КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(21), 2023
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2023.21.99120
УДК 004.056

Соколов Володимир Юрійович
к.т.н., доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Складанний Павло Миколайович
к.т.н., доцент
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

МЕТОДИКА ОЦІНКИ КОМПЛЕКСНИХ ЗБИТКІВ ВІД ІНЦИДЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Інциденти безпеки можуть мати значні економічні наслідки для органів державної влади. Щоб пом'якшити економічні наслідки інцидентів у сфері кібербезпеки, органи державної влади повинні інвестувати в надійні заходи протидії та співпрацю з іншими державними установами, партнерами з приватного сектору та міжнародними організаціями може сприяти підвищенню стійкості та спроможності реагування на кібератаки. В статті використовується аналіз різних вразливостей та механізм перетворення в інцидент безпеки, а також проаналізовані підходи до відслідковування існуючих загроз та методи протидій ним. В якості джерел даних можуть виступати міжнародні та національні організації та асоціацію. Результати з різних звітів агрегуються в залежності від галузі роботи певної організації та її форми власності. Розгляд механік переходу вразливостей в інциденти безпеки дозволяє створювати формалізовані моделі для систем аудиту та розбору виявлених інцидентів або відслідковування в реальному часі. Одним з основних критеріїв є оцінка ризиків кібербезпеки. В публікації запропонований метод, який враховує взаємозв'язок компонентів системи та дозволяє враховувати послідовність задіяності даних компонентів. В якості міжнародного та національного досвіду розглянуті джерела оперативної та звітної інформації про інциденти безпеки. В результаті запропоновані заходи по зменшенню ризику використання існуючих вразливостей для державних інформаційних мереж та систем. Що не єдиний метод якісного переходу по зменшенню збитків від кіберінцидентів полягає в підвищенні якості фахівців з кібернетичної безпеки, тому в статті запропонований нова програма перепідготовки фахівців із суміжних галузей: інформаційних технологій, телекомунікацій, електроніки, радіотехніки, програмування тощо. В результаті даного дослідження видно, що формування політики безпеки для держаних установ має враховувати також економічний вплив та ймовірні збитки від кібернетичних атак. Подальші дослідження спрямовані на валідацію запропонованих рекомендацій щодо формування політики безпеки для держаних та комерційних установ та організацій.

Ключові слова: кібербезпека; захист інформації; вразливість; ризик; інцидент безпеки.

ВСТУП

Інциденти безпеки можуть мати значні економічні наслідки для органів державної влади. Коли органи державної влади та державні підприємства та організації стикаються з інцидентами кібербезпеки, такими як витік даних або атаки з вимогою викупу, можуть виникнути кілька економічних наслідків: перебоїв в наданні послуг, впливу на

© В.Ю. Соколов, П.М. Складанний 2023

економічний розвиток, втрат фінансів, суспільної довіри та інтелектуальної власності, репутаційних збитків, збільшення витрат на кібербезпеку, відновлення та усунення наслідків.

Для органів державної влади, які займаються дослідженнями і розробками або інноваціями, інциденти кібербезпеки, можуть мати довгострокові економічні наслідки. Викрадена або пошкоджена інформація може бути використана конкурентами або супротивниками, що вплине на економічну конкурентоспроможність та інновації.

Постановка проблеми. Щоб пом'якшити економічні наслідки інцидентів у сфері кібербезпеки, органи державної влади повинні інвестувати в надійні заходи з кібербезпеки, включаючи регулярну оцінку ризиків, плани реагування на інциденти, навчання співробітників, а також впровадження передових практик і галузевих стандартів. Крім того, співпраця з іншими державними установами, партнерами з приватного сектору та міжнародними організаціями може сприяти підвищенню стійкості та спроможності реагування на кібератаки. Проактивні зусилля із запобігання інцидентам та ефективного реагування на них у разі їх виникнення є важливими для захисту економіки та державних послуг.

Аналіз останніх досліджень і публікацій. В попередніх дослідженнях [1] – [3] були розглянуті підходи до оцінки ризиків інформаційних загроз, та дана загальна оцінка вартості інцидентів безпеки.

Одним з ефективних методів зменшення ймовірності перетворення вразливості на інцидент безпеки є впровадження стратегії глибинного захисту 'Defense in Depth' (DiD) — багаторівневого підходу до безпеки, який передбачає розгортання декількох заходів безпеки на різних рівнях інформаційної системи. Цей підхід спрямований на створення надлишкових рівнів безпеки, що ускладнює зловмисникам успішну експлуатацію вразливостей: захист периметра [4], контроль доступу [5], керування виправленнями [6],сегментація мережі [7], шифрування [8],виявлення та моніторинг вторгнень [9], безпека додатків [10], тренінги персоналу [11], план реагування на інциденти [12], регулярні оцінки та аудити [13], резервне копіювання та аварійне відновлення [14].

Впроваджуючи ці багаторівневі засоби захисту, організації можуть значно зменшити ймовірність того, що вразливість буде успішно використана і перетвориться на інцидент безпеки. Жоден захід безпеки не є стовідсотково надійним, тому в даному досліджені ми пропонуємо оцінити взаємний вплив вразливості компонентів інформаційної системи.

МЕТОДИКА ДОСЛІДЖЕННЯ

В даній статті використовується аналіз різних вразливостей та механізм перетворення в інцидент безпеки. В якості об'єкту дослідження використовуються інформаційні системи державних і приватних підприємств та організацій. Основним методом дослідження є метод оцінки ризиків кібербезпеки за допомогою розрахунку взаємного впливу та потенційних збитків.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Механіка переходу вразливості в інцидент безпеки

Оцінка ймовірності передбачає, що вразливість буде використана та призведе до інциденту безпеки. Послідовність шляхів та компонентів перетворення показана на рис. 1, де:

– *потенційна вразливість* — це слабкість або недолік системи, який може бути використаний зловмисниками або зловмисними суб'єктами. Вразливості можуть існувати в програмному забезпеченні, апаратному забезпеченні, мережевих конфігураціях або навіть у людських процесах;

– ідентифікація потенційних *суб'єктів загрози* є важливою частиною оцінки ймовірності. Це можуть бути хакери, кіберзлочинні організації, державні зловмисники, інсайдери або навіть випадкові загрози, спричинені авторизованими користувачами;

– оцінка ймовірності враховує *фактори експлуатації*, які визначають легкість або складність використання вразливості. Вони можуть включати такі фактори, як складність вразливості, рівень необхідних технічних знань та доступність інструментів або методів використання вразливості;

– ефективність існуючих засобів *контролю безпеки* та контрзаходів є ще одним важливим аспектом оцінки ймовірності. Ефективні заходи безпеки, такі як брандмауери, системи виявлення вторгнень, контроль доступу та шифрування, можуть значно знизити ймовірність успішної експлуатації;

– оцінка ймовірності часто є частиною більш широкого процесу *управління ризиками*. Розуміючи ймовірність використання вразливості та потенційний вплив, організації можуть приймати обґрунтовані рішення щодо визначення пріоритетів та розподілу ресурсів для зменшення вразливості та реагування на інциденти.

– *аналіз потенційного впливу* інциденту безпеки має важливе значення для розуміння серйозності та наслідків. Вплив може включати фінансові втрати, компрометацію конфіденційних даних, перебої в наданні послуг, шкоду репутації, правові та регуляторні наслідки тощо;

– *оцінка ймовірності* передбачає аналіз різних факторів для визначення ймовірності використання вразливості. Зазвичай вона враховує технічні аспекти вразливості, можливості та мотивацію потенційних зловмисників, а також наявні заходи безпеки.

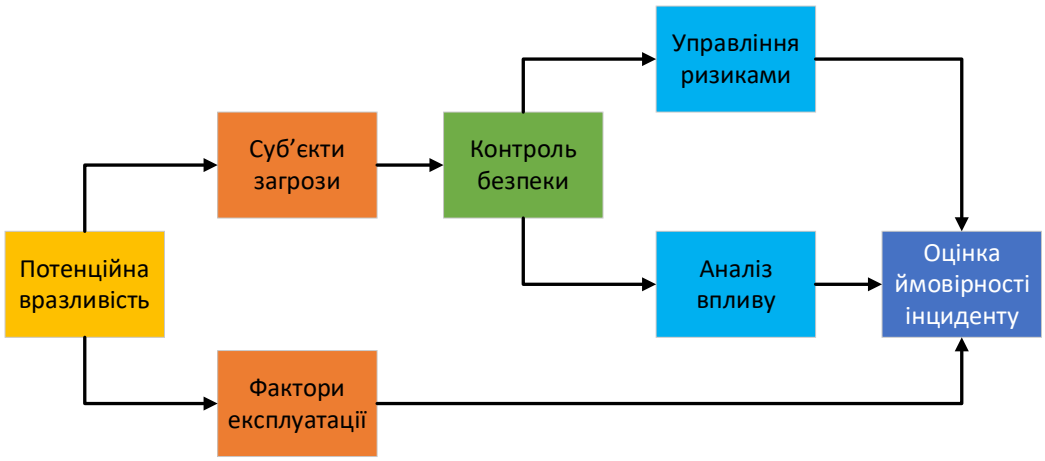

Рис. 1. Схема зв'язків між вразливістю та ймовірністю її реалізації

Оцінка ймовірності не є остаточним прогнозом, а радше обґрунтованою оцінкою, що базується на наявній інформації та аналізі. Це допомагає організаціям зрозуміти потенційні ризики та вжити проактивних заходів для їх зменшення.

Моделювання загроз — це системний підхід до ідентифікації та розуміння потенційних загроз і вразливостей у системі чи програмі. Створення моделі загроз допомагає організаціям завчасно оцінювати ризики безпеці та впроваджувати відповідні засоби пом'якшення. Ключові елементи моделі загроз включають:

1. Визначте цінні *активи*, дані та ресурси, які потребують захисту. Це стосується конфіденційної інформації, інтелектуальної власності, апаратного забезпечення, програмного забезпечення та будь-яких інших критичних компонентів.

2. Визначте всі точки або *інтерфейси* — поверхню атаки, через які користувачі, служби або зовнішні об'єкти можуть отримати доступ до системи або взаємодіяти з нею. Це включає API, мережеві інтерфейси, інтерфейси користувача тощо.

3. Визначте потенційних *суб'єктів загрози*, які можуть націлитися на систему. Це може включати хакерів, кіберзлочинців, інсайдерів, конкурентів, суб'єктів держави або навіть випадкові загрози від авторизованих користувачів.

4. Створюйте сценарії *загроз* або випадки використання, які описують, як різні суб'єкти загрози можуть спробувати використати вразливі місця для компрометації активів або порушення роботи служб.

5. Визначте потенційні слабкі або *вразливі* місця в системі. Це включає як технічні вразливості (наприклад, недоліки програмного забезпечення, неправильні конфігурації), так і пов'язані з людиною вразливості (наприклад, соціальна інженерія, слабкі паролі).

6. Опишіть конкретні методи або прийоми — *вектори* атак, які можуть використовувати зловмисники, щоб використовувати виявлені вразливості та отримати несанкціонований доступ або контроль над активами.

7. Аналізуйте *ризик* та потенційного впливу кожного сценарію загрози, що передбачає оцінку ризику успішних атак і оцінку тяжкості наслідків.

8. Визначте *вимоги безпеки*, необхідні для захисту активів і запобігання успішному використанню вразливостей. Це включає вказівку передових методів безпеки та стандартів, яких слід дотримуватися.

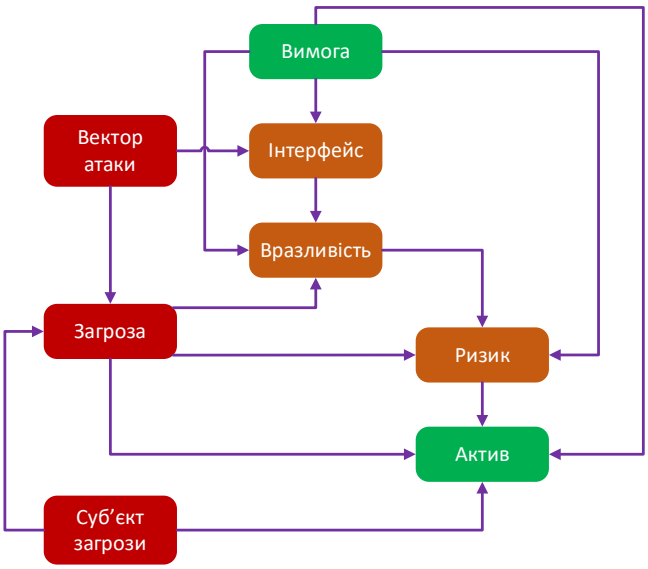

Рис. 2. Взаємозв'язок ключових елементів моделі загроз [15], [16]

Моделювання загроз — це спільна робота, яка включає експертів із безпеки, розробників, архітекторів та інших зацікавлених сторін. Це допомагає організаціям визначати пріоритети заходів безпеки, ефективно розподіляти ресурси та створювати більш стійкі системи проти потенційних загроз.

Також слід зазначити, що документування будь-яких *припущень*, зроблених під час процесу моделювання загроз. Припущення допомагають зберегти ясність щодо обсягу та обмежень моделі. А сам процес моделювання загроз має бути *безперервним*. У міру розвитку системи можуть з'являтися нові загрози, а існуючі ризики можуть змінюватися, що вимагає регулярного оновлення моделі загроз.

Метод оцінки ризиків кібербезпеки

Оцінка ризиків кібербезпеки — це безперервний процес, який вимагає постійного моніторингу та коригування, оскільки ландшафт загроз змінюється і виявляються нові вразливості. Тому розрахунок поточного ризику має проводитися з певної регулярністю або навіть безперервно.

Обчислити точну ймовірність інциденту безпеки досить складно через складність і динамічний характер загроз кібербезпеки. Однак загальний підхід до оцінки ймовірності інциденту безпеки полягає у визначені ймовірності кожного компоненту за певний період часу:

$$P_{\text{інц}} = P_{\text{загр}} \cdot P_{\text{вразл}} \cdot K_{\text{пош}} \cdot I_{\text{впл}}\big|_{t\in[t_0..t_{\text{вияв}}]} \quad (1)$$

де $P_{\text{загр}}$ — ймовірність того, що суб'єкт загрози або зловмисник спробує використати вразливість або здійснити атаку, яка враховує можливості, наміри та історичну поведінку суб'єкта загрози; $P_{\text{вразл}}$ — ймовірність успішного використання вразливості, яка враховує легкість використання, наявність засобів контролю та рівень вразливості; $K_{\text{пош}}$ — поширеність та впізнаваність бренду або компонентів інформаційної системи; $I_{\text{впл}}$ — потенційний вплив або наслідки в разі виникнення інциденту безпеки, який складається з фінансових втрат, витоку даних, перебоїв в обслуговуванні, шкоди репутації, юридичним наслідкам та регуляторним штрафам. Треба зазначити, що час до виявлення $t_{\text{вияв}}$ може наближатися до нескінченності.

Методології оцінки ризиків, такі як якісний або кількісний аналіз ризиків, можуть бути використані для присвоєння значень цим факторам і отримання оціночної ймовірності інциденту безпеки, як показано на рис. 3. Кожен компонент зазвичай оцінюється за шкалою (наприклад, низький, середній, високий) або присвоюються числові значення. Формула часто використовується як якісне представлення, а не як точний математичний розрахунок. Добуток цих значень дає загальний рейтинг ризику, що допомагає організаціям визначати пріоритети своїх зусиль у сфері безпеки.

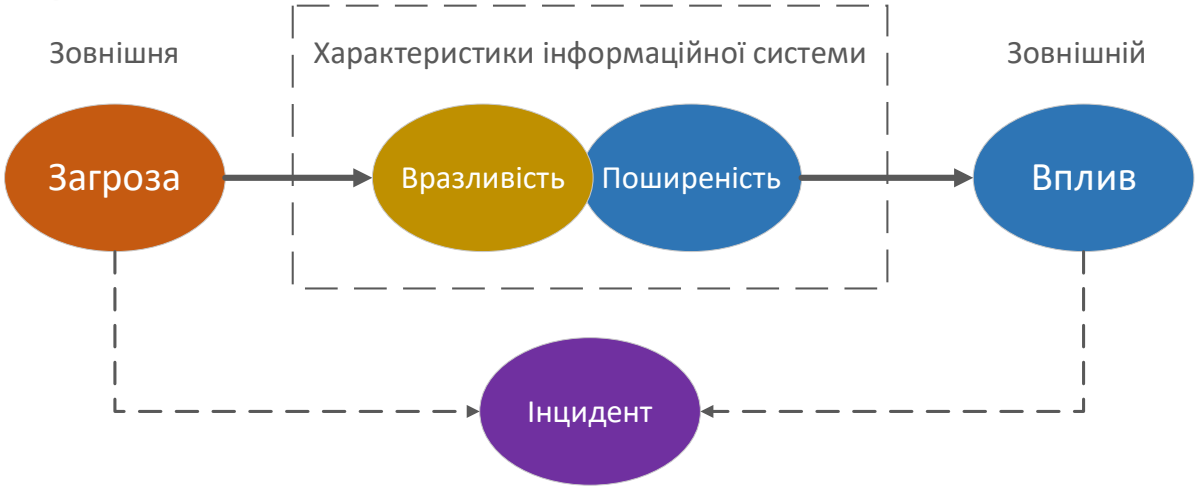

Рис. 3. Співвідношення факторів оцінки інциденту безпеки

Розрахунок ймовірності інциденту безпеки може бути складним завданням через складність і динамічний характер загроз кібербезпеки. Так як загальна забезпеченість безпеки інформаційної безпеки складається з комбінації ймовірностей для кожного компоненту.

Для розрахунку такої системи можна застосувати комбінований підхід. Загальна максимальна сума збитків складається зі прямих і непрямих збитків:

$$\Sigma = \Sigma_{\text{прям}} + \Sigma_{\text{непрям}} + \Sigma_{\text{зз}}\big|_{\Delta t} \tag{2}$$

де $\Sigma_{\text{прям}}$ — збитки від прямих атак за час Δt; $\Sigma_{\text{непрям}}$ — збитки від впливу на попередні ланки; $\Sigma_{\text{зз}}$ — збитки від ланок зворотного зв'язку. Окремо їх можна представити у вигляді сукупності:

$$\begin{cases} \Sigma_{\text{прям}} = \sum P_{\text{пот}} \cdot C_{\text{пот}}, \\ \Sigma_{\text{непрям}} = \sum \delta_{\text{поч–кінц}} \cdot P_{\text{поч}} \cdot C_{\text{кінц}}, \\ \Sigma_{\text{зз}} = \sum \delta_{\text{кінц–поч}} \cdot P_{\text{кінц}} \cdot C_{\text{поч}}, \end{cases} \tag{3}$$

де $P_{\text{пот}}$, $P_{\text{поч}}$ і $P_{\text{кінц}}$ — ймовірність інциденту безпеки для поточного, початкового і кінцевого модулів складної інформаційної системи; $C_{\text{пот}}$, $C_{\text{поч}}$ і $C_{\text{кінц}}$ — потенційні сумарні збитки від інциденту; $\delta_{\text{поч–кінц}}$ і $\delta_{\text{кінц–поч}}$ — коефіцієнт впливу початкового модуля на кінцевий і навпаки.

Для складних систем крім атак на окремі компоненти існує вплив джерел даних на наступні ланки обробки (1–2) і (1–3) на рис. 4. Деякі системи можуть мати і зворотні зв'язки (3–1).

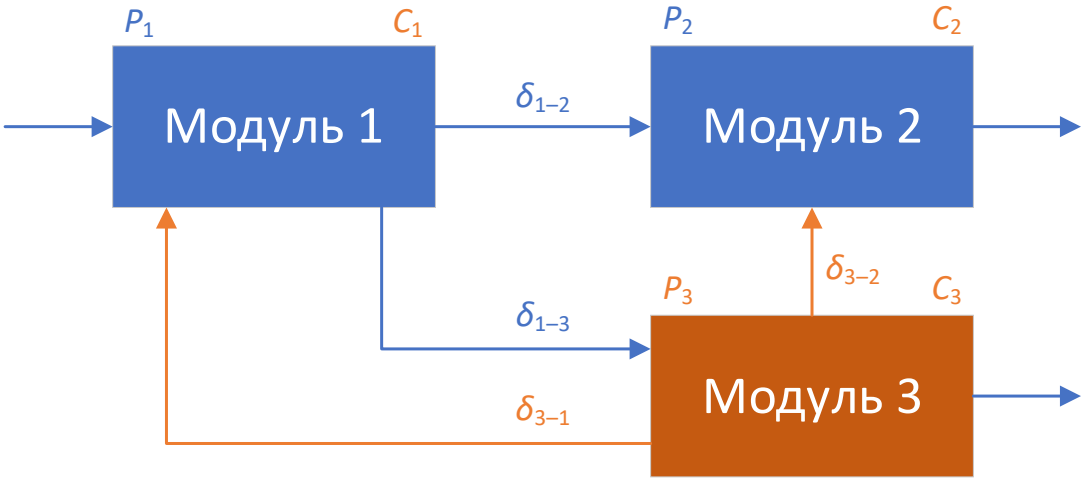

Рис. 4. Взаємний вплив різних компонентів інформаційної системи

Розглянемо окремий випадок, зображений на рис. 4, та з формул (2) і (3) отримаємо:

$$\Sigma = P_3 \cdot C_3 + \delta_{3-2} \cdot P_3 \cdot C_2 + \delta_{3-1} \cdot P_3 \cdot C_1|_{\Delta t} = P_3(C_3 + \delta_{3-2} \cdot C_2 + \delta_{3-1} \cdot C_1)|_{\Delta t}. \quad (4)$$

Обчислити точну ймовірність перетворення потенційної вразливості на інцидент безпеки досить складно, оскільки це пов'язано з невизначеністю та динамічними факторами. Мета полягає в тому, щоб допомогти особам, які приймають рішення, визначити пріоритети в їхніх зусиллях щодо усунення потенційних вразливостей і зниження загального ризику інцидентів безпеки. Крім того, слід регулярно оновлювати та коригувати оцінку, щоб відобразити зміни в ландшафті загроз та конфігурації системи.

Розвиток звітування про інциденти безпеки

Для отримання останньої статистики та інформації про інциденти кібербезпеки рекомендовано звертатися до авторитетних звітів з кібербезпеки, наприклад:

1. Verizon Data Breach Investigations Report, DBIR [17].
2. National Security Agency, NSA [18].
3. Cybersecurity and Infrastructure Security Agency, CISA [19].
4. Internet Security Threat Report, ISTR [20].
5. CrowdStrike Global Threat Report [21].

А також склалася ситуація, в якій індивідуальне відслідковування інцидентів окремої організації вже не може бути покрите самотужки. В такій ситуації державні та міжнародні організації частково беруть функції по моніторингу та протидії на себе. Можна виділити деякі такі організації:

– команди реагування на комп`ютерні надзвичайні ситуації (Computer Emergency Response Teams, CERTs);

– центри обміну та аналізу інформації (Information Sharing and Analysis Centers, ISACs);

– Інтерпол та Європол (European Cybercrime Centre, EC3);

– національні агентства з кібербезпеки: Федеральне бюро розслідувань (Federal Bureau of Investigation, FBI), Міністерство внутрішньої безпеки Сполучених Штатів (Department of Homeland Security, DHS), Національний центр кібербезпеки Сполученого

Королівства (National Cyber Security Centre, NCSC), Австралійський центр кібербезпеки (Australian Cyber Security Centre, ACSC) та ін.;

– глобальні організації з питань безпеки: Всесвітній економічний форум (World Economic Forum, WEF) та Організація Об'єднаних Націй (United Nations, UN);

– приватні компанії з кібербезпеки (Symantec, FireEye, CrowdStrike та інші);

– спільноти з розвідки кіберзагроз з відкритим кодом: Ліга розвідки кіберзагроз (Cyber Threat Intelligence League, CTIL), Мережа розвідки кіберзагроз (Cyber Threat Intelligence Network, CTIN) та ін.

Серед найпоширеніших інцидентів, пов'язаних з інформаційною безпекою, можна виділити наступні:

1. *Фішингові атаки* є однією з найпоширеніших загроз кібербезпеці. Згідно зі звітом DBIR за 2021 рік, на фішингові атаки припадає 36% усіх проаналізованих витоків даних [17].

2. Атаки *вірусів-здирників* полягають у шифруванні даних жертви та вимозі викупу за їх розшифрування. За останні роки кількість атак з вимогою викупу різко зросла, а гучні інциденти зачепили різні організації, зокрема провайдерів критично важливої інфраструктури та державні установи.

3. *Шкідливе програмне забезпечення* (віруси, трояни тощо) залишається значною загрозою, націленою як на окремих осіб, так і на організації.

4. *Внутрішні загрози* пов'язані з особами в організації, які навмисно чи ненавмисно ставлять під загрозу безпеку. Це можуть бути працівники, підрядники або інші довірені особи, які мають доступ до конфіденційної інформації.

5. Порушення даних передбачає несанкціонований доступ до конфіденційної інформації, що призводить до потенційного *витоку персональних або фінансових даних*. Порушення можуть статися через хакерські атаки, дії інсайдерів або випадковий витік інформації.

Заходи по зменшенню ризику використання існуючих вразливостей

Зниження ризику використання відомих та невідомих вразливостей в інформаційній системі має вирішальне значення для забезпечення безпеки та цілісності системи та її даних. Можна виділити кілька ефективних способів зменшити ризик експлуатації:

1. Пасивні заходи:

– *сегментація* мережі та *ізоляція* критично важливих активів і даних за допомогою сегментації мережі може обмежити вплив потенційного порушення;

– захист конфіденційних даних за допомогою *шифрування* забезпечує додатковий рівень безпеки;

– *безпечна конфігурація* систем допомагає зменшити поверхню атаки та потенційні вразливості;

– *безпечна розробка додатків* допомагає запобігти поширеним вразливостям;

– постійне оновлення програмного забезпечення та систем найновішими пакетами безпеки, регламентований механізм *управління виправленнями*;

– наявність чітко розробленого *плану реагування на інциденти* забезпечує швидке та скоординоване реагування на інциденти безпеки;

– попри свою важливість, *фізична безпека*, як правило, менш критична для інформаційних систем порівняно із заходами цифрової безпеки.

2. Активні заходи:

– *безперервний моніторинг* мережевої та системної активності в режимі реального часу допомагає оперативно виявляти загрози та реагувати на них;

– *регулярне резервне копіювання* критично важливих даних захищає від втрати даних у разі порушення;

– впровадження *брандмауерів* та систем виявлення/запобігання вторгненням допомагає відстежувати та контролювати мережевий трафік і виявляти підозрілі дії;

– належний *контроль доступу* та управління дозволами користувачів має вирішальне значення для запобігання несанкціонованому доступу до конфіденційних даних.

3. Превентивні заходи:

– *тренінги* з підвищення обізнаності про безпеку серед співробітників і користувачів за найкращими практиками безпеки допомагають запобігти людським помилкам і атакам соціальної інженерії;

– оцінка та *управління ризиками*, пов'язаними зі сторонніми постачальниками, допомагає захиститися від атак на ланцюги поставок;

– інформованість про *останні загрози* (розвідка) та *оновлення системи* безпеки допомагає ефективно реагувати на нові ризики;

– регулярне *оцінювання вразливостей* дає цінну інформацію про стан безпеки системи.

Заходи по підвищенню якості фахівців з кібербезпеки

Покращення якості освіти для фахівців з кібербезпеки може підвищити їхню здатність до працевлаштування в міжнародних організаціях. Ось кілька стратегій, як цього досягти:

1. Навчальні заклади та організації повинні розробити *комплексні та сучасні навчальні програми*, які охоплюють новітні концепції, технології та найкращі практики кібербезпеки. Навчальна програма повинна відображати швидкозмінний ландшафт кібербезпеки, щоб забезпечити випускників відповідними знаннями та навичками.

2. *Партнерство з професіоналами та галузевими лідерами* може допомогти навчальним закладам узгодити свої програми з реальними викликами та потребами. Гостьові лекції, стажування та спільні проекти можуть надати студентам практичний досвід та ознайомити їх із сучасними галузевими тенденціями.

3. Практичні заняття та симуляції: Включіть у навчальну програму *практичні лабораторні роботи*, вправи з кібербезпеки та симуляції, щоб дати студентами практичний досвід боротьби з реальними кіберзагрозами. Практичні заняття покращують їхні здібності до вирішення проблем та формують впевненість у собі.

4. Заохочуйте студентів до отримання відповідних *сертифікатів*, таких як CompTIA Security+, Certified Ethical Hacker (CEH) або Certified Information Systems Security Professional (CISSP). Ці сертифікати демонструють потенційним роботодавцям експертизу та відданість справі.

5. Заохочуйте участь у *змаганнях з кібербезпеки* та заходах Capture The Flag (CTF). Ці змагання дозволяють учням застосовувати свої знання в конкурентному середовищі, сприяють розвитку навичок і розширенню можливостей для налагодження контактів.

6. *Етична поведінка та дотримання професійних стандартів* мають вирішальне значення у сфері кібербезпеки. Переконайтеся, що етичні міркування та відповідальне використання навичок підкреслюються протягом усього навчального процесу.

7. Сприяйте розвитку культури *безперервного навчання* та професійного розвитку. Заохочуйте студентів бути в курсі останніх тенденцій у сфері кібербезпеки, відвідувати конференції, вебінари та семінари.

8. Різноманітні методи навчання: Пропонуйте *різноманітні методи навчання*, такі як онлайн-курси, віртуальні лабораторії та гнучкі графіки, щоб задовольнити різноманітні потреби студентів та працюючих фахівців.

9. Переконайтеся, що викладачі з кібербезпеки мають відповідний *галузевий досвід та сертифікати*. Досвідчені викладачі можуть надати цінну інформацію та наставництво студентам.

10. Заохочуйте *дослідження* та *інновації* в галузі кібербезпеки та підтримуйте проекти, які сприяють передовим розробкам у цій сфері. Програми, орієнтовані на дослідження, приваблюють студентів і підвищують авторитет установи.

11. На додаток до технічних навичок, зосередьтеся на розвитку у студентів навичок спілкування, роботи в команді та вирішення проблем. Ці *«м'які» навички* необхідні для ефективної співпраці в міжнародних організаціях.

12. Налагодьте міцні зв'язки з потенційними роботодавцями та надайте *допомогу у працевлаштуванні та стажуванні* студентам для отримання практичного досвіду та побудови професійних зв'язків.

Процес підготовки фахівців з кібербезпеки регулюється різними документами та стандартами як на національному, так і на міжнародному рівнях. Ці документи містять керівні принципи, рамки та найкращі практики для розробки навчальних програм з кібербезпеки. Ключові документи приведено в табл. 1.

Таблиця 1

Документи, які регламентують підвищення кваліфікації в сфері кібербезпеки

Документ	**Сфера застосування**	**Ціль**	**Регіон**	**Рік**
CompTIA Security+ Exam Objectives [22]	Початкові знання з кібербезпеки	Визначити знання та навички для фахівців з кібербезпеки початкового рівня	Міжнародний	2019
Academic Curricula Guidelines for Cybersecurity Education [23]	Зміст академічної програми з кібербезпеки	Надати рекомендації для академічних програм з кібербезпеки	Міжнародний	2017
European Cybersecurity Skills Framework (ECSF) [24]	Навички та компетенції з кібербезпеки	Створити загальний еталон для навичок та компетенцій з кібербезпеки в Європі	Європейський Союз	2015
ISO/IEC 27032:2023 [25]	Навчання та тренінги з кібербезпеки	Надати рекомендації щодо освіти та навчання з кібербезпеки	Міжнародний	2023
Certified Information Systems Security Professional (CISSP) [26]	Професійні навички з кібербезпеки	Визначити області знань для фахівців з кібербезпеки	Міжнародний	2019
NICE Cybersecurity Workforce Framework [27]	Таксономія трудових ресурсів у сфері кібербезпеки	Визначити ролі, завдання та навички у сфері кібербезпеки для підтримки розвитку кваліфікованої робочої сили	Сполучені Штати	2017

Методика перепрофілювання спеціалістів з інформаційних технологій

Для забезпечення доступності навчальних програм з кібернетичної безпеки ми пропонуємо наступний орієнтовний набір курсів для піврічної програми підвищення кваліфікації:

1. Основи кібербезпеки:
– принципи та концепції кібербезпеки;
– політики безпеки, моделі та фреймворки;
– управління ризиками та оцінка загроз;
– юридичні та етичні аспекти кібербезпеки.
2. Безпека мережі:
– протоколи та технології мережевої безпеки;
– брандмауери, IDS/IPS і VPN;
– моніторинг мережі та реагування на інциденти;
– захист безпроводових мереж.
3. Захищені системи та програмне забезпечення:
– практики безпечної розробки програмного забезпечення;
– методи безпечного кодування;
– тестування безпеки та оцінка вразливостей;
– безпечна конфігурація та захист системи.
4. Криптографія та захист даних:
– основи криптографії;
– інфраструктура відкритих ключів ‘public key infrastructure’ (PKI);
– алгоритми та протоколи шифрування
– механізми конфіденційності та захисту даних
5. Управління ідентифікацією та доступом:
– методи автентифікації та авторизації;
– єдиний вхід ‘single sign-on’ (SSO) і багатофакторна автентифікація ‘multi-factor authentication’ (MFA);
– контроль доступу на основі ролей ‘role-based access control’ (RBAC).
6. Реагування на інциденти та цифрова криміналістика:
– стратегії виявлення *інцидентів* і реагування;
– локалізація та ліквідація інциденту;
– інструменти та методи цифрової криміналістики;
– ланцюг постачання та збереження доказів.
7. Хмарна безпека:
– Моделі безпеки хмарних обчислень;
– Засоби безпеки постачальника хмарних послуг;
– Захист хмарних програм і даних;
– Хмарне управління та дотримання вимог.
8. Безпека IoT та промислової системи управління ‘industrial control system’ (ICS):
– проблеми безпеки в середовищах IoT та ICS;
– захист пристроїв і комунікацій IoT;
– протоколи безпеки ICS і найкращі практики.
9. Тестування на проникнення та етичне хакерство:
– методології тестування на проникнення;
– оцінка вразливості та використання;
– техніки та інструменти етичного хакерства;
– звітування та усунення знахідок.

10. Безпечне управління IT та відповідність:
– структури управління IT (COBIT [28], NIST [29], ISO [30]);
– відповідність нормативним вимогам (GDPR [31], HIPAA [32], PCI DSS [33]);
– аудит безпеки та забезпечення;
– розробка та впровадження політики безпеки.
11. Управління кібербезпекою:
– управління та стратегія програми безпеки;
– управління ризиками на організаційному рівні;
– бюджет безпеки та розподіл ресурсів;
– планування та координація реагування на інциденти.
12. Практичний проект або стажування для застосування знань і навичок, отриманих під час програми, у реальному контексті.

На однорічну перекваліфікацію в середньому припадає 60 кредитів. Але часто стає потреба в доборі окремих курсів для покриття академічної різниці при вступі, наприклад, до аспірантури або ад'юнктури за спеціальністю 125 «Кібербезпека» [34]. Орієнтовне навантаження приведене в табл. 2 для систем нарахування кредитів: European Credit Transfer and Accumulation System (ECTS), University Credit Transfer System (UCTS) та US Credit System (USCS). Повний обсяг дисциплін допоможе на рік перепрофілювати спеціалістів з суміжних галузей, наприклад, інформаційних технологій, розробки програмного забезпечення, електронних систем або телекомунікацій.

Таблиця 2

Розподіл ECTS, UCTS та USCS кредитів за дисциплінами

№	Дисципліна	Кількість кредитів		
		ECTS	UCTS	USCS
1	Основи кібербезпеки	2	2	1
2	Безпека мережі	6	6	3
3	Захищені системи та програмне забезпечення	4	4	2
4	Криптографія та захист даних	8	8	4
5	Управління ідентифікацією та доступом	4	4	2
6	Реагування на інциденти та цифрова криміналістика	6	6	3
7	Хмарна безпека	4	4	2
8	Безпека IoT та промислової системи управління	4	4	2
9	Тестування на проникнення та етичне хакерство	4	4	2
10	Безпечне управління IT та відповідність	4	4	2
11	Управління кібербезпекою	4	4	2
12	Практичний проект або стажування	10	10	5
	Разом:	60	60	30

Для гармонізації поточних освітніх програм є сенс адаптувати представлені навчальні курси до компетенцій, запропоновані стандартом для другого (магістерського) рівня зі спеціальності 125 «Кібербезпека» [34]. Результати співставлення наведені в табл. 3.

ISSN 2663 - 4023

Таблиця 3

Гармонізація програми перепідготовки до компетенцій другого рівня програми 125 «Кібербезпека»

Шифр	**Компетенція**	**№**	**Дисципліни, які покривають компетенції**
КЗ-1	Застосовувати знання у **практичних** ситуаціях	1	Основи кібербезпеки
		12	Практичний проект або стажування
КЗ-2	Проводити **дослідження** на відповідному рівні	6	Реагування на інциденти та цифрова криміналістика
		9	Тестування на проникнення та етичне хакерство
КЗ-3	**Абстрактне мислення**, **аналіз** та **синтез**	6	Реагування на інциденти та цифрова криміналістика
		9	Тестування на проникнення та етичне хакерство
КЗ-4	Оцінювати та забезпечувати **якість** виконуваних **робіт**	3	Захищені системи та програмне забезпечення
		11	Управління кібербезпекою
КЗ-5	Спілкуватися з представниками інших **професійних груп** різного рівня	8	Безпека IoT та промислової системи управління
		12	Практичний проект або стажування
КФ-1	Обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати **сучасні інформаційні технології**, фізичні та математичні моделі, а також технології створення та використання **прикладного** і **спеціалізованого програмного забезпечення** для вирішення професійних задач у сфері ІБ та/або кібербезпеки	3	Захищені системи та програмне забезпечення
		5	Управління ідентифікацією та доступом
		7	Хмарна безпека
КФ-2	Розробляти, впроваджувати та аналізувати **нормативні документи**, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати **кращі світові практики**, **стандарти** у професійній діяльності в сфері ІБ та/або кібербезпеки	10	Безпечне управління ІТ та відповідність
КФ-3	Досліджувати, розробляти і супроводжувати методи та засоби ІБ та/або кібербезпеки на **об'єктах інформаційної діяльності** та **критичної інфраструктури**	6	Реагування на інциденти та цифрова криміналістика
КФ-4	Аналізувати, розробляти і супроводжувати **систему управління ІБ** та/або кібербезпекою організації, формувати стратегію і **політики ІБ** з урахуванням вітчизняних і міжнародних стандартів та вимог	11	Управління кібербезпекою
КФ-5	Дослідження, системний аналіз та забезпечення **безперервності бізнес/операційних процесів** з метою визначення вразливостей інформаційних систем та ресурсів, **аналізу ризиків** та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики ІБ та/або кібербезпеки організації	10	Безпечне управління ІТ та відповідність
		11	Управління кібербезпекою

КФ-6	Аналізувати, контролювати та забезпечувати **систему управління доступом** до інформаційних ресурсів згідно встановленої стратегії і політики ІБ та/або кібербезпеки організації	2	Безпека мережі
		5	Управління ідентифікацією та доступом
КФ-7	Досліджувати, розробляти та впроваджувати методи і заходи **протидії кіберінцидентам**, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо **попередження** та **аналізу кіберінцидентів** в цілому	6	Реагування на інциденти та цифрова криміналістика
КФ-8	Досліджувати, розробляти, впроваджувати та супроводжувати методи і **засоби криптографічного та технічного захисту** інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики ІБ та/або кібербезпеки організації	4	Криптографія та захист даних
КФ-9	Аналізувати, розробляти і супроводжувати систему **аудиту** та **моніторингу ефективності функціонування** інформаційних систем і технологій, бізнес/операційних процесів в галузі ІБ та/або кібербезпеки організації в цілому	10	Безпечне управління ІТ та відповідність
КФ-10	Провадити **науково-педагогічну діяльність**, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань ІБ та/або кібербезпеки	1	Основи кібербезпеки
		11	Управління кібербезпекою
КФ-11	Здійснювати **наукові** та/або **прикладні дослідження** у галузі ІБ та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність	12	Практичний проект або стажування

Курси до компетенцій «Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity», запропоновані міжнародними оргацізаціями Association for Computing Machinery, IEEE Computer Society та ін. [23], [35], також практично повністю покриваються стандартом за спеціальністю 125 «Кібербезпека» [34], [36] (див. табл. 4).

Таблиця 4

Відповідність міжнародного програми Cybersecurity Curricula компетенціям

Курс	**Навички по курсу**	**Компетенція**
Безпека даних	Основні поняття криптографії	КФ-8
	Цифрова криміналістика	КФ-7
	Наскрізний безпечний зв'язок	КФ-3
	Цілісність даних і аутентифікація	КФ-6
	Безпека зберігання інформації	КФ-6
Безпека програмного забезпечення	Основні принципи дизайну: привілеї, відкритий дизайн і абстракція	КЗ-3
	Вимоги безпеки та їх роль у проектуванні	КЗ-4
	Проблеми реалізації	КФ-1
	Статичні та динамічні випробування	КЗ-2
	Налаштування та виправлення	КЗ-1
	Етика в розробці, тестуванні та розкритті вразливостей	КФ-10
Безпека компонентів	Уразливості компонентів системи	КФ-11
	Життєвий цикл компонентів	КФ-5
	Принципи проектування безпечних компонентів	КФ-1
	Безпека управління ланцюгом поставок	КЗ-5

	Тестування безпеки	КЗ-2
	Зворотне проектування	КФ-1
Безпека підключення	Системи, архітектура, моделі та стандарти	КФ-11
	Інтерфейси фізичних компонентів	КФ-8
	Інтерфейси програмних компонентів	КФ-1
	Атаки на підключення	КЗ-1
	Трансмісійні атаки	—
Безпека системи	Холістичний підхід	КЗ-4
	Політика безпеки	КФ-4
	Автентифікація	КФ-6
	Управління доступом	КФ-4
	Моніторинг	КФ-9
	Відновлення	КФ-7
	Тестування	КЗ-2
	Документація	КФ-2
Безпека людини	Управління ідентифікацією	КФ-6
	Соціальна інженерія	—
	Усвідомлення і розуміння	КЗ-3
	Конфіденційність і безпека соціальної поведінки	КФ-6
	Конфіденційність і безпека персональних даних	КФ-6
Організаційна безпека	Управління ризиками	КФ-5
	Управління та політика	КФ-4
	Закони, етика та комплаєнс	КФ-2
	Стратегія та планування	КФ-9
Соціальна безпека	Кіберзлочинність	КФ-7
	Кібернетичне право	КФ-2
	Кіберетика	КФ-10
	Кіберполітика	КЗ-5
	Конфіденційність	КФ-6

З порівняння видно, що поточний стандарт практично повністю покриває вимоги, наприклад, на соціальній інженерії побудована значна кількість сучасних атак [37]. Також слід зазначити, що в міжнародній рекомендації до курсів приведений новий термін «трансмісійні атаки ‘transmission attacks’», для якого відсутня відповідність в місцевому стандарті.

Рекомендації для формування політики безпеки для держаних установ

Політика безпеки державних інформаційних систем повинна бути комплексною та адаптованою до конкретних потреб і вимог урядової організації. Хоча конкретні елементи можуть відрізнятися, надійна політика безпеки, як правило, включає наступні ключові елементи:

1. Чітко визначте загальні *цілі політики безпеки та сферу її застосування*, включаючи системи та дані, на які вона поширюється.

2. Окресліть *ролі та обов’язки* різних зацікавлених сторін, включаючи системних адміністраторів, власників даних, працівників служби безпеки та кінцевих користувачів.

3. Опишіть процес виявлення, оцінки та *управління ризиками* кібербезпеки для державних інформаційних систем.

4. Створити систему *управління безпекою*, включаючи залучення керівних і директивних органів до питань безпеки.

5. Визначте схему *класифікації інформаційних активів* на основі їхньої чутливості та встановіть інструкції для роботи з кожним рівнем класифікації.

6. Сформуйте підходи до *контролю доступу та автентифікації*: визначте правила надання та відкликання доступу до інформаційних систем і даних, а також необхідні механізми автентифікації.

7. Розгляньте питання захисту конфіденційних даних, дотримання *правил конфіденційності* та процедур обробки даних.

8. Окресліть заходи з підвищення *обізнаності працівників* щодо безпеки та проведіть тренінги з реагування на інциденти, пов'язані з безпекою.

9. Впровадити процедури виявлення інцидентів та порушень безпеки, *реагування* на них і *звітування* про них.

10. Встановіть рекомендації щодо *захисту мережевої інфраструктури* організації, включаючи брандмауери, системи виявлення/запобігання вторгненням та шифрування.

11. Визначте процес *безпечної конфігурації* та підтримки інформаційних систем, включно з регулярними виправленнями та оновленнями.

12. Розробити рекомендації щодо регулярного *резервного копіювання даних* та плану аварійного відновлення для забезпечення безперервності бізнесу. Розробіть комплексний план забезпечення *безперервності бізнесу* на випадок інцидентів або катастроф у сфері кібербезпеки, а також процедуру та аварійного відновлення.

13. Оцініть та уніфікуйте процедуру управління ризиками безпеки, пов’язаними зі *сторонніми* постачальниками та постачальниками послуг.

14. Запровадьте процедури *аудиту та моніторингу* ефективності засобів контролю та політик безпеки.

15. Забезпечте чіткий процес ескалації для *повідомлення про інциденти безпеки* та їх вирішення відповідними органами влади.

16. Визначте вимоги до регулярних оцінок безпеки, *тестування вразливостей* і проникнення.

17. Розгляньте заходи безпеки для *захисту фізичних активів*, таких як центри обробки даних, сервери та точки доступу.

18. Переконайтеся, що політика узгоджується з відповідними законами, нормативними актами та галузевими стандартами.

19. Зобов’язуйтесь постійно оцінювати та *вдосконалювати політику безпеки* з урахуванням нових загроз та змін у технологіях. Політика безпеки повинна регулярно переглядатися та оновлюватися, щоб адаптуватися до нових загроз та мінливих обставин. Крім того, вона має бути чітко доведена до відома всіх зацікавлених сторін і послідовно застосовуватися в усіх державних інформаційних системах для підтримання сильної позиції безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті проаналізовані підходи до відслідковування існуючих загроз та методи протидій ним. В якості джерел даних можуть виступати міжнародні та національні організації та асоціацію. Результати з різних звітів агрегуються в залежності від галузі роботи певної організації та її форми власності. Розгляд механік переходу вразливостей в інциденти безпеки дозволяє створювати формалізовані моделі для систем аудиту та розбору виявлених інцидентів або відслідковування в реальному часі. Одним з основних критеріїв є оцінка ризиків кібербезпеки. В публікації запропонований метод, який враховує взаємозв’язок компонентів системи та дозволяє враховувати послідовність задіяності даних компонентів.

В якості міжнародного та національного досвіду розглянуті джерела оперативної та звітної інформації про інциденти безпеки. В результаті запропоновані заходи по зменшенню ризику використання існуючих вразливостей для державних інформаційних мереж та систем. Що не єдиний метод якісного переходу по зменшенню збитків від кіберінцидентів полягає в підвищенні якості фахівців з кібернетичної безпеки, тому в статті запропонований нова програма перепідготовки фахівців із суміжних галузей: інформаційних технологій, телекомунікацій, електроніки, радіотехніки, програмування тощо.

В результаті даного дослідження видно, що формування політики безпеки для держаних установ має враховувати також економічний вплив та ймовірні збитки від кібернетичних атак.

Подальші дослідження спрямовані на валідацію запропонованих рекомендацій щодо формування політики безпеки для держаних та комерційних установ та організацій.

ПОДЯКА

Автор даної публікації висловлює подяку Володимиру Леонідовичу Бурячку, завідувачу кафедри інформаційної та кібернетичної безпеки (Державний університет телекомунікацій та Київський університет імені Бориса Грінченка), який був безпосереднім керівником і впроваджувачем інноваційних методів в навчанні, а також активно надихав і залучав студентів до наукової роботи [38] – [42].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Kuzminykh, I., et al. (2021). Information Security Risk Assessment. *Encyclopedia, 1(3),* 602–617. https://doi.org/10.3390/encyclopedia1030050

2 Bebeshko, B., et al. (2022). Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency. *Journal of Theoretical and Applied Information Technology*, *100(24)*, 7390–7404.

3 Buriachok, V., Sokolov, V., Skladannyi, P. (2019). Security Rating Metrics for Distributed Wireless Systems. In *8th International Conference on "Mathematics. Information Technologies. Education," vol. 2386*, 222–233.

4 Гулаг, Г., *та ін.* (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка, 1(17)*, 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158

5 Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In *Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2)*, 197–206.

6 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Сучасний захист інформації*, *1*, 82–89.

7 Grechaninov, V., et al. (2022). Models and Methods for Determining Application Performance Estimates in Distributed Structures. In *Cybersecurity Providing in Information and Telecommunication Systems, 3288(1)*, 134–141.

8 Sokolov, V., Skladannyi, P., Hulak, H. (2022). Stability Verification of Self Organized Wireless Networks with Block Encryption. In *Cybersecurity Providing in Information and Telecommunication Systems, 3137*, 227–237.

9 Киричок, Р., *та ін.* (2021). Правила реалізації експлойтів під час активного аналізу захищеності корпоративних мереж на основі нечіткої оцінки якості механізму валідації вразливостей. *Кібербезпека: освіта, наука, техніка, 2(14)*, 148–157. https://doi.org/10.28925/2663-4023.2021.14.148157

10 Гулаг, Г., *та ін.* (2020). Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. *Кібербезпека: освіта, наука, техніка, 2(10)*, 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
11 Kyrychok, R., et al. (2016). Problems of Ensuring Security Control of Corporate Networks and Ways to Solve Them. *Scientific Records of the Ukrainian Research Institute of Communications, (3)*, 48–61.
12 Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Emerging Technology Trends on the Smart Industry and the Internet of Things*, *3149*, 107–117.
13 Рой, Я., Мазур, Н., Складанний, П. (2018). Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка, 1(1)*, 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693
14 Соколов, В., Курбанмурадов Д. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616
15 Thiel, F., et al. (2015). Cloud Computing in Legal Metrology. In 17th International Congress of Metrology. EDP Sciences. https://doi.org/10.1051/metrology/20150016001
16 International Organization for Standardization (2023). ISO/IEC 15408-1:2022. nformation security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1: Introduction and general model. https://www.iso.org/standard/72891.html
17 Verizon (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/T18a/reports/2023-data-breach-investigations-report-dbir.pdf
18 National Security Agency (2022). Network Infrastructure Security Guide. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/ctr_nsa_network_infrastructure_security_guide_20220615.PDF
19 Cybersecurity Infrastructure Security Agency (2023). Identity and Access Management: Recommended Best Practices for Administrators. https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/esf%20identity%20and%20access%20management%20recommended%20best%20practices%20for%20administrators%20pp-23-0248_508C.PDF
20 NortonLifeLock (2022). Cyber Safety Insights Report. Global Results. https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2022_NLCSIR_Global_Report.pdf
21 CrowdStrike (2023). Global Threat Report. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf
22 CompTIA (2019). Security+. Certification Exam Objectives. No. SY0-601, ver. 3.0. https://www.comptia.jp/pdf/CompTIA%20Security+%20SY0-601%20Exam%20Objectives%20(3.0).pdf
23 Joint Task Force on Cybersecurity Education (2018). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
24 European Union Agency for Cybersecurity (2022). European cybersecurity skills framework (ECSF): User Manual. https://doi.org/10.2824/95989
25 International Organization for Standardization (2023). ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security. https://www.iso.org/standard/76070.html
26 Sisler, J. (2019). CISSP Study Guide. Certification Training. Datasage. https://isc2rduchapter.org/wp-content/uploads/2019/02/CISSP.pdf
27 Newhouse, W., et al. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-181
28 Lepofsky, R. (2014). COBIT 5 for Information Security. In: The Manager's Guide to Web Application Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-0148-0_10
29 National Institute of Standards and Technology (2023). Discussion Draft of the NIST Cybersecurity Framework 2.0 Core https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
30 International Organization for Standardization (2020). ISO/IEC 19788-1:2011. Information Technology. Learning, Education and Training. Metadata for Learning Resources. Part 1: Framework. https://www.iso.org/standard/50772.html

31 The European Parliament and of the Council (2018). Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

32 U.S. Department of Health and Human Services Office for Civil Rights (2013). HIPAA Administrative Simplification. Regulation Text. 45 CFR Parts 160, 162, and 164. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

33 PCI Security Standards Council (2022). PCI DSS, ver. 4.0. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

34 Міністерство освіти і науки України (2021). Стандарт вищої освіти України. Другий (магістерський) рівень. 12 Інформаційні технології. 125 Кібербезпека, Наказ №332 від 18.03.2021 р. https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx

35 Tang, C. (2020). ACM CYBER2YR2020 Curriculum Guidelines. Innovations in Cybersecurity Education National CyberWatch Center, 44. https://www.nationalcyberwatch.org/wp-content/uploads/2020/04/NCC_2020_Innovations_Booklet_Online.pdf

36 Соколов, В., Складанний, П. (2023). Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». *Кібербезпека: освіта, наука, техніка, 4(20)*, 183–204. https://doi.org/10.28925/2663-4023.2023.20.182203

37 Соколов, В. (2022). Підходи до формування наукового мислення у здобувачів вищої освіти з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, *2*(*18*), 124–137. https://doi.org/10.28925/2663-4023.2022.18.124137

38 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57

39 Buriachok, V, *et al.* (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. *Lecture Notes on Data Engineering and Communications Technologie*, *178*, 533–551. https://doi.org/10.1007/978-3-031-35467-0_32

40 Бурячок, В., Шевченко, С., Складанний, П. (2018). Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. *Кібербезпека: освіта, наука, техніка*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104

41 Бурячок, В., *та ін.* (2021). Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень*: Кібербезпека: освіта, наука, техніка*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Volodymyr Y. Sokolov
Ph.D., associate professor
associate professor of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Pavlo M. Skladannyi
Ph.D., associate professor
head of Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

METHODOLOGY FOR ASSESSING COMPREHENSIVE DAMAGES FROM AN INFORMATION SECURITY INCIDENT

Abstract. Security incidents can have significant economic consequences for public authorities. To mitigate the economic impact of cybersecurity incidents, public authorities must invest in robust countermeasures, and collaboration with other government agencies, private sector partners, and international organizations can help increase resilience and response capacity to cyber attacks. The article uses the analysis of various vulnerabilities and the mechanism of transformation into a security incident, as well as analyzed approaches to monitoring existing threats and methods of countering them. International and national organizations and associations can act as data sources. Results from various reports are aggregated depending on the field of work of a certain organization and its form of ownership. Consideration of the mechanics of the transition of vulnerabilities into security incidents allows the creation of formalized models for audit systems and analysis of detected incidents or real-time monitoring. One of the main criteria is the assessment of cyber security risks. The publication proposes a method that takes into account the interrelationship of system components and allows taking into account the sequence of engagement of these components. Sources of operational and reporting information on security incidents are considered as international and national experiences. As a result, measures are proposed to reduce the risk of using existing vulnerabilities for state information networks and systems. Since the only method of qualitative transition to reduce losses from cyber incidents is to improve the quality of cyber security specialists, the article proposes a new retraining program for specialists from related fields: information technology, telecommunications, electronics, radio engineering, programming, etc. As a result of this study, it can be seen that the formation of security policy for state institutions should also take into account the economic impact and probable losses from cyber attacks. Further research is aimed at validating the proposed recommendations for the formation of security policy for state and commercial institutions and organizations.

Keywords: cyber security; information protection; vulnerability; risk; security incident.

REFERENCES

1 Kuzminykh, I., et al. (2021). Information Security Risk Assessment. *Encyclopedia, 1(3)*, 602–617. https://doi.org/10.3390/encyclopedia1030050

2 Bebeshko, B., et al. (2022). Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency. *Journal of Theoretical and Applied Information Technology*, *100(24)*, 7390–7404.

3 Buriachok, V., Sokolov, V., Skladannyi, P. (2019). Security Rating Metrics for Distributed Wireless Systems. In *8th International Conference on "Mathematics. Information Technologies. Education," vol. 2386*, 222–233.

4 Hulak, H., et al. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Cybersecurity: Education, Science, Technique, 1(17)*, 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158

5 Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In *Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2)*, 197–206.

6 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Modern Information Protection, 1*, 82–89.

7 Grechaninov, V., et al. (2022). Models and Methods for Determining Application Performance Estimates in Distributed Structures. In *Cybersecurity Providing in Information and Telecommunication Systems, 3288(1)*, 134–141.

8 Sokolov, V., Skladannyi, P., Hulak, H. (2022). Stability Verification of Self Organized Wireless Networks with Block Encryption. In *Cybersecurity Providing in Information and Telecommunication Systems, 3137*, 227–237.

9 Kyrychok, R., et al. (2021). Rules for the Implementation of Exploits during an Active Analysis of the Corporate Networks' Security based on a Fuzzy Assessment of the Quality of the Vulnerability Validation Mechanism. *Cybersecurity: Education, Science, Technique, 2(14)*, 148–157. https://doi.org/10.28925/2663-4023.2021.14.148157

10 Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Cybersecurity: Education, Science, Technique, 2(10)*, 6–28. https://doi.org/10.28925/2663-4023.2020.10.628

11 Kyrychok, R., et al. (2016). Problems of Ensuring Security Control of Corporate Networks and Ways to Solve Them. *Scientific Records of the Ukrainian Research Institute of Communications, 3*, 48–61.

12 Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149*, 107–117.

13 Roy, Y., Mazur, N., Skladannyi, P. (2018). Audit of Information Security Is the basis of Effective Protection of the Enterprise. *Cybersecurity: Education, Science, Technique, 1(1)*, 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693

14 Sokolov, V., Kurbanmuradov D. (2018). The Method of Combating Social Engineering at the Objects of Information Activity. *Cybersecurity: Education, Science, Technique, 1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

15 Thiel, F., et al. (2015). Cloud Computing in Legal Metrology. In 17th International Congress of Metrology. EDP Sciences. https://doi.org/10.1051/metrology/20150016001

16 International Organization for Standardization (2023). ISO/IEC 15408-1:2022. nformation security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1: Introduction and general model. https://www.iso.org/standard/72891.html

17 Verizon (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/T18a/reports/2023-data-breach-investigations-report-dbir.pdf

18 National Security Agency (2022). Network Infrastructure Security Guide. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/ctr_nsa_network_infrastructure_security_guide_20220615.PDF

19 Cybersecurity Infrastructure Security Agency (2023). Identity and Access Management: Recommended Best Practices for Administrators. https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/esf%20identity%20and%20access%20management%20recommended%20best%20practices%20for%20administrators%20pp-23-0248_508c.pdf

20 NortonLifeLock (2022). Cyber Safety Insights Report. Global Results. https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2022_NLCSIR_Global_Report.pdf

21 CrowdStrike (2023). Global Threat Report. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf

22 CompTIA (2019). Security+. Certification Exam Objectives. No. SY0-601, ver. 3.0. https://www.comptia.jp/pdf/CompTIA%20Security+%20SY0-601%20Exam%20Objectives%20(3.0).pdf

23 Joint Task Force on Cybersecurity Education (2018). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

24 European Union Agency for Cybersecurity (2022). European cybersecurity skills framework (ECSF): User Manual. https://doi.org/10.2824/95989
25 International Organization for Standardization (2023). ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security. https://www.iso.org/standard/76070.html
26 Sisler, J. (2019). CISSP Study Guide. Certification Training. Datasage. https://isc2rduchapter.org/wp-content/uploads/2019/02/CISSP.pdf
27 Newhouse, W., et al. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-181
28 Lepofsky, R. (2014). COBIT 5 for Information Security. In: The Manager's Guide to Web Application Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-0148-0_10
29 National Institute of Standards and Technology (2023). Discussion Draft of the NIST Cybersecurity Framework 2.0 Core https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
30 International Organization for Standardization (2020). ISO/IEC 19788-1:2011. Information Technology. Learning, Education and Training. Metadata for Learning Resources. Part 1: Framework. https://www.iso.org/standard/50772.html
31 The European Parliament and of the Council (2018). Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
32 U.S. Department of Health and Human Services Office for Civil Rights (2013). HIPAA Administrative Simplification. Regulation Text. 45 CFR Parts 160, 162, and 164. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
33 PCI Security Standards Council (2022). PCI DSS, ver. 4.0. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
34 Ministry of Education and Science of Ukraine (2021). Standard of Higher Education of Ukraine. Second (Master's) Level. 12 Information Technologies. 125 Cybersecurity, No. 332 dated March 18, 2021 https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx
35 Tang, C. (2020). ACM CYBER2YR2020 Curriculum Guidelines. Innovations in Cybersecurity Education National CyberWatch Center, 44. https://www.nationalcyberwatch.org/wp-content/uploads/2020/04/NCC_2020_Innovations_Booklet_Online.pdf
36 Sokolov, V., Skladannyi, P. (2023). Comparative Analysis of Strategies for Building Second and Third Level of 125 "Cyber Security" Educational Programs. *Cybersecurity: Education, Science, Technique, 4(20)*, 183–204. https://doi.org/10.28925/2663-4023.2023.20.182203
37 Sokolov, V. (2022). Approaches to the Formation of Scientific Thinking in Cybersecurity High School Students. *Cybersecurity: Education, Science, Technique*, *2*(*18*), 124–137. https://doi.org/10.28925/2663-4023.2022.18.124137
38 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57
39 Buriachok, V, *et al.* (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. *Lecture Notes on Data Engineering and Communications Technologie, 178*, 533–551. https://doi.org/10.1007/978-3-031-35467-0_32
40 Buriachok, V., Shevchenko, S., Skladannyi, P. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104
41 Buriachok, V., *et al.* (2021). Interdisciplinary Approach to the Development of Risk Management Skills on the basis of Decision-Making Theory. *Cybersecurity: Education, Science, Technique*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License
.