викликає, в свою чергу, певні фізіологічні зміни в її організмі. Існують три основні типи детектора брехні: поліграф (polygraph, psychological stress evaluator), сигналізатор психологічного стресу (psychological stress signalizer) і аналізатор стресу за голосом (vocal stress analyzer) # *2.* алгоритм роботи деякого людино-машинного комплексу, який дозволяє організувати інформаційну взаємодію з об'єктом, що досліджується, таким чином, щоб у процесі цієї взаємодії виявити наявність у об'єкта, що досліджується, прихованих знань із певної теми.

stress test – стрес-тест # випробування, у якому певні режими роботи змінюються щодо їх номінальних значень, щоб виявити несправності чи їх можливість.

stroke character generator – генератор штрихових символів # генератор символів, який генерує відображення

символів, що складаються з лінійних сегментів.

strong prime number – сильне просте число # просте число *p*, у якого числа $p \pm 1$ мають хоча б один великий простий дільник.

strong pseudoprime number – сильне число псевдопросте # число складене, яке не визначається простим тестом Мілера-Рабіна.

structure – структура # будова # форма # 1. взаєморозміщення та взаємозв'язок складових частин цілого # 2. устрій, організація чого-небудь.

structuring – структурування # визначення внутрішнього устрою чого-небудь.

struggle – боротьба # *1.* активне противенство, зіткнення між протилежними соціальними групами, течіями в суспільстві і т. ін., протистояння # *2.* діяльність, що має на меті подолати або знищити кого-, що-небудь # *3.* діяльність, скерована на створення, досягнення чого-небудь.

stucturization – структурування # див. structuring.

student virus – студентський вірус # украй примітивний, простий вірус комп'ютерний, що містить велику кількість помилок в алгоритмі його побудови і викликає локальні "епідемії". Як правило, такі віруси не набувають широкого поширення, швидко виявляються і знищуються, проте, встигають заподіяти шкоду в місці свого розмноження.

study – аналіз # див. analysis.

stuff – матеріал # див. material

sub-activity – підвид діяльності # застосування компонента довіри # сімейства довіри прямо не розглядаються в цьому стандарті, оскільки при проведенні оцінювання завжди використовується тільки один компонент довіри з застосовуваного сімейства.

subject – суб'єкт # 1. носій певного роду діяльності; джерело активності, спрямованої на об'єкт # 2. особа або організація, що має певні права й обов'язки # 3. активний логіковий об'єкт, який може отримати доступ до інших об'єктів # наприклад процес, який охоплює виконання програми # суб'єкт може викликати пересилання інформації між об'єктами чи може змінити стан системи опрацювання даних.

subject authentication – автентифікація суб'єкта # функція захисту, в результаті виконання якої з певними гарантіями виконують підтвердження суб'єкта заявленим про себе характеристикам (наприклад, ідентифікаторові).

subject of legal regulation in information sphere – суб'єкт правового регулювання в інформаційній сфері # юридичні і фізичні особи, які створюють (продукують) і споживають інформацію; юридичні і фізичні особи, які розробляють і застосовують системи інформаційні, технології і засоби їхнього забезпечення; органи державної влади і місцевого самоврядування;

інформаційні організації, підприємства, заклади, які формують ресурси інформаційні і надають користувачам інформацію з них.

sublayer – підрівень # підрозділ рівня.

subnetwork-address – адреса підмережі # ідентифікатор, наданий уповноваженим по реєстрації підмережі точки підключення підмережі.

subscribed QoS – підписана якість обслуговування # якість обслуговування, параметри якої встановлені за узгодженням з користувачем і внесені в профіль якості обслуговування. Користувач не може самостійно модифікувати профіль якості обслуговування, хоча може мати кілька таких профілів.

subscriber – абонент # користувач # користувач, уповноважений застосовувати один або кілька сервісів офісної автоматизованої системи # див. user.

subscriber station – пункт # див. terminal.

subscriber terminal – абонентський пункт # комплекс технічних засобів в системі телеоброблення даних, призначений для обміну інформацією між віддаленим користувачем і ЕОМ; робоче місце віддаленого користувача (абонента). Абонентський пункт забезпечує введення даних, передачу їх лініями зв'язку в ЕОМ і назад, виведення даних.

subscripting – індексація # посилання на елемент масиву за допомогою матричного посилання та одного чи кількох виразів, які під час оцінювання позначають положення елемента.

subscription fraud – шахрайство з контрактом # надання невірних даних при укладанні контракту, використання послуг у кредит з наміром не сплачувати за них.

substitution – заміщення # шифрування, яке замінює бітові рядки чи рядки символів на інші бітові рядки чи рядки символів # отриманий зашифрований текст називається шифром заміни.

subsystem – підсистема # *1.* елемент ієрархічної структури відкритої системи, який безпосередньо взаємодіє тільки з елементами суміжного вищого чи нижчого рівня структури цієї відкритої системи # *2.* частина системи, яка є сукупністю деяких відносно автономних елементів і разом з тим характеризується підпорядкованістю функціонування всієї системи.

subsystem notification – підсистема сповіщення # частина системи охорони об'єктів, яка повинна сповіщати співробітників служби безпеки, насамперед, охоронців, органи охорони, пожежну охорону тощо про проникнення зловмисників на територію, що охороняється, про пожежу або інші стихійні лиха, захист від яких передбачений завданнями системи. Основу цієї підсистеми складають технічні засоби охорони.

sum – задача # див. problem.

supersector – суперсектор # сектор великого розміру записаний на диск, як частина методу захисту від копіювання.

suppression – блокування # заходи і дії спрямовані на те, щоб силою покласти кінець чому-небудь, знищити, заглушити.

surface – поверхня # зовнішня сторона чого-небудь.

surveillance – розвідка # див. intelligence, scouting, reconnaissance, secret service.

susceptibility – сприйнятливість # здатність реагування на будь-які сигнали, завади тощо.

swapping – підкачування # свапування # процес, який виконує заміну вмісту основної пам’яті з вмістом допоміжного (зовнішнього) запам’ятовувального пристрою.

switch – комутатор # пристрій, що забезпечує з'єднання між мережними пристроями за допомогою внутрішніх механізмів комутації, з технологією комутації, що звичайно реалізовано на другому або третьому рівні еталонної моделі взаємодії відкритих систем

switching – комутування # переключення, встановлення зв’язку.

symbol – символ # 1. умовне позначення будь-якого предмета, поняття або явища. Символи бувають речові, графічні # 2. знак, одиниця алфавіту # 3. послідовність з одного або декількох знаків, що використовуються для позначення чого-небудь.

symbolic address – символьні адреси # ідентифікатори, які представляють адреси.

symmetric binary channel – бінарний симетричний канал # канал, призначений для пересилання повідомлень, що складаються з бінарних символів, і мають властивість рівності умовних ймовірностей зміни одного символа до іншого символа.

symmetric cryptography – симетрична криптографія # криптографія, у якій однаковий ключ застосовується для шифрування та дешифрування.

symmetric cryptosystem – симетрична криптосистема # криптосистема, у якої ключі зашифровування (розшифровування) або однакові, або легко виводяться один з одного, забезпечуючи таким чином спільний ключ.

synchronous data network – мережа передавання даних синхронна # мережа передавання даних, що використовує метод синхронізації передавання між вузлами комутації або між вузлом комутації і апаратурою передавання даних.

synonym – синонім # див. synonymous name.

synonymous name – синонімічне ім'я # ім'я, що ідентифікує об'єкт, що вже ідентифікований іншим індивідуальним ім'ям. Загальні імена синонімів є загальними розпізнавальними іменами, що надані тому ж самому наборові.

syntactic check – синтаксичний # контроль виразів вихідної програми,

що виконується транслятором на етапі синтаксичного аналізу і і має за мету виявлення синтаксичних помилок.

system – система # сукупність об’єктів і відносин між ними, що створюють єдине ціле. Система задається (описується) наступними параметрами (характеристиками): метою і задачами (конкретизованою в просторі і часі метою); входами і виходами системи; обмеженнями, які необхідно враховувати при побудові (модернізації, оптимізації) системи; процесами всередині системи, які забезпечують перетворення входів у виходи.

system administrator – системи адміністратор # особа, що відповідає за експлуатацію системи та підтримку її в працездатному стані.

system analysis – системний аналіз # *1.* аналіз об’єкта дослідження як сукупності елементів, що утворюють систему. У наукових дослідженнях він передбачає оцінку поведінки об’єкта як системи з усіма факторами, які впливають на його функціонування. Системний аналіз можна здійснювати у відповідності до етапів системного аналізу. Кінцевим результатом системного аналізу є побудова моделі системи і розробка пропозицій з її удосконалення або зміни # *2.* аналіз призначення системи, яку передбачають проектувати, і встановлення множини вимог, яким вона повинна відповідати. Єдиної методики системного аналізу в наукових дослідженнях поки що немає. У практиці досліджень його застосовують з використанням таких методик: процедур теорії дослідження операцій, яка дає змогу дати кількісну оцінку об’єктам дослідження; аналізу систем дослідження об’єктів в умовах невизначеності; системотехніки, яка охоплює проектування і синтез складних систем у процесі дослідження їхнього функціонування.

system analysis – системний аналіз # систематичне дослідження реальної чи планової системи для визначення інформаційних вимог та процесів системи та способів їх взаємозв'язку між собою та будь-якою іншою системою.

system analyst – системний аналітик # аналітик в галузі систем операційних, систем програмування, систем автоматизованих.

system approach – системний підхід # методологічний напрям в науці, основне завдання якого складає розроблення методів дослідження і конструювання складноорганізованихоб’єктів – систем різних типів і класів (найчастіше таких, що слабо формалізуються). Системний підхід є певним етапом в розвитку методів пізнання, методів дослідницької і конструкторської діяльності, способів опису і пояснення природи об’єктів, що аналізуються або створюються штучно. Системний підхід реалізують на основі

принципів системного підходу та потребує від фахівців системного мислення. З позиції системного підходу сукупність взаємозв'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації, створює систему захисту інформації.

system approach to information security – системний підхід до інформаційної безпеки # розгляд безпеки інформаційної з позицій підходу системного. Дозволяє підвищити ефективність наукового осмислення проблеми інформаційної безпеки від загрози нових небезпек інформаційних (інформаційно-технічних), зумовлених досягненнями науково-технічного прогресу. Системний підхід потребує визначення і розгляду суб'єктів інформаційної безпеки, засобів і об'єктів інформаційної безпеки, принципів забезпечення інформаційної безпеки, джерел небезпеки інформаційної, напрямків небезпечних інформаційних потоків.

system check – контроль системний # контроль загального функціонування обчислювальної системи в процесі її експлуатації.

system description – опис системи # документація, яка випливає з проекту системи, що визначає організацію, основні характеристики та вимоги до обладнання та програмного забезпечення системи.

system design – проектування системи # процес визначення архітектури апаратного й програмного забезпечення, компонентів, модулів, інтерфейсів та даних для системи, що задовольняють заданим вимогам.

system development – розробляння системи # процес, який зазвичай охоплює аналіз вимог, проектування системи, впровадження, документацію та забезпечення якості.

system documentation – системна документація # колекція документів, які описують вимоги, можливості, обмеження, проектування, експлуатацію та обслуговування системи опрацювання інформації.

system follow-up – аналіз реалізування системи # дослідження впливу системи після досягнення стабілізованого стану експлуатаційного використання.

system integrity – цілісність системи # якість системи опрацювання даних, що виконує свою робочу мету, одночасно запобігає внесенню змін до ресурсів або використання ресурсів несанкціонованими користувачами, та запобігає внесенню неналежних змін або неналежного використання ресурсів уповноваженими користувачами.

system journal – системний журнал # набір даних, в який операційна система записує інформацію, що характеризує хід обчислювального процесу (виконання завдань, опис подій, заміну носіїв, повідомлення операторові і т. ін.).

system key – системний ключ # ключ, що забезпечує захист системних засобів від доступу несанкціонованого.

system maintenance – обслуговування системи # модифікація системи для виправлення несправностей, підвищення продуктивності або адаптації системи до змін середовища чи змінених вимог.

system object – об’єкт комп’ютерної системи # див. product object.

system security – захист системи # сукупність заходів, що вживаються для виключення несанкціонованого доступу до програм і даних системи або випадкового втручання в її роботу.

system security function – функція системи захисту # здатність відкритої системи виконувати обробку, пов'язану з безпекою.

system security object – об'єкт системи захисту # об'єкт, який представляє набір відповідних функцій системи захисту.

system software – системне програмне забезпечення # незалежне від застосування програмне забезпечення, яке підтримує виконання програмного забезпечення прикладного рівня # наприклад операційна система.

system target of evaluation – мета оцінювання системи # операційна система, якою керують у відповідності з її експлуатаційною настановою, включаючи як технічні, так і операційні засоби керування.

system viability – живучість системи # здатність системи до збереження своїх основних функцій, навіть при пониженій ефективності системи, при дії факторів катастрофічного характеру – на відміну від надійності як здатності системи виконувати свої функції в нормальних, наперед заданих умовах.

system vulnerability – вразливість системи # нездатність системи протистояти реалізації певної загрози або сукупності загроз. Вразливість системи може бути наслідком неадекватного проектування чи неповного налагодження системи або результатом злого наміру, наприклад, при наявності «троянського коня».

systemic check authenticity – контроль достовірності системний # метод контролю достовірності оброблення інформації на основі сукупності системних заходів, таких як: оптимізація структури оброблення; підтримання характеристик обладнання в заданих межах; підвищення культури оброблення інформації; навчання і стимулювання обслуговуючого персоналу; створення оптимального числа копій і (або) передісторії! програм вихідних і поточних даних; визначення оптимальної величини пакетів даних і швидкості первинного оброблення, процедур доступу до масивів даних і т. ін.

systems analysis – аналіз систем # систематичне дослідження реальної чи планової системи для визначення інформаційних вимог та процесів системи та способів їх взаємозв'язку між собою та будь-якою іншою системою.

system-title – символьне ім'я системи # ім'я, унікальне в межах середовища

ВВС, що використовується для ідентифікації однієї реальної відкритої системи.

T

table – таблиця # зведення, перелік предметів, розпис відомостей про що-небудь, розміщених у певному порядку, за графами.

tag – атрибут доступу # див. access mediation information.

tailgate – «чорний» вхід # отримання несанкціонованого фізичного доступу, слідуючи за авторизованою особою через контрольовану точку доступу.

target contrast – контрастність об’єктів # контрастність цілей # ступінь відмінності об’єктів спостереження (цілей) на фоні місцевості, води, навколишніх предметів, що дозволяє виявити і розпізнати об’єкти (цілі) візуально, за допомогою інфрачервоних приладів, РЛС, магнітометрів та інших технічних засобів розвідки. Розрізняють оптичну, теплову (інфрачервону), радіолокаційну та магнітну контрастність об’єктів.

task – завдання # див. assignment, job, mission.

task administrator – адміністратор завдань # спеціальна посадова особа, яка входить до складу адміністрації банку даних і виконує підготовку запитів на формування звітів складної форми і змісту. Засобами адміністратора завдань є діалогова (інтерактивна) мова і генератор звітів.

task of choosing a zone of intellectual counteraction – завдання вибору зони інтелектуальної протидії # завдання інтелектуальної протидії, що передбачає реалізацію перерозподілу навантаження на мережу інформаційно-обчислювальну (ІОМ), викликаного інформаційною війною, та оптимізацію розташування в ІОМ вузлів інтелектуальної протидії (центрів безпеки).

task of choosing the kind of intellectual counteraction – завдання вибору виду інтелектуальної протидії # завдання інтелектуальної протидії, яке полягає у попередньому виборі типу стратегії протидії на основі проведеної класифікації несанкціонованого доступу.

task of classifying unauthorized access – завдання класифікації несанкціонованого доступу # завдання інтелектуальної протидії, виконання якого передбачає: класифікацію об’єкта несанкціонованого доступу; класифікацію суб’єкта несанкціонованого доступу; класифікацію зброї інформаційної, що використовується.

task of implementing an intellectual counteraction – завдання здійснення інтелектуальної протидії # завдання інтелектуальної протидії, що охоплює побудову програми інтелектуальної протидії, що здійснює імітацію функціонування об’єкта атаки та власне реалізацію інтелектуальної протидії.

task of protection – завдання захисту # в “загальних критеріях” декларуються наступні завдання: захист від загроз порушення конфіденційності (несанкціонованого одержання) інформації з усіх каналів її витоку, особливо за рахунок каналів побічного електромагнітного випромінювання і наведення та прихованих каналів зв’язку; захист від загроз порушення цілісності (несанкціонованого змінювання інформації); захист від загроз порушення доступності інформації (несанкціонованого або випадкового обмеження інформації й ресурсів самої системи); захист від загроз аудита системи (наприклад, загрози несанкціонованих вторгнень в систему, маніпуляцій з протоколами обміну і і аудита, із загальносистемним програмним забезпеченням).

TCB – trusted computing base – комплекс засобів захисту.

TCP – transmission control protocol – протокол керування передаванням.

TCSC – trusted computer system criteria – китерій безпеки комп’ютерних систем.

TCU – trunk coupling unit – модуль з’єднання з магістраллю.

TDMA – time division multiple access – множинний доступ з часовим розподіленням каналів.

technical channel of information leakage – технічний канал витоку інформації # сукупність носіїв інформації, середовища її поширення та засобів технічної розвідки.

technical compatibility – сумісність технічна # забезпечення автоматичного функціонування комплексу технічних засобів АСОІ різних рівнів, в тому числі обмін інформацією і можливість спільного розв’язання великомасштабних завдань.

technical controls – технічні засоби керування # керування безпекою (тобто засоби захисту і заходи протидії), які переважно запроваджуються і виконуються інформаційною системою за допомогою механізмів, що містяться в апаратних, програмних або мікропрограмних компонентах забезпечення системи.

technical fraud – технічне шахрайство # неправомочне виготовлення телефонних апаратів стільникового зв’язку або платіжних телефонних карток з фальшивими ідентифікаторами абонентів, номерів та платіжних відміток.

technical information security principle – принцип технічного захисту інформації # принципи, що лежать в основі технічного захисту інформації. Поділяються на дві групи: принципи, що визначають загальні вимоги до способів і засобів захисту інформації; принципи, що визначають підходи до організації та забезпечення захисту інформації. До принципів першої групи відносяться принципи, аналогічні принципам добування інформації: принцип безперервності захисту інформації; принцип активності захисту

інформації; принцип скритності захисту інформації; принцип цілеспрямованості захисту інформації; принцип комплексного використання способів і засобів захисту інформації. Принципи другої групи дозволяють забезпечити раціональний рівень захисту інформації та скоротити витрати її організації. Ця група охоплює наступні принципи: принцип відповідності рівня захисту цінності інформації; принцип гнучкості захисту інформації; принцип багатозональності захисту інформації; принцип багаторубіжності захисту інформації. Крім указаних принципів при побудові конкретної системи захисту доцільно враховувати також наступні принципи: мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами захисту інформації; надійність в роботі технічних засобів системи, яка би виключала як нереагування на загрози безпеці (пропуски загроз) інформації, так і на реакції при їхній відсутності; обмежений і контрольований доступ до елементів системи забезпечення безпеки інформації; безперервність роботи в будь-яких умовах функціонування об'єкта захисту, в тому числі при короткочасному вимкненні електроенергії; адаптованість (пристосованість) системи до змін навколишнього середовища. Реалізація вказаних принципів в системі захисту дозволять наблизити її до абсолютної, тобто забезпеченої усіма можливими способами захисту і здатної в будь-який момент свого існування прогнозувати настання загрозливої події за час, достатній для приведення в дію адекватних заходів.

technical intelligence – технічна розвідка # несанкціоноване здобування інформації за допомогою технічних засобів та її аналіз.

technical intelligence model – модель технічної розвідки # формалізований опис мебтодів, засобів та можливостей технічної розвідки.

technical means identification and authentication – ідентифікування і встановлення автентичності технічних засобів # процедура допуску (відмови допуску) до входу в систему користувача з певного термінала. Може здійснюватися за допомогою паролів. Пароль можна використати не тільки для автентифікації користувача і термінала по відношенню до системи, але й для зворотного встановлення автентичності ЕОМ по відношенню до користувача. Це важливо, наприклад, в обчислювальних мережах, коли зв'язок здійснюється з територіально віддаленими об'єктами. В цьому випадку застосовують одноразові паролі або більш складні системи шифрування інформації.

technical protection information level – рівень [технічного] захисту інформації # див. protection information level.

technical protection method – технічний метод захисту # метод захисту, що полягає у використанні технічних засобів.

technical protection of information – технічний захист інформації # діяльність, спрямована на запобігання витоку інформації технічними каналами, її блокуванню та/або порушенню цілісності.

technical protection of information – технічний захист інформації #одна з основних компонент комплексу заходів захисту інформації, що складає державну, службову, комерційну або особисту таємницю. Технічний захист інформації охоплює комплекс нормативно-правових, організаційних і технічних заходів забезпечення безпеки інформації технічними засобами. Він виконує наступні завдання: попередження проникнення зловмисника до джерел інформації з метою її знищення, викрадення або зміни (модифікації); захист носіїв інформації від знищення в результаті впливу стихійних сил і насамперед пожежі і води (піни) при її гасінні; попередження витоку інформації різноманітними технічними каналами.

technical radio analysis – технічний аналіз радіосигналів # визначення умов добування інформації про радіозасоби та їхніх користувачів, що міститься в радіосигналах. Досягнення цієї мети здійснюють виконанням послідовності часткових завдань: визначення параметрів і розпізнавання типів сигналів і повідомлень; визначення інформативності параметрів сигналів як ознак їхніх джерел (інформативність повідомлень визначають на етапі аналізу їхнього змісту). Результати технічного аналізу радіосигналів дозволяють надати рекомендації з пошуку і виявлення, пеленгування, розпізнавання, перехоплення, реєстрації сигналів і повідомлень, а також їхнього оброблення.

technological convergence in information industry – технологікова конвергенція в інформаційній індустрії # конвергенція, викликана тим, що переведена в цифрову форму інформація може передаватися будь-якими засобами комунікацій – телефонними і і кабельними лініями, через супутники, мобільний і безпроводовий зв’язок. Внаслідок технологічної конвергенції розпочалося розмивання границь між традиційно різними секторами індустрії інформаційної – комп’ютерною, телекомунікаційною, засобів масової інформації і т.ін. Технологікова конвергенція й можливість прориву на нові ринки привели до масових об’єднань компаній в двох напрямках: об’єднуються фірми, які зайняті виробництвом змісту (інформаційні агентства, видавничі будинки, кіностудії), і телекомунікаційні оператори, які володіють засобами доставки змісту населенню; зливаються компанії, що володіють

різними частинами інфраструктури інформаційної, – телефонні оператори дальнього й місцевого зв'язку, вироробники комп'ютерів, програмного забезпечення, систем кабельного мовлення, сунуті пікового і і мобільного зв'язку. Мета об'єднань – збільшення капіталу, завоювання нових ринків збуту, підвищення конкурентоспроможності.

Конвергенція технологій і зливання компаній, у свою чергу, приводить до лібералізації законодавчих і нормативних актів, які регулюють традиційно різні сектори інформаційної індустрії.

technological documentation – технологікова документація # документація технічна, що визначає технологічний процес виготовлення або ремонту виробу, комплектацію деталей, матеріалів, оснастки, технологічних документів і маршрут проходження виробу цехами (службами) підприємства. До технологічної документації відносять технологічні карти, відомості і інструкції. Технологічну документацію регламентують стандартами Єдиної системи технологічної документації.

technological environment of automated system – технологічне середовище автоматизованої системи # програмні й апаратні засоби системи автоматизованої, за допомогою яких здійснюються усі операції над інформацією в автоматизованій системі. До технологічног середовища автоматизованої системи також відносять комплекс засобів захисту. Оцінкою технологічного середовища автоматизованої системи є множина $T = \{t_1, t_2 .. t_n\}$, елементами якої є показники, що характеризують його окремі параметри.

technological espionage – технологічний шпіонаж # напрям діяльності розвідки з добування відомостей та інформації про технологічні процеси. Ефективний на короткочасних етапах розвитку економіки, так як високі темпи науково-технічного прогресу дозволяють швидку зміну технологій.

teg – тег # сукупність атрибутів асоційованих із користувачем, процесом або проектом. Тег може бути унікальним ідентифікатором, мітка безпеки або цілісності, ключ криптографічний, Таблиця прав доступу або інші атрибута у відповідності з реалізованою в комп'ютерній системі політикою безпеки.

telecommunication service – мережний сервіс # термін, який включає сервіси перенесення даних (тобто встановлення фізичного чи віртуального з'єднання між терміналами користувачів) та додаткові сервіси, які доповнюють чи модифікують основні сервіси.

telecommunication(s) – телекомунікації # загальна форма електронного обміну інформацією будь-якого типу (даних, телевізійних зображень, факсиміле і т. ін.). Телекомунікації

складають інфраструктуру сучасної економіки. Одна з найбільш важливих тенденцій їхнього розвитку – процес злиття локальних, місцевих і глобальних мереж, який істотно впливає на масштабність економічних процесів, діяльність корпорацій і фірм. Це об'єднання здійснюється на основі технологій Ін- тернету як найбільш зручного засобу взаємодії різноманітних інформаційних систем. Транспортна функція телекомунікацій забезпечує високошвидкісне, надійне переміщення інформації і буде зростати разом із становленням глобальної економіки. В багатьох галузях т. стають необхідним елементом виробництва (банківська справа, телемаркетинг, комп'ютерне проектування і виробництво, торгівля і т. ін.).

teleconference – телеконференція # інтегральний перелік послуг мережі обчислювальної, який використовується з метою комунікації користувачів на основі передавання і оброблення мовної, текстової інформації і відеоінформації.

teleconferencing – телеконференцзв'язок # використання мереж обчислювальних для забезпечення комунікацій між розосередженими групами користувачів.

telefax – телефакс # абонентська система, яка працює на базі телефонної мережі загального користування і призначена для передавання текстів.

telephoto lens – телеоб'єктив # об'єктив з великою фокусною відстанню (300 – 4800 мм), призначений для спостереження (зйомки) на великій відстані від об'єкта спостереження.

teletex – телетекс # система (служба) передавання літеро-цифрової ділової кореспонденції, що побудована за абонентським принципом, в якій як пункти абонентські використовуються комп'ютери персональні або спеціалізовані пристрої.

teletext – телетекст # система одностороннього широкомовного передавання текстової інформації на екрани телевізорів.

teletype – телетайп # телеграфний апарат для приймання повідомлень в цифро-літерній формі.

television broadcast – телевізійне мовлення # одна з найбільш ефективних форм впливу психологічного. Його роль безперервно зростає з розширенням мережі супутникового телебачення, цифрового телебачення, приєднання телебачення до Інтернету. Психологічний вплив за допомогою м. т. має цілий ряд переваг у порівнянні з іншими формами ведення психологічної війни: телевізійне мовлення має найсильніший вплив на формування суспільної думки – ефект присутності, синхронності, причетності глядача до подій, що відбуваються на екрані телевізора,

заставляє його вірити у правдивість поданого йому матеріалу; за допомогою телевізійного мовлення можна показати конкретні епізоди бойових дій, фотодокументи, що пропагують міць і силу своєї зброї або демонструють звірячість противника; телебачення дозволяє передавати факсимільним способом різноманітні друковані видання, в тому числі листівки, в інші країни світу; при неможливості прямої передачі на телевізійні приймачі (або ретрансляції передач) населення і військовополонені можуть дивитися їхні записи за допомогою відеомагнітофонів.

telex – телекс # міжнародна служба зв'язку, що забезпечує обмін повідомленнями між телеграфними апаратами (телетайпами) абонентів через комутований зв'язок загального призначення.

TEMPEST – запобігання витоку інформації через побічні випромінювання і наведення #

template – шаблон # еталонний шаблон, який порівнюєть з цілим або частиною об'єкта, який потрібно визнати. Шаблон застосовують для розпізнавання символів чи мови, виявлення цілей тощо.

template matching – порівняння з еталоном [шаблоном] # зіставлення шаблонів за допомогою еталонів.

tentative check of information security – контроль захисту інформації попередній # контроль захисту інформації, що здійснюється при будь-яких змінах складу, структури і алгоритму функціонування системи захисту інформації, в тому числі: після встановлення нового технічного засобу захисту або зміни організаційних заходів; після проведення профілактичних і ремонтних робіт засобів захисту; після усунення виявлених порушень в системі захисту.

term – термін # слово або словосполучення, що виражає певне поняття якоїсь галузі науки, техніки, мистецтва, суспільного життя тощо.

terminal – пункт # місце зосередження чого-небудь.

terminal – термінал # 1. пристрій для взаємодії користувача або оператора з системою обчислювальною # 2.в мережах ЕОМ – пристрій, що є джерелом або одержувачем даних.

terminal – термінал # функційний блок в системі чи мережі обмінювання даними, через який дані можуть бути введені чи отримані.

terminal mobility – мобільність терміналу # здатність терміналу отримувати доступ до телекомунікаційних послуг у різних місцях та у русі, і здатність мережі ідентифікувати і локалізувати термінал.

terminal node – термінальний вузол # вузол, який не має підпорядкованого вузла.

terminal user – термінала користувача # користувач обчислювальної системи, який взаємодіє з ЕОМ за допомогою термінала.

terminated – завершено # стосується стану виконаної задачі, коли усі

події, що залежать від цієї задачі, було вирішено та її запис про активацію було ліквідовано.

terminology – термінологія # 1. розділ лексики, що охоплює терміни різних галузей знань # 2. сукупність термінів якоїсь галузі науки, техніки, мистецтва або всіх термінів даної мови.

test – тест # стандартне завдання, метод випробування, що застосовується у різних галузях науки для одержання кількісної характеристики певних явищ.

test and maintenance program – програма тестування та технічного обслуговування # програма, призначена для тестування функційного блока в першу чергу для технічного обслуговування чи перевірки роботи.

test check – тестовий контроль # перевірка працездатності комплексу засобів автоматизації за допомогою випробувальних програм. Тестовий контроль не завжди виявляє збої.

testing – тестування # процес виконання тесту за певною методикою.

testing laboratories attestation – атестація випробувальних лабораторій # засвідчення компетентності випробувальної лабораторії і її оснащеності, які забезпечують проведення на належному технічному рівні усіх передбачених нормативно-технічною документацією випробувань заданих видів продукції і (або) видів випробувань.

TETRA – terrestrial trunked radio – наземне транкінгове радіо.

the electric field – екранування електричного поля # локалізація поля електричного шляхом нейтралізації зарядів в металевому заземленому екрані, викликаних джерелами цього поля. Унаслідок екранування напруженість електричного поля за екраном зменшується. Для стікання зарядів з екрана необхідно забезпечити його заземлення з малим (менше 4 Ом) опором.

thematic role – тематична роль # набір функцій, які об'єкт може виконувати під час виконання сценарію # тематичні ролі заповнюються акторами.

theoretical cryptanalysis – теоретичний криптоаналіз # криптоаналіз шляхом аналізу криптосистеми за допомогою наукових методів.

theoretical informatics – теоретична інформатика # див. scientific informatics.

theory – теорія # 1. логічне узагальнення практичного досвіду людей # 2. система вірогідних наукових знань про якусь сукупність об’єктів, яка описує, пояснює і передбачає явища певної частини предметної. Теорія є найдосконалішою формою відображення дійсності.

theory of complexity of calculations – теорія складності обчислень # розділ теорії алгоритмів, що вивчає складність процесу застосування алгоритму до вихідних даних.

theory of destruction information – теорія ураження інформації # складова частина теорії інформаційної боротьби. Охоплює загальні положення і теорію сил і засобів ураження інформації. Загальні положення визначають предмет, завдання і зміст теорії ураження інформації, форми і способи ураження інформації, основні фактори, що впливають на зміст і ефективність ураження інформації.

theory of forces and means information destruction – теорія сил і засобів ураження інформації # складова частина теорії ураження інформації, що визначає та вивчає показники оцінки ефективності ураження інформації, математичну модель ураження інформації, стан підготовки і вирішення завдань ураження інформації.

theory of information – теорія інформації # математична дисципліна, що вивчає властивості інформації та процеси її передавання. Теорія інформації фокусує увагу на таких аспектах зв'язку, як кількість інформації (даних), швидкість та коректність їхнього передавання, пропускна здатність каналу як стосовно інформації в каналі зв'язку, так і стосовно інформації в суспільстві. Теорія інформації, сформульована математиком К. Шеноном у 1948 р., спочатку призначалася для інженерного зв'язку, але нині має відношення до різних сфер діяльності, включаючи комп'ютерну галузь.

theory of systems – теорія систем # галузь науки, пов'язана з вивченням систем з метою виявлення їхніх загальних характеристик і класифікації.

thermal imager – тепловізор # див. infrared imager.

thermal imaging – теплобачення # див. infrared imaging.

thesaurus – тезаурус # 1. сукупність понять із певної галузі науки, накопичених людиною чи колективом. У вузькому розумінні – словник, який відображає смислові зв'язки між словами або іншими смисловими елементами даної мови, і призначений для пошуку слів за їхнім смислом # 2. в системах інформаційних автоматизованих – автоматичний словник, що відображає семантичні відношення між лексичними одиницями інформаційно-пошукової мови і призначений для пошуку слів за їхнім смислом, запитів.

third party – третя сторона /третья сторона/ [] – особа або орган, які визнаються незалежними від сторін учасників у питанні, що розглядається.

threat – загроза # 1. потенційне порушення комп'ютерної безпеки # 2. будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі.

threat analysis – аналізування загроз # дослідження дій та подій, які можуть негативно вплинути на систему опрацювання даних.

threat category – категорія загрози # категорія, що пов'язана з загрозою безпеці інформації (даних). Так в мережах обчислювальних виділяють п'ять категорій загроз: розкриття змісту повідомлень, що передаються; аналіз трафіка, що дозволяє визначити належність відправника і одержувача даних до однієї з груп користувачів мережі; зміна потоку повідомлень, що може привести до порушення режиму роботи будь-якого об'єкта, що керується з віддаленої ЕОМ; неправомірна відмова в наданні послуг; несанкціоноване встановлення з'єднання. Згідно до визначення терміну «безпека інформації» першу і другу загрозу можна віднести до витоку інформації, третю і п'яту – до її модифікації, а четверту загрозу до порушення процесу обміну інформацією, тобто до її втрати.

threat for information – загроза для інформації # витік, порушення цілісності інформації або відмова в авторизованому доступі до неї.

threat of integrity violation – загроза порушення цілісності # загрози безпеці обчислювальної системи, що полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів із сторони середовища експлуатації системи. Найбільш актуальна ця загроза для систем передавання інформації – комп'ютерних мереж і систем телекомунікації.

threat of malfunction – загроза порушення працездатності # загрози безпеці обчислювальної системи, спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність обчислювальної системи, або її ресурси стають недоступними # див. availability.

threat of privacy violation – загроза порушення конфіденційності # загрози безпеці обчислювальної системи, спрямовані на розголошення інформації з обмеженим доступом.

threat to information – загроза для інформації # витік, можливість блокування або порушення цілісності інформації. Загроза для інформації може здійснюватися під час застосовування технічних засобів чи технологій, недосконалих щодо захисту інформації.

threat to information security – загроза безпеці інформації # загрози викрадення, зміни або знищення інформації. Бувають випадковими або навмисними. В найбільш загальному випадку загрози проявляються наступними шляхами: унаслідок дій зловмисників; спостереження за джерелами інформації; підслухування конфіденційних розмов людей і

сигналів акустичних працюючих механізмів; перехоплення електричних, магнітних і електромагнітних полів, сигналів електричних і радіоактивного випромінювання; несанкціонованого розповсюдження матеріально-речовинних носіїв за межі контрольованої зони; розголошення інформації людьми, що володіють інформацією секретною або конфіденційною; утрати носіїв з інформацією (документів, носіїв машинних, зразків матеріалів і т. ін.); несанкціонованого розповсюдження інформації через поля і електричні сигнали, що випадково виникають в електричних і радіоелектронних приладах в результаті їхнього старіння, неякісного конструювання (виготовлення) та порушень правил експлуатації; впливу стихійних сил, насамперед, вогню під час пожежі і води в ході гасіння пожежі та витоку води в аварійних трубах водопостачання; збоїв в роботі апаратури збирання, оброблення, зберігання і передавання інформації, викликаних її несправністю, а також ненавмисних помилок користувачів або обслуговуючого персоналу; впливу потужних електромагнітних і електричних промислових і природних завад.

threat to security of computing system – загроза безпеці обчислювальної системи # впливи на систему обчислювальну, які прямо або побічно можуть нанести шкоду її безпеці. Розробники вимог безпеки і засобів захисту виділяють три види загроз: загрози порушення конфіденційності інформації, що обробляється; загрози порушення цілісності інформації, що обробляється; загрози порушення працездатності системи (відмови в обслуговуванні).

threat to security of information exchange network – загроза безпеці мережі обміну інформацією # потенційно можлива подія, яка може вчинити небажаний вплив на мережу обміну інформацією (MOI), а також на інформацію, що зберігається, обробляється й передається в ній. Виділяють три основних види загроз безпеці MOI: загрози розкриття конфіденційної інформації; загрози цілісності інформації, що полягають у зловмисному змінюванні даних; загрози відмови в обслуговуванні, що полягають в блокуванні доступу до деякого ресурсу системи обчислювальної або MOI.

threshold function – порогова функція # двозначна функція перемикання одного чи кількох необов'язково булевих аргументів, яка приймає значення одиниці, якщо задана математична функція аргументів перевищує задане порогове значення, а в іншому приймає значення нуля # наприклад порогова функція f(a[нижній індекс 1], ..., a[нижній індекс n]) = 0, якщо g [менший або рівний] T; F(a[нижній індекс 1], ..., a[нижній індекс n]) = 1, якщо g > T з g = W[нижній індекс 1]a[нижній індекс 1] + ... + W[нижній індекс

n]a[нижній індекс n], де W[нижній індекс 1], ..., W[нижній індекс n] є позитивними вагами для реальних аргументів a[нижній індекс 1], …, a[нижній індекс n] і T є порогом.

threshold operation – порогова операція # операція, для оцінювання порогової функції її операндів.

ticket – мандат на право доступу # представлення одного чи кількох прав доступу до об'єкта, що має власник. Мандат на право доступу являє собою дозвіл на доступ.

time – час # 1. одна з основних форм існування матерії, яка виявляється в тривалості буття # 2. тривалість існування явищ і предметів.

time bomb – часова бомба # різновид логічної бомби, яка спрацьовує у певний (визначений) момент часу.

time condition of reconnaissance contact – часова умова розвідувального контакту # умова, що передбачає необхідність функціонування органу добування інформації синхронно з роботою джерела інфор-

time network transparency – часова прозорість мережі # здатність мережі забезпечувати тривалість затримки інформації і коливань затримки, відповідних нормативній якості обслуговування.

time slot – часовий квант # будь-який цикловий часовий інтервал, який можна однозначно призначити та визначити.

time stamp – мітка часу # надійний параметр, що змінюється в часі, який позначає момент часу відносно загальної точки відліку.

time stamp – штамп часу # час створення або модифікації даних.

time-division switching – комутування з часовим поділом # метод комутації каналів з часовим мультиплексуванням, що ґрунтується на розподілі комутованих даних різноманітних каналів по часових інтервалах усередині кадру.

timeliness – своєчасність # термін, що означає здійснення в необхідний момент, у свій час.

timeliness of acquired information – своєчасність добутої інформації # забезпечення подання добутої інформації керівництву у встановлені строки, протягом яких вона повністю відповідає реальній обстановці. Своєчасність є важливим показником її якості, так як вона впливає на ціну інформації. Своєчасність добутої інформації слід оцінювати відносно тривалості її життєвого циклу. Якщо час старіння інформації значно більший за час її використання після добування, то вона своєчасна, у протилежному випадку – вона застаріла.

time-out – блокування за перевищенням ліміту часу # подія, призначена для виникнення після закінчення заздалегідь визначеного минулого часу. Блокаванню за перевищенням ліміту часу можна запобігти, надіславши відповідний сигнал; умова блокування за перевищенням ліміту часу може бути скасована через отримання відповідного

сигналу скасування блокування за перевищенням ліміту часу.

timing recovery – відновлювання синхронізації # виведення циклічного сигналу синхронізації з прийнятого цифрового сигналу на основі періодичності часових інтервалів.

TKIP – temporal key integrity protocol – протокол цілісності тимчасового ключа.

TLS – transport layer security – безпека транспортного рівня.

top management – вище керівництво # особа чи група людей, хто управляє та контролює організацію на вищому рівні. Вище керівництво має право делегувати повноваження й забезпечувати ресурсами всередині організації. Якщо сфера застосування системи керування охоплює лише частину організації. тоді вище керівництво відносять до тих. хто управляє та контролює цю частину організації.

top secret information – цілком таємні відомості # відомості у галузі воєнної, зовнішньополітичної, економічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, розповсюдження яких може нанести шкоду інтересам міністерства (відомства) або галузей економіки держави в одній або декількох із перелічених галузей.

top-level domain name – ім'я домену верхнього рівня # атрибут адреси O/R, що визначає найвищий єрархічний рівень у географічній або організаційній структурі системи опрацювання повідомлень. В Інтернеті ім'я домену верхнього рівня – це назва країни чи англійська абревіатура типу "com", "edu", "gov", "mil", "net" або "org.".

touch screen – сенсорний екран # дисплей, який дає змогу користувачеві взаємодіяти з системою опрацювання даних, торкнувшись області на своєму екрані.

touch sensitive screen – сенсорний екран # дисплей, який дає змогу користувачеві взаємодіяти з системою опрацювання даних, торкнувшись області на своєму екрані.

TPM – trusted platform module – модуль заслуговуючих довіри платформ.

trace – слід # *1.* запис про виконання всієї чи частини програми, що показує послідовність виконуваних вказівок чи операторів, операндів та їх імен, а також результати # *2.* виробляти сліду.

trace program – програма відстежування # програма, яка виробляє слід.

tracing – **1.** відстеження # односпрямований зв'язок між двома сукупностями сутностей, який показує, які сутності першої сукупності яким сутностям з другої відповідають # **2.** трасування # проведенні лінії, що вказує напрямок проходження, пролягання чогось.

tracing routing – трасування маршрутизації # процедура одержання інформації про

маршрутизатори (вузли), через які проходять пакети до комп'ютера (здійснюються командою tracert). Дозволяє виявити помилки маршрутизації, наприклад, "зациклення" – передавання пакетів від хоста до хоста по колу.

track – доріжка # на носії даних – шлях, пов'язаний з єдиною головкою зчитування/запису, коли носій даних проходити повз неї.

track density – щільність розташування доріжок # кількість доріжок на одиницю довжини, виміряна в напрямку, перпендикулярному до доріжки. Щільність розташування доріжок зворотно пов'язана з висотою доріжок.

track pitch – висота доріжок # відстань між сусідніми доріжками, виміряна в напрямку, перпендикулярному до доріжки # висота доріжки зворотна відносно щільність розташування доріжок.

traffic – трафік # потік повідомлень в мережі передавання даних; робоче навантаження лінії зв'язку.

traffic analysis – **1.** аналіз трафіка # висновок про стан інформації на основі спостереження за потоками трафіка: наявність, відсутність, обсяг, напрямок і частота # **2.** аналізування трафіку # виведення інформації про спостереження за потоком трафіку # наприклад аналізування наявності, відсутності, кількості, напрямку та частоти переміщення.

traffic analysis – аналіз трафіка # прослуховування трафіка з метою збирання паролів, ключів, іншої ідентифікаційної або автентифікаційної інформації.

traffic contract – угода з навантаження # сукупність параметрів навантаження і якості обслуговування користувача, значення яких визнає або встановлює функція керування визнанням з'єднання при кожному запиті з'єднання віртуального тракту чи віртуального каналу.

traffic flow – інформаційний потік # information flow.

traffic flow confidentiality – конфіденційність потоку трафіка # послуга конфіденційності, призначена для захисту від аналізу трафіка.

traffic padding – заповнення трафіку [незначущою інформацією] # *1.* генерація фіктивних сеансів обміну даними, фіктивних блоків даних і/або фіктивних даних у складі блоків даних # *2.* контрзаходи, які генерують неправдиві дані в середовищі пересилання даних, щоб зробити аналіз або дешифрування трафіку складнішим.

traffit flow confidentiality – конфіденційність потоку трафікую.

transaction – транзакція # *1.* дискретна подія між об'єктом і постачальником послуг, яка підтримує ділові або програмні цілі # *2.* набір пов'язаних між собою операцій, які характеризуються чотирма властивостями: атомарність, несуперечність, локалізація та тривалість. транзакція унікально

ідентифікується ідентифікатором транзакції.

transfer – пересилання # відправлення даних з одного місця зберігання до іншого.

transfer check – контроль передавання # контроль правильності виконання процедури передавання даних і вірогідності інформації, що передається. Одним з методів к. п. є контроль на парність.

transfer rate – [фактична] швидкість пересилання даних # середня кількість бітів, символів або блоків, що передають за одиницю часу між двома точками.

transfer time – час пересилання # часовий інтервал між часом, коли починається пересилання даних, і момент, коли він закінчується.

transform – перетворити # змінити форму даних у відповідності до вказаних правил, без принципових змін значень даних.

transformation – трансформація # зміна, перетворення виду, форми, істотних властивостей чого-небудь.

transient data – тимчасові дані # дані, які переміщаються до інформаційної системи і виходять з неї, або, у випадку розподіленої системи, між двома компонентами системи.

transient error – помилка через випадкові обставини # нерегулярна помилка #

transition – перехід # тимчасовий феномен, що розділяє два послідовні сигнальні елементи, що мають різні значущі умови в дискретному сигналі.

translator – транслятор # 1. проміжний пристрій для підсилення, перетворення і передавання сигналів електричних зв'язку, радіосигналів, телевізійних тощо # 2. програма або технічний засіб ЕОМ, призначені для перекладу описів алгоритмів з однієї формальної мови на іншу.

translucent cryptography – напівпрозора криптографія # принцип побудови криптосистем з відновленням ключів, запропонований M. Bellare та R. Rivest'oM.

transmission channel – канал пересилання # засіб пересилання сигналів одному напрямку між двома точками.

transmission code – код передавання # код, що використовується для кодування інформації, що передається лініями зв'язку.

transmission control protocol – протокол керування передаванням # протокол транспортного рівня, орієнтований на з'єднання, який забезпечує гарантовану доставку даних між взаємодіючими процесами однієї або різних пакетних мереж.

transmission medium – середовище пересилання # природне чи штучне середовище, яку передає сигнали.

transmission path delay – затримка під час пересилання # деякий час, потрібний для переміщення між двома найбільш віддаленими станціями даних в мережі з загальною шиною.

transmit – передавати # відправляти з одного місця для прийому в іншому місці.

transmitter – передавач # технічний пристрій, призначений для перетворення сигналу джерела інформації, в форму, яка забезпечує його запис на носій інформації, що відповідає середовищу розповсюдження. В найбільш загальному випадку п. виконує наступні функції: створює (генерує) поля (акустичне, електромагнітне) або електричний струм, які переносять інформацію; здійснює запис інформації на носій (модуляцію інформаційних параметрів носія), підсилює потужність сигналу (носія з інформацією); забезпечує передавання (випромінювання) сигналу в середовище розповсюдження в заданому секторі простору.

transparent code – прозорий код # код, який допускає інверсію символів, що надходять на вхід декодера.

transport – транспортування # перевезення кого-, що-небудь з одного місця в інше.

transport network – мереда транспортного рівня # частина обчислювальної мережі, яка виконує функції транспортного, мережного, канального і фізичного рівнів і має фізичні засоби з'єднання та пов'язані з ними станції.

transposition – перестановка # шифрування, яке переставляє біти чи символи відповідно до певної схеми # результуючий зашифрований текст, що називається шифром перенесення.

transputer – трансп'ютер # схема інтегральна надвелика, яка має процесор, засоби міжпроцесорного зв'язку, власну пам'ять оперативну і засоби доступу до пам'яті зовнішньої.

trap – пастка # хитрий маневр, прийом для заманювання противника в невигідне, небезпечне становище.

trap door – «лазівка» # залишена розробником недокументована функція, використання якої дозволяє оминути механізми захисту.

trapdoor – шлях обходу системи захисту # прихований програмний або апаратний механізм, зазвичай створений для тестування та усунення несправностей, який може бути використаний для обходу комп'ютерної безпеки.

tree – дерево # структура даних, що містить вузли, які єрархічно пов'язані між собою з не більше ніж одним батьківським вузлом для кожного вузла та лише з одним кореневим вузлом.

tree structure – деревоподібна структура # структура даних, яка організовує об'єкти чи атрибути як вузли, з не більше ніж одним батьківським вузлом для кожного вузла та лише з одним кореневим вузлом.

Trojan horse – троянський кінь # можливо, нешкідлива програма, що містить зловмисну логіку, яка дає

змогу несанкціоноване збирання, фальсифікацію чи знищення даних.

trojan horse – троянський кінь # програма, яка в доповнення до основних (проектних і документованих) надає додаткові, але не описані в документації функціональні можливості, спрямовані на те, щоб обійти контроль доступу і привести до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхні мережі. Ці можливості можуть само ліквідуватись, що робить неможливим їхнє виявлення, або ж можуть реалізуватися постійно, але існувати потай. За характером загрози троянський кінь належить до загроз активних, що реалізуються програмними засобами, які працюють у пакетному режимі. Найбільш небезпечним є опосередкований вплив, при якому троянський кінь діє в межах повноважень одного користувача, але в інтересах іншого користувача, встановити особу якого інколи неможливо.

trojan horse in electronic circles – троянський кінь в електронних колах # створення певних логічних зв'язків в електронних колах апаратних засобів комп'ютерної техніки для автоматичного виконання несанкціонованих маніпуляцій за аналогією з програмною реалізацією троянського коня.

trojan worm – троянський черв'як # різновид троянського коня, особливістю якого є те, що в нього закладений алгоритм саморозмноження, програмне автоматичне відтворення троянського коня. Програми-черв'яки автоматично копіюють себе в пам'яті одного або декількох комп'ютерів (при наявності комп'ютерної мережі) незалежно від інших програм. При цьому використовується тактика вірусів комп'ютерних.

troposcatter link – тропосферна лінія зв'язку # різновид лінії зв'язку радіорелейної, що використовує явище розсіювання ультракоротких радіохвиль у неоднорідностях тропосфери, що викликаються нерівномірністю станів різних точок тропосфери, безперервним перемішуванням і зміщенням повітряних мас в результаті нерівномірного розігрівання Сонцем різноманітних ділянок поверхні Землі і шарів тропосфери. Для забезпечення стійкого тропосферного радіозв'язку застосовуються антени з високим коефіцієнтом підсилення (40-50 дБ), потужні передавачі (1-10 кВт) і високочутливі приймачі. Тропосферні лінії зв'язку найчастіше мають протяжність 140-150 км.

trunk cable – магістральний кабель # кабель, що з'єднує модуль з'єднання з магістраллю для забезпечення обмінювання даними між станціями пересилання даних.

trunk connecting unit – модуль з'єднання з магістраллю # магістральне під'єднання # фізичний пристрій, який з'єднує станцію даних з магістральним кабелем за допомогою відгалуженого кабелю # в модулі з'єднання з магістраллю є засоби для додавання терміналів мережу чи в обхід неї.

trunking gateway – **1.** канальний шлюз # **2.** канальний медіа шлюз # шлюз між мережею з комутацією каналів і мережею з комутацією пакетів, який об'єднує функції медіашлюзу і шлюзу сигналізації.

trunking media gateway – **1.** канальний шлюз # **2.** канальний медіа шлюз # шлюз між мережею з комутацією каналів і мережею з комутацією пакетів, який об'єднує функції медіашлюзу і шлюзу сигналізації.

trust framework – довірча структура # система вимог і механізмів примусу для сторін, що обмінюються інформацією, яка засвідчує особу.

trusted computer system – надійна комп'ютерна система # система опрацювання даних, яка забезпечує достатню безпеку комп'ютера для одночасного доступу до даних користувачами з різними правами доступу та до даних з різною класифікацією безпеки та категоріями безпеки.

trusted computer system criteria – китерій безпеки комп'ютерних систем # стандарт інформаційної безпеки, розроблений міністерством оборони США у 1983 році з метою визначення вимог безпеки, що пред'являються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і вироблення відповідної методології аналізу політики безпеки, що реалізується в комп'ютерних системах воєнного призначення. У критеріях пропонуються три категорії вимог безпеки — політика безпеки, аудит і коректність, в рамках яких сформульовані шість базових вимог безпеки: політика безпеки, мітки — в рамках політики безпеки; ідентифікація і автентифікація, реєстрація і облік — в рамках аудита; контроль коректності функціонування засобів захисту, безперервність захисту – в рамках коректності. Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, а дві останні – на якість самих засобів захисту.

trusted computing base – комплекс засобів захисту # 1. сукупність програмних і технічних засобів, що створені і підтримуються для забезпечення захисту засобів обчислювальної техніки або автоматизованих систем від доступу несанкціонованого до інформації # 2. сукупність програмно-апаратних засобів, в тому числі програм пристроїв запам'ятовуючих постійних, які забезпечують реалізацію політики безпеки інформації. У системі комп'ютерній будь-який її компонент, який внаслідок якого-небудь впливу здатний спричинити порушення

політики безпеки, повинен розглядатися як частина комплекса засобів захисту.

trusted functionality – довірча функційність # функціювання, що сприймається правильним, відповідно вимогам певного критерію, наприклад, критерію, запропонованого за допомогою стратегії захисту.

trusted information communication entity – довірча організація інформаційного обміну # незалежна організація, яка підтримує обмін інформацією всередині об'єднання спільного користування інформацією

trusted third party – довірена третя сторона # орган або його агент, якому інші учасники довіряють займатись спеціалізованою діяльністю (наприклад, діяльністю, пов'язаною з безпекою) # довірена третя сторона є довіреною для об'єкта та/або верифікатора для цілей автентифікації.

trusted third party – надійна третя сторона # третя сторона, яка використовується іншими сторонами для служб верифікації.

TS – time slot – часовий квант.

TTP – trusted third party – надійна третя сторона.

tunnel – тунель # канал передавання даних між мережними пристроями, що встановлюється через наявну мережну інфраструктуру # тунелі можуть встановлюватися шляхом використання таких технічних прийомів, як протокольна інкапсуляція, комутація на основі міток або віртуальних каналів.

tunneling – тунелювання # процес, в ході якого створюється логічне з'єднання між двома кінцевими точками. Тунелі, звичайно, описуються у віртуальних приватних мережах, де дві кінцеві точки здійснюють комунікацію за допомогою інкапсуляції різних протоколів.

tunnelling – тунелювання # інкапсуляція протоколу А у протокол В, за якої протокол А взаємодіє з В, як з канальним рівнем. Застосовується для обміну даними між адміністративними доменами, які використовують протокол, не підтримуваний мережею, що їх з'єднує.

tuple – кортеж # у реляційній базі даних, частина відношень, яка однозначно описує виникнення об'єкта та його атрибути # кортеж може бути представлений одним рядком таблиці відношень.

twisted pair – звита пара # передавальне середовище, яке складено з двох ізольованих електричних провідників, скручених разом.

two-way message – двостороннє повідомлення # спосіб подання аргументів у вигляді повідомлення, що містить як аргументи джерела інформації, так і контраргументи противника, які доведеться викривати. Така побудова повідомлення служить спонукальним мотивом до активної розумової

діяльності об’єкта, в результаті того здійснюється перегляд суджень, що складалися у нього раніше. Двостороннє повідомлення спрямовують переважно на людей з високим рівнем освіти, що відчувають потребу в зіставленні різних поглядів, точок зору, думок, оцінок. В цей же час двостороннє повідомлення як би випереджає аргументацію противника і створює передумови для утворення певного імунітету проти його офіційної пропаганди.

type – тип # 1. зразок, для групи предметів; вид, рід, різно видність чого-небудь # 2. форма чого-небудь, що має певні ознаки.

type conversion – перетворення типів даних # перетворення подання значень даних одного типу даних у відповідності з іншим типом даних, який зазвичай виконується, щоб уникнути неприпустимої невідповідності типу даних. Перетворення типів даних серед числових типів часто допускається, але може спричинити втрату чіткості, точності чи обох.

U

UDP – user datagram protocol – **1.** протокол передавання дейтаграм користувача # **2.** дейтаграмний протокол користувача.

ultimate – кінцевий користувач # див. end user.

UMTS – universal mobile telecommunications system – універсальна система мобільного обміну даними.

unauthorized access – неавторизований доступ # несанкціонований доступ # див. illegal access.

unauthorized access [to information] – несанкціонований доступ [до інформації] # доступ до інформації, за якого порушуються порядок його здійснення і встановлені правові норми.

unauthorized access to hardware – несанкціонований доступ до апаратури # див. illegal access to hardware.

unauthorized access to information – несанкціонований доступ до інформації # доступ до інформації під час якого порушуються встановлені правові норми і порядок його здійснення (правила розмежування доступу). У системі комп’ютерній доступ несанкціонований (НСД) може здійснюватися як з використанням штатних засобів (сукупністю програмно-апаратного забезпечення, включеного до складу системи розробником під час розроблення або адміністратором системи в процесі експлуатації), що входять в затверджену конфігурацію комп’ютерної системи, так і з використанням програмно-апаратних засобів, включених до її складу зловмисником. До основних способів НСД відносяться: безпосереднє звертання до об’єктів комп’ютерної системи з метою одержання певного виду доступу; створення програмно-

апаратних засобів, що виконують звернення до об'єктів в обхід засобів захисту; модифікація засобів захисту, що дозволяє здійснити НСД; впровадження в комп'ютерну систему програмних або апаратних механізмів, що порушують структуру й функції системи і дозволяють здійснити НСД.

unauthorized operation – несанкціонована операція # будь-яка недозволена дія, яка виконується користувачем.

unauthorized operation in the information-computer network – несанкціонована операція в інформаційно-обчислювальній мережі # вплив інформаційний на ресурси інформаційні, персонал, інформаційні системи мережі інформаційно-обчислювальної (ІОМ), елементи ІОМ і ІОМ у цілому, а також підготовка цього впливу.

unauthorized user – незареєстрований користувач # 1. користувач обчислювальної системи, який не стоїть на обліку в даній системі колективного користування # 2. користувач, який працює на ЕОМ не по графіку.

uncertainty – невизначеність # умова, яка виникла, коли значення неможливо визначити в процесі аналізу, або факт чи правило в базі знань залишається під сумнівом.

unconditional attack – безумовна атака # атака на віддалену мережу обміну інформацією , початок здійснення якої є безумовним по відношенню до об'єкта атаки, тобто атаку здійснюють негайно й безвідносно до стану мережі і об'єкта атаки.

unconditionally secure – абсолютна криптостійкість # див. perfect secrecy.

undelete – відновлювання # відновлювання тексту чи графіки, які раніше були видалені, але зміни яких не були остаточними, як наприклад, за допомогою команди збереження.

undoubted signature – безперечний підпис # схема цифрового підпису, що використовує протокол заперечення.

uneven code – нерівномірний код # код, комбінації кодові якого мають неоднакову довжину.

unicity distance – однозначно визначена відстань # щонайменша кількість символів вхідного тексту, за якими теоретично стає можливою атака криптоаналітична лише з відомим шифртекстом.

unified messaging – уніфікований обмін повідомленнями # об'єднання обміну різними типами повідомлень (електронної пошти, факсимільними, голосовими, короткими та іншими повідомленнями мобільного зв'язку) у єдиний сервіс, що дозволяє користувачу мати єдину поштову скриньку для доставки і зберігання всіх повідомлень, доступу до них та сповіщень.

unilateral notification – одностороннє повідомлення # спосіб подання аргументів у вигляді повідомлення, що містить аргументи тільки джерела інформації. Такі повідомлення більш ефективні тоді, коли об'єкт психологічного впливу не відчуває

ворожих почуттів по відношенню до джерела інформації і, до того ж, має низький рівень освіти. Об'єкт у цьому випадку здатний відносно легко прийняти точку зору джерела інформації. Одностороннє повідомлення можна також використовувати для впливу переконуючого на людей, що мають різний освітній рівень.

unintended resistance – ненавмисна опірність # властива багатьом людям схильність в усьому сумніватися, недовірливість та інші прояви загальної критичності.

unintentional threat– випадкова загроза # див. accidental threat.

unit – функційний блок # пристрій # див. device.

unit of measurement – одиниця вимірювань # конкретна кількісна величина, визначена та прийнята в рамках конвенції, з якої складаються інші кількісні величини такого типу для визначення їх величини відносно цієї кількісної величини.

unit string – одиничний рядок # рядок, що містить один елемент.

unit test – одиничний тест # тестування окремих програм або модулів на предмет відсутності помилок аналізу чи програмування.

unitary code – унітарний код # код, що складається з однієї цифри, що повторюється необхідне число разів.

universal address administration – універсальне адміністрування адрес # адміністрування адрес, під час якому всі індивідуальні адреси локальної мережі унікальні в одній або іншій локальній мережі.

universal personal telecommunication service – сервіс універсального персонального зв'язку # сервіс, що надає можливість персональної мобільності.

unmasking object – демаскуючий об'єкт # об'єкт, на основі ознак якого можна не тільки виявити об'єкт, що належить захисту, але і визначити його характеристики. Окреслення в об'єкті захисту о. д. дозволяє вирішувати питання захисту про нього шляхом захисту інформації про о. д. Як і демаскуючі ознаки о. д. поділяються за інформативністю на іменні, прямі і непрямі, за часом прояву – постійні, періодичні і епізодичні.

unpack – розпакування # відновлювання вихідної форми даних із упакованих даних.

unpacked decimal notation – розпакований десятковий запис # двійковий десятковий запис, в якому кожна десяткова цифра представлена одним байтом.

unpredictable ensembles – непередбачуваний ансамбль # ансамбль, для якого для префіксу довільної довжини s_a випадкового слова $Z_n \in /Z_n/_{n \in N}$, $\sigma \in /0,1/$, $s \in /0,1/^{k-1}$ та довільного алгоритму поліноміального ймовірнісного A з входом s виконує нерівність $|P[A(s) = \sigma] - 1/2 | < 1/n^c$ для довільної константи c при досить великих n, де $P[X]$ – ймовірність випадкової події X.

unrecoverable error – невиправна помилка # помилка, виправлення якої неможливе без застосування методів відновлювання поза межами програми.

unrecoverable error – фатальна помилка # помилка, для якої неможливе усунення помилки без використання методів або ресурсів, зовнішніх щодо порушеного функційного модуля.

unrestricted recognition system – необмежена система розпізнавання # розпізнавач мови відкритий для незареєстрованих користувачів, який може надійно працювати з користувачами, які рідко чи ніколи його не застосовували.

unsatisfactory quality of service – низька якість обслуговування # якість обслуговування, нижча за пороговий рівень, який відповідає бальній оцінці «задовільно», встановленій чинною системою показників якості обслуговування.

untraceability – невідслідкованість # властивість транзакції, коли абонент є не тільки анонімним, але і дві транзакції, які створені одним і тим абонентом, не можуть бути ув’язані між собою при будь-яких обставинах. Така властивість досить часто застосовується в системах електронних

upload – завантаження # пересилання програм чи даних із під’єднаного комп'ютера на комп'ютер із більшими ресурсами, зазвичай, від персонального комп'ютера до мейнфрейму.

UPS – uninterruptible power supply – джерело безперебійного живлення.

usability test – тест на використання # перевірка, яка здійснюється для визначення того, чи виконує реалізована система функційні цілі, встановлені її користувачами.

USB – universal serial bus – універсальна послідовна шина.

user – користувач # 1. той, хто користується будь-чим # 2. фізична особа, яка може взаємодіяти з комп’ютерною системою через наданий їй інтерфейс.

user authentication – автентифікація користувача # перевірка відповідності користувача ідентифікаторові, що пред’являють його.

user category – категорія користувача # класифікаційна група, до якої віднесений даний користувач або група користувачів. За обсягом знань у галузі програмного забезпечення та ступенем їхнього використання в виробничій діяльності користувачі поділяються на системних програмістів (найвища категорія), прикладних програмістів та кінцевих користувачів.

user certificate –користувача # див. certificate.

user communication – користувач зв’язку # фізичні і юридичні особи, які є споживачами послуг зв’язку.

user datagram protocol – **1.** данограмний протокол користувача # **2.** дейтаграмний протокол користувача # протокол транспортного рівня, призначений

для обміну данограмами через пакетну мережу, який використовує протокол IP для перенесення пакетів та не гарантує доставку повідомлень і не запобігає появі дублюючих пакетів.

user ID – user identification – ідентифікатор користувача.

user identification – ідентифікація користувача # символьний рядок або шаблон, який застосовується системою опрацювання даних для ідентифікації користувача.

user identification and authentication – ідентифікування і встановлення автентичності особистості # процедура допуску (відмови допуску) користувача до інформації обмеженого використання на основі збігу образу (системи ідентифікаторів), який знімається з особистості користувача, з образом, що зберігається (з урахуванням вимог щодо безпеки інформації) у захищеній пам’яті системи обчислювальної.

user logging – реєстрування користувачів # процес входу користувача в інформаційну систему.

user manual – посібник користувача # документ, у якому описані правила використання функційного блока, і у якому може наводитись перелік прав та обов'язків користувача, власника та постачальника підрозділу.

user object –користувач # подання фізичного користувача в системі комп’ютерній, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

user processor – процесор користувача # процесор, який забезпечує послуги для людини-користувача і який є клієнтом (безпосередньо або непрямо) контролера бази даних.

user profile – профіль користувача # *1.* облікові дані користувача, які зазвичай застосовуються для контролю доступу # профіль користувача може містити такі дані, як: ідентифікатор користувача, ім'я користувача, пароль, права доступу та інші атрибути # *2.* шаблон діяльності користувача, який може застосовуватися для виявлення змін у його діяльності.

user terminal – термінал користувача # термінал, призначений для індивідуальної роботи користувача.

user violato – порушник # див. infringer.

userid – ідентифікатор користувача # число або літеро-рядковедане, що ідентифікує користувача в системі обчислювальній.

user's guide – настанова користувача # документ, у якому описані правила використання функційного блока, і у якому може наводитись перелік прав та обов'язків користувача, власника та постачальника підрозділу.

user-tuned system – система, налаштовувана під користувача # незалежна від спікера система, здатна модифікувати та оновлювати свій шаблон мови, для відстеження відмінностей між зразками мови, та підвищення своєї продуктивності #

можливість покращення продуктивності є своєрідним навчанням.

utility program – утиліта # програма, що надає загальні, часто необхідні послуги для користувачів комп'ютера та обслуговуючого персоналу # наприклад діагностична програма, програма трасування, програма сортування.

utility routine – програма утиліта # забезпечує загальні, часто необхідні послуги для користувачів комп'ютера та обслуговуючого персоналу # наприклад процедура введення.

V

vaccine – вакцина # антивірус, заздалегідь введений (імплантований) у програму, яку захищають.

vaccine program – програма вакцинації # програма, призначена для виявлення вірусів і, можливо, запропонування чи вжиття заходів щодо виправлення.

validation – **1.** дієздатність # тест на визначення, чи реалізована система виконує свої попередньо встановлені вимоги # **2.** затвердження # підтвердження наданням об’єктивних доказів, що вимоги для певного визначеного застосування або прикладної системи виконано.

validation test – тест на дієздатність # тест на визначення, чи реалізована система виконує свої попередньо встановлені вимоги.

validity – достовірність, вірогідність # див. adequacy.

validity message estimating by Kant's scheme – оцінювання достовірності повідомлення за схемою Канта # якісно-кількісний спосіб кількісної оцінки достовірності повідомлення. У відповідності з ним діапазон можливих імовірностей розбивається на 7 інтервалів і достовірність конкретної інформації оцінюється в шансах: достовірна інформації (ймовірність відсутності неправдивої інформації є близькою до 1); майже визначено, що інформація достовірна (9 шансів проти одного); є багато шансів, що інформація достовірна (3 шанси проти одного); шанси приблизно однакові (1 за, 1 проти); є багато шансів, що інформація недостовірна (3 шанси проти одного); майже визначено, що інформація недостовірна (за 9 шансів проти одного); недостовірна інформація (ймовірність неправдивої інформації є близькою до 1).

validity of intelligence information – достовірність розвідувальної інформації # ступінь відповідності отриманої інформації розвідувальної дійсній обстановці. Достовірність розвідувальної інформації досягають: позначенням часу здійснення подій, відомості про які отримують; ретельним вивченням та порівнянням даних, отриманих із різних джерел; перевіркою сумнівних відомостей; своєчасним викриванням дезінформаційних та маскувальних заходів противника; виключенням спотворення інформації, що

передається за допомогою технічних засобів зв’язку.

validity of obtained information – достовірність добутої інформації # ступінь відповідності отриманої інформації дійсній обстановці. Достовірність добутої інформації. досягається: позначенням часу здійснення подій, відомості про які отримують; ретельним вивченням та порівнянням даних, отриманих з різних джерел; перевіркою сумнівних відомостей; своєчасним викриванням дезії, формаційних та маскувальних заходів противника; виключенням спотворення інформації, що передається за допомогою технічних засобів зв’язку. Для оцінки достовірністі добутої інформації використовують наступні часткові показники: достовірність повідомлень (відносно відсутності неправдивих повідомлень і даних); розбірливість мови; імовірність помилкового або неспотвореного прийому дискретної одиниці (біта, символу, цифри, букви, слова).

validity period – термін дії # період часу, протягом якого ідентичність чи повноваження можуть бути використані в одній або декількох транзакціях.

value – цінність # сукупність таких властивостей чого-небудь, як важливість, значність, необхідність.

value estimation of information – оцінка вартості інформації # оцінка цінності інформації # дані, що визначають цінність інформації. Для одержання цих даних застосовують різноманітні підходи: квазіекономічний – за основу береться інформація як товар, що має свою ринкову ціну; прагматичний – цінність інформації визначається найвирішальнішою ситуацією; це означає, що інформація тим цінніша, чим швидше вона сприяє вирішенню проблеми; праксеологічний – цінність інформації визначається результативністю дій для досягнення наміченої мети; семантичний – цінність інформації визначається мірою, в якій вона служить для збагачення знань споживача.

variable – змінна # чотиривимірна величина, представлена описом або неявним описом, що охоплює ідентифікатор, набір атрибутів даних, одну чи кілька адрес і значень даних, де зв'язок між адресами та значеннями даних може змінюватися. На деяких мовах програмування адреси можуть відрізнятися, тому і пов'язані значення даних можуть відрізнятися. На інших мовах програмування адреси залишаються фіксованими, але пов'язані дані можуть змінюватися у процесі виконання.

variable function generator – генератор змінних функцій # генератор функцій, в якому генерована ним функція може бути встановлена користувачем до початку чи під час обчислення.

variable trace – трасування змінних # запис імен та значень змінних, доступних або змінюваних під час виконання програми.

variable-length code – код змінної довжини # 1. код, в якому фіксоване число символів вихідного повідомлення кодується в змінне число вихідних символів # 2. код із змінною довжиною комбінації кодової.

variant – варіант # конфігурація всієї інформаційної системи або її частини, яка співіснує з системою, що має іншу конфігурацію, але забезпечує ті самі засоби.

vector – вектор # величина, що зазвичай характеризується упорядкованим набором скалярів.

Venn diagram – діаграма Венна # діаграма, в якій набори представлені областями, зображеними на поверхні.

verbal broadcast – усне мовлення # вплив інформаційно-психологічний, який здійснюється шляхом передавання через звукомовні станції різноманітних повідомлень і програм, які безпосередньо сприймають військовослужбовці противника, його цивільне населення, полонені. Переваги усного мовлення: високий ступінь оперативності; високий ступінь конкретності; сприйняття передач усного мовлення не потребує використання спеціальних технічних засобів; при усному мовленні можливий «зворотній зв'язок» з об'єктом впливу (сприйняття його реакції на передачу); усне мовлення передбачає використання музики, шумів та інших звукових ефектів, що підвищує емоційний вплив на слухачів. Недоліки, що знижують ефективність усного мовлення: вплив бойових і природних шумів, погодних і кліматичних умов, а також завад, які може створювати спеціально противник; радіус дії усного мовлення обмежений відносно невеликим простором; велика можливість виявлення і придушення противником звукомовного засобу.

verbal model – модель вербальна # словесний опис моделі на мові природній або професійно-орієнтованій.

verdict – вердикт # висновок оцінювача (позитивний, негативний або неостаточний) відносно деякого елементу дій оцінювача, компоненту або класу довіри.

verification – **1.** верифікація # підтвердження наданням об'єктивних доказів, що встановлені вимоги виконано # **2.** тестування узгодженості # **3.** перевірка # *1.* порівняння діяльності, процесу чи продукту з відповідними вимогами чи технічними умовами # наприклад порівняння специфікації з моделлю політики безпеки чи порівняння об'єктного коду з вихідним кодом # *2.* тест системи, який підтверджує, що вона відповідає всім визначеним вимогам на певному етапі її розробляння # **4.** контрольна перевірка # процедура оцінювання, яка використовується для підтвердження того, що контроль безпеки операційної системи запроваджений і виконаний

правильно і є ефективним при застосуванні.

verification – верифікація # *1.* процес перевірки достовірності інформації шляхом вивчення її джерел та їхньої надійності # *2.* в програмуванні – доказ правильності програми # *3.* певна сукупність вимог із захисту засобів обчислювальної техніки від доступу несанкціонованого до інформації.

verification authentication information – інформація перевірки повноважень.

verification test – тест на підтвердження # тест системи, який підтверджує, що вона відповідає всім визначеним вимогам на певному етапі її розробляння

verifier – верифікатор # учасник, який підтримує ідентифікаційну інформацію # верифікатор може брати участь у багатьох фазах EAAF та може надавати верифікацію повноважень та/або верифікацію ідентифікаційної інформації.

version – версія # конфігурація всієї інформаційної системи або її частини, яка існує в певний момент часу.

version space – простір версій # набір усіх концептуальних описів, що сумісні з наявними даними, знаннями чи припущеннями.

vertical fragmentation – вертикальне фрагментування # фрагментація, де розподіли формуються для одного типу значень даних для всіх екземплярів.

vertical masks – вертикальні маски # маски оптичні штучні, призначені для захисту об’єктів від спостерігання із землі.

very large-scale integration – надвелика інтегральна схема # мікросхема інтегральна із ступенем інтеграції понад 1000 елементів в кристалі.

VHF – very high frequency – надвисока частота.

viability – живучість # термін, що означає життєздатність, витривалість, стійкість, тривале збереження.

video – відео # в складних словах указує на належність поняття до зображення телевізійних, радіолокаційних та інших складних електричних сигналів на екрані електронно-променевої трубки.

video camera – відеокамера # див. camera-recorder.

video control switch – комутатор системи відеоконтролю # комутатор, призначений для приєднання декількох (4-16) камер телевізійних до одного монітора з послідовним переключенням в ручному або автоматичному режимах.

video image – відеозображення # зображення, представлене сигналом електричним, наприклад, стандартним сигналом телевізійним.

video server – відео-сервер # сервер, який зберігає відеоінформацію для подальшого використання її користувачами.

video-monitoring system motion detector – детектор руху системи відеоконтролю # пристрій, призначений для сповіщення оператора системи відеоконтролю

або вмикання відеомагнітофона при зміні картинки на одній або декількох камерах телевізійних. Детектори руху випускаються у вигляді окремих блоків, що сполучаються з іншими елементами системи відеоконтролю, або ними можуть обладнуватися мультиплексори. Ступінь зміни зображення (швидкість руху зловмисника), що викликає сигнал тривоги, встановлюється оператором за допомогою регулятора порога спрацьовування.

videosignal – відеосигнал # сигнал електричний, призначений для створення зображення.

videotex – відеотекс # система доступу до баз даних через мережі зв'язку, яка забезпечує передавання текстів і зображень. Як приймач даних може використовуватися ПЕОМ або побутовий телевізор із спеціальним пристроєм.

views – переконання # свідомі, стійкі мотиви діяльності людей, що мають за звичай ідеологічну основу, і виявляються в їхніх діях, вчинках і поведінці.

vims protection – захист від вірусів # сукупність програмних засобів та організаційних заходів, спрямованих на виключення зараження файлів вірусом комп'ютерним # див. antivirus.

violation – порушення # 1. дія, спрямована на заважання нормальному стану, розвитку будь-чого, переривання будь-якого процесу # 2. невиконання, недотримування будь-чого.

virgin medium – незаповнений носій # інформаційний носій даних в якому або на якому не було зареєстровано ні знаків посилань, ні даних користувача.

VIRS – voice interactive response system – система голосової інтерактивної відповіді.

virtual – віртуальний # *1.* можливий; той, що може або має проявитися # *2.* характеристика пристрою або об'єкта, що не існує насправді. Способи використання віртуальних пристроїв відрізняються від способів використання звичайних пристроїв чи об'єктів. Наприклад, користувач може працювати з віртуальним диском як з фізичним, але насправді цей диск є частиною комп'ютерної пам'яті.

virtual address – віртуальна адреса # у системі віртуального зберігання, адреса, призначена для місця зберігання в зовнішній пам'яті, для забезпечення доступу до цього місця таким чином, якби воно було частиною основного сховища.

virtual channel switching – комутування віртуальних каналів # в обчислювальних мережах вид комутації, який поєднує переваги комутації пакетів і комутації каналів. З'єднання в основному здійснюються на рівні транспортному, а користувач звільнюється від необхідності контролювати послідовність проходження інформації мережею.

virtual circuit – віртуальний канал # канал передавання даних між вузлами мережі, тимчасово утворений для окремих пакетів в різних, як правило, фізичних каналах, зі збереженням цілісності прийманих даних.

virtual local area network – віртуальна локальна [комп'ютерна] мережа # *1.* група робочих станцій, можливо у різних фізичних сегментах локальних комп'ютерних мереж, яка, незалежно від фізичного місцезнаходження цих станцій, взаємодіє так, ніби вони є однією локальною комп'ютерною мережею # *2.* віртуальна локальна мережа # незалежна мережа, створена з логічної точки зору усередині фізичної мережі.

virtual machine – віртуальна машина # віртуальна система опрацювання даних, яка доступна для особистого користування певного користувача, але функції якої виконують за допомогою обмінюванню ресурсів системи опрацювання реальних даних.

virtual memory – віртуальна пам'ять # місце зберігання, що може розглядатися як основне адресне сховище користувача, який застосовує комп'ютерну систему, де віртуальні адреси відображаються в реальних адресах. Розмір віртуального сховища обмежується схемою адресації комп'ютерної системи та кількістю наявної допоміжної пам'яті, а не фактичною кількістю основних місць зберігання.

virtual object – віртуальний об'єкт # ідеальний об'єкт, описаний у вигляді діючою програмної моделі. У взаємодії з користувачем проявляє себе як реальний об'єкт.

virtual path – віртуальний тракт # сукупність віртуальних каналів, пов'язаних спільним значенням ідентифікатора тракту.

virtual private network – віртуальна приватна мережа # мережа, що складається з фізичних компонентів мережі загального користування і приватної мережі, які сумісно забезпечують функціональність приватної мережі за допомогою віртуальних каналів.

virtual storage – віртуальне сховище # місце зберігання, що може розглядатися як основне адресне сховище користувача, який застосовує комп'ютерну систему, де віртуальні адреси відображаються в реальних адресах.

virtual terminal – віртуальний термінал # узагальнена логікова модель різних терміналів певного класу, яка описує, як будуть працювати термінали цього класу в середовищі OSI.

virtualization – віртуалізація # перехід на більш високий рівень абстракції у керуванні конкретними конфігураціями системи обчислювальної.

virus – вірус # програма, яка поширюється, модифікуючи інші програми таким чином, щоб вони містили, можливо, змінену копію себе, і яка буде виконуватись під час виклику зараженої програми # вірус

часто спричиняє пошкодження чи незручності, і може викликатися певною подією, такою як настання заздалегідь визначеної дати.

virus interaction – взаємодія вірусів # модифікування кодів або блокування одного вірусу комп'ютерного іншим при одночасному знаходженні їх у пам'яті оперативній. В більш широкому розумінні – зміна функціонування одного комп'ютерного вірусу під впливом іншого.

virus signature – сигнатура вірусу # унікальний бітовий рядок, який є загальним для кожної копії певного вірусу і який може застосовуватися програмою сканування для виявлення наявності вірусу.

virus-infected program – вірусоносій # див. contagious program.

VLAN – virtual local area network – віртуальна локальна [комп'ютерна] мережа.

VM – virtual machine – віртуальна машина.

vocoder – вокодер # клас передавальних систем, що базуються на принципі аналізу і синтезу мовного сигналу. У передавальній частині вокодера з мовного сигналу виділяються інформаційні параметра спектра мови, що змінюються повільно, основний тон вокалізованих (дзвінких) звуків і переходи тон-шум глухих звуків. В. розрізняються в залежності від параметрів, що виділяються. Розповсюджені вокодери смугові і вокодери з лінійним передбаченням. В. для телефонного закритого зв'язку із швидкістю передавання 4800 біт/с забезпечують розбірливість складів до 93% (розбірливість слів сягає 99%) при задовільному упізнаванні абонента). В телефонних каналах низької якості швидкість інформаційного потоку на виході в. знижують до 2400 біт/с при збереженні достатньої розбірливості, але низького упізнавання голосу абонента.

voice control system – система голосового керування # система, в якій розпізнавач мови видає команди для комп'ютерного керування обладнанням у відповідь на мовне введення # наприклад робот, який реагує на прості голосові команди для руху.

voice controller – голосове керування # система, в якій розпізнавач мови видає команди для комп'ютерного керування обладнанням у відповідь на мовне введення # наприклад робот, який реагує на прості голосові команди для руху.

voice interactive response system – система голосової інтерактивної відповіді # функційна одиниця для інтерактивної голосової відповіді.

voice mail – голосова пошта # оцифроване голосове повідомлення, яке зберігається та пересилається одному чи кільком отримувачам.

voice prompt – голосова підказка # усне повідомлення, яке застосовується як керівництво користувача через діалогове вікно з системою голосової відповіді.

voice recognition – розпізнавання голосу # перетворення мовного сигналу, реалізоване за допомогою функційного блока, за допомогою подання деяких акустичних характеристик голосу. Розпізнавання голосу застосовується у розпізнаванні акустичних систем.

voice response – голосова відповідь # синтезований мовний сигнал, що надається у відповідь на запит користувача.

voice security – захист мовної інформації # комплекс заходів, спрямованих на протидію зловмисним спробам несанкціонованого доступу до мовної інформації.

voice signature – голосовий підпис # голосовий зразок певного користувача, який застосовується для його ідентифікації.

voiceprint – голосова печатка # голосовий зразок певного користувача, який застосовується для його ідентифікації.

voice-recognition unit – блок розпізнавання голосу # функційний блок, який розпізнає обмежену кількість голосових команд і перетворює їх на еквівалентні цифрові сигнали, які можуть слугувати в якості вхідних даних для комп'ютера чи ініціювати інші бажані дії # таке периферійне обладнання може застосовуватися зі спеціальним пристроєм розпізнавання мови чи без нього.

voice-response prompt – голосова відповідь # усне повідомлення, яке застосовується як керівництво користувача через діалогове вікно з системою голосової відповіді.

VoIP – voice over IP – передавання мовлення через IP.

voluntary certification – добровільна # сертифікація на відповідність вимогам, не віднесеним нормативними документами до обов’язкових, яка проводиться на добровільних засадах за ініціативою виробника, постачальника чи споживача продукції.

VPN – private virtual network – приватні віртуальні мережа

VPN – virtual private network – віртуальна приватна мережа.

VPN – virtual private network – віртуальна приватна мережа.

VR – voice response – голосова відповідь.

vulnerability – вразливість # 1. чутливість до чогось, легке піддавання дії, впливові чого-небудь # 2. властивість будь-чого легко і швидко піддаватися дії зовнішніх впливів.

vulnerability – вразливість # слабкість або недоліки у системі опрацювання даних # якщо вразливість співвідноситься із загрозою, існує ризик.

vulnerability – уразливість # слабкість ресурсу СУІБ або заходів безпеки, якою можуть скористатися одна чи більше загроз.

vulnerability assessment – оцінювання уразливості # дослідження об’єкта оцінювання з метою визначення можливості реалізації загроз.

vulnerability of information exchange network – вразливість мережі обміну інформацією # характеристика мережі обміну інформацією, що обумовлює можливість виникнення загрози її безпеці.

W

WAN – wide area network – глобальна мережа.

WAP – wireless application protocol – протокол застосувань для бездротових мереж.

wave band – діапазон радіохвиль # визначена ділянка довжин радіохвиль, якій присвоєна умовна назва. За довжиною радіохвиль виділяють такі діапазони радіохвиль: декамегаметрових (10-100 Мм), мегаме- трових (1-10 Мм), гектокілометрових (100-1000 км), міріаметрових (10-100 км), кілометрових (1-10 км), гектометрових (100-1000 м), декаметрових (10-100 м), метрових (1-10 м), дециметрових (10-100 см), сантиметрових (1-10 см), міліметрових (1-10 мм) та децимілiметрових (0,1-1 мм) радіохвиль. В залежності від особливостей розповсюдження, а також генерування, випромінювання і приймання радіохвиль виділяють такі діапазони радіохвиль: наддовгих (довжиною понад 10 км), довгих (1-10 км), середніх (100-1000 м), коротких (10-100 м) та ультракоротких (довжиною до 10 см) радіохвиль.

wave range – діапазон радіохвиль # див. wave band.

WDP – wireless datagram protocol – протокол бездротових дейтаграм.

weak bit – слабкий біт # біт навмисно написаний на диску зі слабкою силою магнітного поля, який може інтерпретуватися як нуль або один, і який написаний як частина методу захисту від копіювання.

weak keys – слабкі ключі # специфічні ключі, які зменшують стійкість даного шифру (або складність шифру (cipher complexity)) порівняно з іншими ключами. Для шифру DES існує 4 к. с., які генерують однакові підключі для всіх циклів; 12 так званих напівслабких ключів (semi-weak keys), які генерують тільки два різних підключі та незначну кількість напівслабких ключів (demi-semi-weak keys), які у свою чергу генерують чотири різних підключі. Незважаючи на дуже незначну кількість к. с. серед усіх 256 ключів DES, їх треба відкидати при генеруванні ключів. Якщо для шифру не існує к. с., то говорять про лінійний простір ключовий шифру. Це, наприклад, заявлено для шифру Skipjack та шифру MARS.

weapon – зброя # див. arm.

weighted code – зважений код #позиційний код # код подання чисел, в якому кожній позиції присвоєна певна вага.

WEP – wired equivalent privacy – захист, еквівалентний дротовій мережі.

wide area network – глобальна обчислювальна мережа # мережа, яка надає послуги зв'язку на географічну територію, більшу, ніж та, яку обслуговує локальна мережа чи мережа великих територій.

wide track – широка доріжка # набір з двох або більше сусідніх доріжок на диску, на який написані ті ж дані, як частина методу захисту від копіювання.

wideband – широкосмуговий канал # смуга частот, яку застосовують для застосунку, що вимагає широкого діапазону частот # широкосмуговий канал може бути розділений на кілька більш вузьких смуг, кожна з яких може бути використана для різних цілей, або бути доступною для різних користувачів.

WiFi hot spot – **1.** активна зона доступу WiFi # **2.** хот спот # зона, у якій обладнання користувачів виявляє наявність точки доступу бездротової мережі WiFi.

WiMAX – worldwide interoperability for microwave access – технологія широкосмугового доступу в мікрохвильовому діапазоні.

winchester disk – вінчестер # малогабаритний пакет дисків жорстких магнітних, що загерметизовані разом з головками запису-читання. Використовується як зовнішня незмінна пам’ять ЕОМ.

wired-in check authenticity – апаратний контроль достовірності # див. hardware check authenticity.

wireless datagram protocol – протокол бездротових дейтаграм # один із застосовних протоколів бездротового обміну даними, аналогічний дейтаграмному протоколу користувача UDP.

wireline – проводова лінія зв’язку # лінія зв’язку, призначена для передавання електричних сигналів проводами. Проводову лінію зв’язку поділяють на повітряні і кабельні. Основними параметрами проводової лінії зв’язку є ширина спектра частот, що пропускається ними, і власне загасання.

wiretapping – перехоплення інформації в дротових лініях # прихований доступ до певної частини схем даних для отримання, модифікації чи вставки даних.

WLAN – wireless local area network – бездротова локальна мережа.

work – діяльність # див. activity, activities.

work environment of automated system – робоче середовище автоматизованої системи # приміщення і територія, в яких розташована система автоматизована, технічне обладнання, що не зв’язане з обробленням інформації, і правила функціонування автоматизованої системи. Оцінкою даного середовища є множина $P = \{p_1, p_2, ..p_n\}$, елементами якої є показники, що характеризують окремі параметри робочого середовища.

work unit – крок оцінювання # найменша структурна одиниця роботи оцінювання # кожна дія в методології оцінювання охоплює в

себе один або декілька кроків оцінювання, які згруповані в межах дії методології оцінювання відносно елементів змісту та подання свідчень або елементів дій розробника # наприклад кроки оцінювання ідентифіковані умовним позначенням типу: ALC_TAT.1-2. У цьому позначенні послідовність символів ALC_TAT.1 вказує на підвид діяльності з цього стандарті, а завершальна цифра (2) вказує, що це другий крок оцінювання в підвиді діяльності ALC_TAT.1.

workstation – робоча станція # функційна одиниця, яка зазвичай має спеціальні обчислювальні можливості і охоплює в себе користувацькі вхідні та вихідні одиниці # напаприклад програмний термінал, непрограмний термінал чи автономний мікрокомп'ютер.

world information space – світовий інформаційний простір # основа суспільства інформаційного, в якому діють великі інформаційні конгломерати, що об’єднують системи створення інформації (видавничі будинки, редакції газет і журналів, телемережі, телестудії) і мережі її розповсюдження (кабельні, телефонні, комп’ютерні, супутникові) та функціонують глобальні міжнародні інформаційно-телекомунікаційні мережі, що охоплюють більшість країн світу. Мережі надають споживачеві широкий набір інформаційних продуктів і послуг. Це ділова, освітня, розважальна інформація, електронні газети і журнали, бази даних практично в усіх галузях життєдіяльності суспільства, електронна пошта, доступ до різноманітних інформаційних ресурсів бібліотек, державних і приватних закладів і компаній.

WORM – write once read many – запам’ятовувальний пристрій з одноразовим записом та багаторазовим зчитуванням.

worm – черв’як # самодостатня програма, яка може поширюватися за допомогою систем опрацювання даних або комп'ютерних мереж # хробаки часто розроблені таким чином, щоб застосовувати наявні ресурси, такі як простір зберігання чи час опрацювання.

worm virus – віруси-черв’яки # комп’ютерні віруси , що розповсюджуються в комп’ютерній мережі і так же як і віруси-супутники, не заражають “батьківські” програми, файли або сектори на дисках. Віруси-черв’яки проникають у пам’ять комп’ютера з комп’ютерної мережі і після визначення адрес інших комп’ютерів, розсилають за цими адресами свої копії. Такі віруси іноді створюють робочі файли на дисках операційної системи, проте можуть і взагалі не звертатися до ресурсів обчислювальної системи (за винятком оперативної пам’яті).

WPA – Wi-Fi protected access – захищений доступ у бездротових мережах.

write – писати # робить постійний або тимчасовий запис даних у пристрої зберігання даних або на носій даних # фрази "читати" і "зчитати" часто відрізняються від фраз "написати" і "писати" лише з точки зору опису. Наприклад, Пересилання блока даних з внутрішньої пам'яті на зовнішню пам'ять може бути названа «запис на зовнішню пам'ять» або «читання з внутрішньої пам'яті» або як обидва.

write access – доступ до запису # право доступу, яке дає дозвіл на запис даних # доступ до запису може дати дозвіл на додавання, зміну, видалення чи створення даних.

write cycle time – час циклу записування # мінімальний проміжок часу між початком наступного циклу запису накопичувача, що має окремі цикли читання та запису.

write head – записувальна головка # магнітна головка, що здатна тільки записувати.

write protection – захист від записування # спосіб захисту інформації на диску та (або) в оперативній пам’яті, який полягає в забороні звернення до файла для виконання операції записування даних. Дозволяється тільки читання даних. Це дає змогу запобігти записуванню нових даних і зберегти наявні дані від руйнування. Реалізується шляхом встановлення ключів захисту або за допомогою мітки зчитування на диску.

write protection label – позначка захисту від запису # позначка, наявність чи відсутність якої на дискеті запобігає запису на цій дискеті.

write-enable ring – кільце дозволу на запис # знімне пластикове чи металеве кільце, наявність або відсутність якого на магнітній стрічці котушки заважає писати на магнітній стрічці і тим самим запобігає випадкове стирання файлу.

Z

zero – нуль # номер, який під час додаванні чи вирахуванні з будь-якого іншого номера не змінює значення цього іншого номера # нуль може мати різні подання на комп'ютерах, таких як позитивно чи негативно підписаний нуль (що може бути результатом віднімання від нього самого підписаного номера) та нульової рухомою точками (в якій частина фіксованого крапки дорівнює нулю, тоді як показник у представленні з рухомою комою може змінюватися).

zero knowledge proving – доведення з нульовим знанням # доведення без розголошення # протокол криптографічний для доведення одним з учасників протоколу іншому факту володіння певними секретними даними без розкриття цих даних. При цьому учасник, якому доводиться факт володіння, не отримує жодної інформації про секретні дані, якими володіє інший учасник.

zero suppression – **1.** усунення нулів # усунення незначущих нулів від числа

2. функція усунень нулів # функція, яка забезпечує процес, за допомогою якого небажані нулі пропускаються з друкованого чи відображеного результату розрахунку.

zero-address instruction – інструкція нульової адреси # інструкція, яка не має адресної частини # напаприклад певні інструкції для машинного стека; інструкція HALT.

zerofill – занулення # заповнює невикористані місця зберігання з символьним поданням, позначаючи їх нулями.

zeroization – обнуління # спосіб стирання збережених в електронному вигляді даних, криптографічних ключів та критичних параметрів, шляхом зміни або видалення вмісту сховища даних, щоб запобігти поверненню даних.

zone – зона # певний простір, район, територія, що характеризується спільними ознаками.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII.
2. Бабак В. П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В. П. Бабак, О. Г. Корченко. – К.: НАУ, 2003. – 670 с.
3. Гладун А.Я., Хала К.О. ДСТУ 2382:2018 Інформаційні технології. Словник термінів.- К.: Вид. УкрНДНЦ, 2018.-552с.
4. Словник термінів з кібербезпеки / За заг. ред. Копана О.В., Скулиша Є.Д. – К. : ВБ "Аванпост-Прим", 2012. – 214 с.
5. Тлумачний словник з інформатики / Г.Г. Півняк, Б.С. Бусигін, М.М. Дівізінюк та ін. – Д., Нац. гірнич. ун-т, 2010. – 600 с.
6. Пройдаков Е.М., Теплицький Л.А. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування.- Вид. 1 – К.:Видавничий дім «СофтПрес», 2005.-2005.
7. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний електронний навчальний довідник/ За ред. Кривуци В.Г.- Київ: ООО «Д.В.К.», 2005.-508с.
8. Пройдаков Е.М., Теплицький Л.А. Большой англо-русский толковый словарь по вычислительной технике и информационным технологиям(ВТ/ИТ) – М.: Издательство «РТСофт», 2015.- 1600с.
9. Гладун А. Я., Рогушина Ю. В. “Семантичні технології: принципи та практики (монографія)”. – К. : ТОВ «ВД «АДЕФ- Україна», 2016. – 388 с.
10. Гладун А. Я., Рогушина Ю. В. “Data Mining: пошук знань в даних. Підручник”. – К. : ТОВ «ВД «АДЕФ- Україна», 2015. – 432с.
11. A glossary of computing term. Longman Group Ltd., UK, 1995.-380 pp.
12. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. “Інформаційна безпека особистості, суспільства, держави: Підручник“. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.
13. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник.-К.: Видавництво УкрНДНЦ, 2015.- 112с.
14. Бурячок В.Л. Кібернетична безпека — головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. — 2011. — № 3 (26). — С. 104-114.
15. Бурячок В.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу // Захист інформації. — 2013. — Том 15, № 1. — С. 5-12.
16. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. — К. : ВБ «Аванпост-Прим». — 2012. — С. 31.
17. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки. (монографія)/ В. Л. Бурячок.— К.: НАУ, 2013.— 432 с.
18. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк// Безпека інформації.— 2013.— Т. 19, № 2.— С. 118–129.

19. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010 [Електронний ресурс].— Режим доступу: http://web.ebscohost.com.
20. Encyclopedia Britannica. WEB-сайт (Електрон. ресурс) / Спосіб доступу: URL: http://www.Britannica.com
21. Wikipedia, the Free Encyclopedia. WEB-сайт (Електрон. ресурс) / Спосіб доступу: URL: http://www.wikipedia.org/wiki/Development (http://en.wikipedia.org/wiki/)
22. Англо-російсько-український словник з геоінформатики / Б.С. Бусигін, Г.М. Коротенко, Л.М. Коротенко та ін. – Вид. 1. – К.: Карбон, 2007. – 438 с.
23. Бартків А.Б. та ін. Англо-українсько-російський словник з інформатики. – К.: Вища школа, 1995. – 445 с.
24. Бех П.О. Російсько-англо-український словник з інформатики та обчислювальної техніки: (З покажч. англ. і укр. термінів). – К.: Спалах, 1998. – 504 с. (Программа «Трансформація гуманітарної освіти в Україні»).
25. Григорьев В.Л. Англо-русский толковый словарь РС. – М.: Компьютер, ЮНИТИ, 1997. – 471с.
26. Інформатика та обчислювальна техніка: Короткий тлумачний словник. – К.: Либідь, 2000. – 320 с.
27. Карачун В.Я. Англо-український словник-довідник скорочень у галузі комп'ютерної техніки. – К.: Т-во "Знання", 2000. – 158 с.
28. Колисниченко Д.Н. Англо-русский толковый словарь компьютерных терминов / Под ред. М.В. Финкова. – СПб.: Наука и техника, 2006. – 288 с.
29. Коссак О.М. Англо-український словник з інформатики та обчислювальної техніки / Лінгв. ред. О.Р. Микитюк. – Львів: СП «БАК», 1995. – 304 с.
30. Мирончиков И.К., Павловцев В.А. Англо-русский толковый словарь по Интернет. – Минск, М.: ИСК, 2000. – 134 с.
31. Митчелл Ш. Толковый словарь компьютерных технологий. – СПб.: ООО «ДиаСофтЮП», 2002. – 720 с.
32. Першиков В.И., Марков А.С., Савинков В.М. Русско-английский толковый словарь по информатике. – 3-е изд., перераб. – М.: Финансы и статистика 1999. – 363 с.
33. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed United States Government Accountability Office, Washington, July 2010 [Електронний ресурс].— Режим доступу: https://www.ebsco.com/ .
34. Мельник, С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка.— К.: ВІКНУ, 2011.— Вип. 30.— С. 159–165.
35. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша — К.: ВБ «Аванпост-Прим», 2012.— 214 с.
36. Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/2824-15.— Офіц. вид.— К.: Відомості Верховної Ради України від 10.02.2006.

37. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Відомості Верховної Ради України від 01.12.1992.
38. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 30.07.2003, № 139.
39. Про державну службу спеціального зв'язку та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 11.04.2006, № 68.
40. Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV [Електронний ресурс].— Режим доступу: http://zakon1.rada. gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 24.12.2003, № 243.
41. Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, № 80/94-ВР [Електронний ре- сурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Відомості Верховної Ради України від 02.08.1994.
42. Про доступ до публічної інформації: за станом на 09.06.2013 р. / Закон, затверджений ВР України 13.01.2011, № 2939-VI [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/2939-17.
43. Про оборону України: за станом на 01.07.2013 р. / Закон, затверджений ВР України 06.12.1991, № 1932-XII [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12.— Офіц. вид.— К.: Відомості Верховної Ради України від 03.03.1992.
44. Про засади внутрішньої і зовнішньої політики: за станом на 01.07.2010 р. / Закон, затверджений ВР України 01.07.2010, № 2411-VI [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show /2411-17.— Офіц. вид.— К.: Відомості Верховної Ради України від 08.10.2010.
45. Про об'єкти підвищеної небезпеки: за станом на 18.11.2012 р. / Закон, затверджений ВР України 18.01.2001, № 2245-III [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/2245-14.— Офіц. вид.— К.: Відомості Верховної Ради України від 13.04.2001.
46. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007 [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/maincgi.— Офіц. вид.— К.: Урядовий кур'єр від 07.03.2007, № 43.
47. Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 р. / Указ Президента України від 8.02.2009 р., № 514/2009 [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Офіційний вісник України від 20.07.2009.

48. Про Воєнну доктрину України: за станом на 22.06.2012 р. / Указ Президента України від 15.06.2004, № 648/2004 [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/648/2004.— Офіц. вид.— К.: Офіційний вісник України від 13.08.2004.
49. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007, № 537-V [Електронний ресурс].— Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16.— Офіц. вид.— К.: Відомості Верховної Ради України від 23.03.2007.
50. Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України: проект за станом на 06.03.2013 р. № 2483 [Електронний ре- сурс].— Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998.
51. Семенов, Ю. А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности [Електронний ресурс] / Ю. А. Семенов.— Режим доступу: http://book.itep.ru/10/2012.htm
52. Competitive intelligence [Електронний ресурс].— Режим доступу: http://en.wikipedia.org/wiki/Competitive_intelligence.
53. Карпов, Г. Атака на DNS или ночной кошмар сетевого администратора [Електронний ресурс] / Геннадий Карпов.— Режим доступу: http://www.hackzone.ru/articles/dns-poison.html, 02.06.2007.
54. Инциденты информационной безопасности: рекомендации по реагированию.— М.: Group-IB и LETA, 2011.— 20 с.
55. Харченко, В. П. Кибертерроризм на авиационном транспорте / [В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк] // Проблеми інформатизації та управління: Зб. наук. праць.— 2009.— Вип. 4 (28).— С. 131–140.
56. Дубов, Д. В. Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван.— К.: НІСД, 2011.— 30 с.
57. Гавриш, С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії [Електронний ресурс] / С. Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика).— Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm
58. Довгань, О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // Інформаційна безпека людини, суспільства, держави.— 2011.— № 3 (7).— С. 49–53.
59. Гаврилов, Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю. В. Гаврилов, Л. В. Смирнов.— М.: ЮИ МВД РФ, 2003.— 66 с.
60. Національний стандарт України ДСТУ ISO/IEC 18053:2018 Інформаційні технології. Телекомунікації та обмін інформацією між системами. Словник термінів у сфері телекомунікаційних за стосунків з комп'ютерною підтримкою. Стадія ІІІ. – К.:УкрНДНЦ – 122с.

61. Банкет В.Л.. и др. Защита информации в системах телекоммуникации, — О.: Изд-во УГАС, 1997. — 95 с.
62. Бармен Скотт Разработка правил информационной безопасности,: Пер, с англ, — М.: Издательский дом “Вильямс”, 2002, — 208 с.
63. Введение в криптографию/Под общ, ред. В,В, Ященко, — 2-е изд., испр, — М.: МЦНМО: “ЧеРо”, 1999. — 272 с.
64. Вербіцький О.В. Вступ до криптології, — Л,: Видавництво науково-технічної літератури, 1998. — 247 с.
65. Ганенко О.Ю, Защита информации. Основи информационного управления, СПб.: Изд. дом “Сентябрь”, 2001. — 228 с.
66. Горохов П.К, Информационная безопасность. Англо-русский словарь, — М.: Радио и связь, 1995.— 224 с.
67. Демин В.П., Куприянов А.И., Сахаров А.В. Радиоэлектронная разведка и радиомаскировка. — М.: Изд-во МАИ, 1997. — 156 с.
68. Зегжда Д.П., Ивашко Л.М. Как построить защищенную информационную систему/Под научной редакцией Зегжды Д.П.. и Платонова В.М. — СПб: Мир и семья, 1997 - 312 с.
69. Землянова Л.Д, Зарубежная коммуникативиетика в преддверии информационного общества: Толковый словарь терминов и концепций. М.: — Изд-во Моск. ун-та, 1999. — 301 с.
70. Зима В.М., Молдовян А.А., Молдовян П.А. Компьютерные сети и защита передаваемой информации, — Спб.: Изд-во Спб. ун-та, 1998, — 328 с.
71. Коваленко М.М. Комп’ютерні віруси і захист інформації. К,: Наукова думка, 1999. - 269 с.
72. Комп’ютерний словник / Пер. з англ. В. О. Соловйова. - К.: Україна, 1997. - 470 с.
73. Конхейм А.Г. Основы криптографии / Пер. с англ.. — М.: Мир, 1987. — 412 с.
74. Кузьминой Т.В. Криптографические методы защиты информации. — Новосибирск: Наука. Сиб. предприятие РАН, 1998.—194 с.
75. Мельников В.В. Защита информации в компьютерных системах. — М.: Финансы и статистика; Электроинформ, 1997. — 368 с.
76. Новий тлумачний словник української мови у чотирьох томах, — К.: Видавництво “Аконіт”, 1998.
77. Петраков А.В. Основы практической защиты информации. — М.: Радио и связь, 1999. — 368 с,
78. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа/Пер. с англ. В. Смирнова. — М.: КРОН-ПРЕСС, 1999. — 816 с. — Серия “Экспресс”.
79. Словарь по кибернетике / Под ред. В.М. Глушкова. — К.: Главная редакция УСЭ, 1979, — 624 с.
80. Словник іншомовних слів / За ред. О.С. Мельничука, — К.: Головна редакція УРЕ, 1974. — 776 с,
81. Толковый словарь по основам информационной деятельности, — К.: УкрИНТЭИ, 1995. — 252 с.
82. Хорошко В.О. та ін. Термінологічний довідник з питань технічного захисту інформації. — Київ. 1998. — 135 с.

83. Брукшир Дж. Г. Введение в компьютерные науки.- К.: Издательский дом «Вильямс», 2001.-688с.
84. Великий тлумачний словник сучасної української мови/ Укладач і головний редактор В.Т.Бусел.-К.:Ірпінь: ВТФ «Перун», 2004.-1440с.
85. Масловский Е.К. Англо-русский словарь по основам компьютерной грамотности. - М.: Издательское объединение “ЮНИТИ", 1993. — 164 с.
86. Миромчиков И.К., Павловцев В.А. Англо-русский толковый словарь по Интернет. Изд. 3-3. - Мн.: Харвест, М. Аст, 2000. - 288 с.
87. Невдяев Л.М. Телекоммуникационные технологии Англо-русский словарь-справочник. - М.: МЦНТИ, ООО “Мобильные телекоммуникации". 2002. — 592 с.
88. Орлов С. Современный англо-русский словарь по вычислительной технике. - М.: ЛОРИ, 1996. - 588 с.
89. Севастьянов А.В. Англо русский толковый словарь сокращениий в области компьютерных и информационных технологий. — М.: ЭКОМ, 1995. — 288 с.
90. Смит Р. Аутентификация: от паролей до открытых ключей. — М.: Издательский дом “Вильямс", 2002. — 432 с.
91. Рицар Б., Семенистий К., Кочан І. Російсько-український та українсько-російський словник з радіоелектроніки. - Львів: “Логос", 1995. — 608 с.
92. Гсйченко В.В., Завірюхіна В.М., Зеленюк О.О. та ін. Російсько-український словник наукової термінології: Математика. Фізика. Техніка. Науки про Землю та Космос. - К.: Наукова думка, 1998. - 892 с.
93. Англо-український словник з інформатики та обчислювальної техніки / Лінгв. редактор О.Р. Микитюк. - Львів: СП “БаК", 1995.-304 с.
94. Karen Southwick. High Noon: the inside story of Scott McNealy and the rise of Sun Microsystems. John Wiley & Sons. 1999. - 242 pp.
95. Kevin D. Mitnik. The Art of Deception. Wiley Publishing, USA. 2002. - 352 pp.
96. Tom Clancy. The Bear and the Dragon. Penguin Books, 2001. — 1138 pp.
97. Michael Lewis. The new new things. A Silicon Valley Story. Coronet books, 2000. — 413 pp.
98. Glossary of Security Terms. Доступ в Інтернет: https://www.sans.org/security-resources/glossary-of-terms/
99. Cyber Security Glossary. Доступ в Інтернет: https://www.cybrary.it/glossary/
100. Glossary of cyber security terms. Доступ в Інтернет: https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Glossary-of-cyber-security-terms/
101. Explore Terms: A Glossary of Common Cybersecurity Terminology. Доступ в Інтернет: https://niccs.us-cert.gov/about-niccs/glossary
102. Computer Security – Terminologies. Доступ в Інтернет: https://www.tutorialspoint.com/computer_security/computer_security_terminologies.htm
103. Donald L. Brinkley and Roger R. Schell Concepts and Terminology for Computer Security. Доступ в Інтернет: https://www.acsac.org/secshelf/book001/02.pdf

104. William Jackson A comprehensive list of security terms you should know. Доступ в Інтернет: https://gcn.com/articles/2013/06/17/nist-infosec-cybersecurity-glossary.aspx
105. Cyber Security Glossary. Доступ в Інтернет: https://www.optus.com.au/content/dam/optus/documents/enterprise/pdf/Cybersecurity-Glossary_FINAL.pdf
106. IT Security Terminology. Доступ в Інтернет: http://www.onu.edu/information_technology/it_security/it_security_terminology

Довідкове видання

А.Я. Гладун, О.О. Пучков, І.Ю. Субач, К.О. Хала

Англо-український
СЛОВНИК ТЕРМІНІВ
з інформаційних технологій та кібербезпеки

В авторській редакції

Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Підписано до друку 13.12.2018. Формат 60×84$^{1}/_{16}$. Папір офіс. Гарнітура Times.

ІСЗЗІ КПІ ім. Ігоря Сікорського,
м. Київ вул. Верхньоключова, 4, тел. 204-91-51