КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.159171
УДК [005.53 + 519.816] : 004.056.52

Автушенко Олександр Семенович
кандидат педагогічних наук, доцент, доцент кафедри
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0003-0910-7552
avtushenko_a@ukr.net

Гирда Віра Анатоліївна
старший інженер
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0002-3858-4086
gidraponka@ukr.net

Кожедуб Юлія Василівна
кандидат технічних наук, старший науковий співробітник
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0001-6181-5519
JuliaKozhedub@email.ua

Максимець Андрій Володимирович
старший інженер
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0003-3551-0628
andy.west.corp@gmail.com

АНАЛІЗ МЕТОДІВ, СПОСОБІВ, МЕХАНІЗМІВ, ІНСТРУМЕНТІВ ТЕОРІЇ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. У статті подано розгорнутий аналіз методів, способів, механізмів, інструментів теорії прийняття рішень для моделювання систем захисту інформації. Наведено основні термінологічні поняття і надано їх розгорнуте визначення. Показано поєднання елементів теорії прийняття рішень з системами захисту інформації. Сполучною ланкою для цього слугує теорія ймовірностей. Досліджено питання процедури прийняття рішення як процесу. Закцентовано увагу на якісних параметрах процедури прийняття рішення, що можуть бути придатними для цілей захисту інформації. Зроблено аналогії, що вказують на застосовність методів теорії прийняття рішення для створення моделі системи захисту інформації. Механізми реалізації показано на алгоритмах прийняття рішення. За допомогою інструментів теорії прийняття рішення встановлено, що на їх основі можна формалізувати, як математичними піктограмами, так і вербалізацією, процес моделювання. Загалом змальовано поетапний процес проєктування системи захисту інформації. Зроблено висновки, що формалізація як вид знакового моделювання одночасно з застосуванням теорії прийняття рішення – найкращий варіант для описової частини системи захисту інформації. З'ясовано, що моделювання є найкращим науковим інструментом для поєднання теоретичних викладок і практичного застосунку широкого кола питань наукових досліджень і зокрема сфери захисту інформації. Для підтримки прийняття рішень особою, яка приймає рішення, інакше кажучи децидентом, в сфері захисту інформації важливо, що офіцер з безпеки або системний адміністратор мав досвід і навички щодо регламентованих дій. Такі дії – це як відомі напрацювання в цій сфері діяльності, так і синтез уже відомих алгоритмів для досягнення

стану захищеності інформації загалом. Автоматизація в діяльності особи, яка приймає рішення можлива через впровадження системи підтримки прийняття рішень, що широко поширювані в автоматизованих системах: комп'ютерних системах і мережах, особливо там де є потреба аналізувати значні потоки даних.

Ключові слова: захист інформації; моделювання; модель системи захисту інформації; процес прийняття рішень; системи підтримки прийняття рішень; теорія прийняття рішень.

ВСТУП

Теорія прийняття рішень − область дослідження, в якій використовують поняття і методи математики, статистики, економіки, менеджменту, психології; вона вивчає закономірності вибору людьми шляхів вирішення різного роду завдань, а також досліджує способи пошуку найбільш вигідних з можливих рішень.

Теорію прийняття рішень (ТПР) застосовують для аналізу тих проблем, які можна відносно легко й однозначно формалізувати, а результати досліджень – адекватно інтерпретувати. Методи ТПР використовують у різних галузях управління: проектуванні складних технічних і організаційних систем, плануванні, організації та розвитку процесів економіки тощо. Застосування засобів і методів ТПР спричинено швидким розвитком і ускладненням зв'язків, пошуком залежності між процесами та явищами, які раніше здавались не пов'язаними один з одним. Витрати на прийняття ефективних рішень зростають, наслідки помилок стають усе серйознішими, а звернення до досвіду та інтуїції фахівців не завжди зумовлює вибір найкращої стратегії. Застосування методів ТПР дає змогу розв'язати цю проблему швидко та достатньо точно й ефективно.

Постановка проблеми. Теорія прийняття рішень − область дослідження, в якій використовують поняття і методи математики, статистики, економіки, менеджменту, психології; вона вивчає закономірності вибору людьми шляхів вирішення різного роду завдань, а також досліджує способи пошуку найбільш вигідних з можливих рішень.

Теорію прийняття рішень (ТПР) застосовують для аналізу тих проблем, які можна відносно легко й однозначно формалізувати, а результати досліджень – адекватно інтерпретувати. Методи ТПР використовують у різних галузях управління: проектуванні складних технічних і організаційних систем, плануванні, організації та розвитку процесів економіки тощо. Застосування засобів і методів ТПР спричинено швидким розвитком і ускладненням зв'язків, пошуком залежності між процесами та явищами, які раніше здавались не пов'язаними один з одним. Витрати на прийняття ефективних рішень зростають, наслідки помилок стають усе серйознішими, а звернення до досвіду та інтуїції фахівців не завжди зумовлює вибір найкращої стратегії. Застосування методів ТПР дає змогу розв'язати цю проблему швидко та достатньо точно й ефективно.

Аналіз останніх досліджень і публікацій. У [8] запропоновано структуру СППР з управління виробничою логістикою промислового підприємства, яка дає змогу підвищити ефективність функціонування виробничої системи (через скорочення часу для прийняття рішень, засноване на інформації про фактичні запаси, планові простої та втрати), визначити ціну помилки управлінських рішень, щоб уникнути можливості її повторення в майбутньому. Проілюстровано основні аспекти функціонування запропонованої СППР на прикладі процесу конвертерного виробництва сталі на металургійному заводі, наведено докладний опис кожного з представлених у структурі системи блоку. Запропоновано механізм прийняття рішень, який базується на тісній взаємодії між модулем моделювання, базою знань, базами даних, на основі якої формуються рекомендації з переміщення того чи іншого агрегату, задіяного у процесі конвертерного виробництва сталі. Ґрунтуючись на досвіді розробки подібних систем,

запропоновано групову обробку даних, яка передбачає використання персонального інтерфейсу для кожної категорії користувачів, що дасть можливість залучити основних учасників виробничого процесу до прийняття рішень, колективного формулювання нових ідей. Наголошено, що підвищення ефективності функціонування економічних об'єктів можливо, насамперед, за допомогою грамотного застосування та подальшого вдосконалення інформаційних систем (ІС).

У [9] розглянуто переваги застосування операційної системи Android під час розроблення мобільного додатку для підтримки прийняття рішення на основі методу аналізу ієрархій. Наведено приклади розв'язання задач вибору в мобільній версії СППР NooTron.

У [10] розглянуто підхід до вирішення питання затребуваності СППР в е-державі. Виділено два класи ІС – системи оперативної обробки транзакцій та СППР, досліджено їх основні характеристики. Показано необхідність СППР для е-держави. Перераховано основні технології, що використовуються під час розробки СППР для е-держави.

Як видно з наведено, тематика цих статей безпосередньо пов'язана з ТПР. За допомогою цієї теорії можна описати будь-які процеси, зокрема вона є придатною і для моделювання систем захисту.

Мета статті. Основним методом аналізу функціонування СЗІ, як і взагалі складних систем, є створення відповідних моделей. Основне призначення таких моделей полягає в об'єктивній оцінці загального стану функціонування системи з точки зору ступеня вразливості або рівня захищеності інформації в ній. Необхідність в таких оцінках зазвичай виникає під час вироблення рішень щодо покращення організації захисту інформації з можливістю нарощування потужностей захисту і прогнозування анормальних станів (пов'язаних, наприклад, з антропогенними чинниками).

Ідеальна СППР повинна має такі характеристики [3-4]:

– використовує слабкоструктуровані та нечіткі дані;

– оперує зі слабкоструктурованими рішеннями;

– підтримує як взаємозалежні, так і послідовні рішення;

– може застосовувати знання;

– підтримує моделювання та прогнозування;

– може бути легко побудована, якщо може бути сформульована логіка конструкції СППР;

– проста у застосуванні та модифікації;

– підтримує три фази ППР: інтелектуальну частину, проєктування та вибір;

– призначена для децидентів різного рівня;

– може бути адаптована до індивідуального та групового застосування;

– підтримує різні стилі та методи рішень, що можуть бути корисними при застосуванні групою децидентів;

– проявляє гнучкість і адаптується до змін в організації та в її оточенні;

– дозволяє людині керувати ППР за допомогою комп'ютера, а не навпаки;

– підтримує еволюційне застосування та легко адаптується до змінюваних вимог;

– підвищує ефективність ППР.

Метою цієї статті є моделювання СЗІ за допомогою методів, способів, механізмів, інструментів ТПР, а основним завданням цього дослідження є розроблення моделі захисту для науково обґрунтованого процесу створення СЗІ на основі оцінювання ефективності прийнятих рішень і вибору раціонального варіанту технічної реалізації СЗІ з урахуванням оптимального рівня розвитку методології захисту інформації.

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Рішення – результат інтелектуальної діяльності людини, що призводить до певного висновку та/або до необхідних дій. Під час прийняття рішення роблять вибір між альтернативними та, як правило, конкуруючими можливостями. Децидент – особа чи група осіб, які приймають рішення. Завданням прийняття рішення називають таке завдання, яке можна сформулювати в термінах мети, засобів і результату [1].

Рішення поділяють на: організаційні; програмовані; непрограмовані; інтуїтивні; такі, що ґрунтуються на міркуваннях [1, 11]. Міркування за аналогією, як основа організаційного рішення, корисні, тому що багато ситуацій в організаціях повторюються, вони є циклічними. Раціональне рішення не залежить від минулого досвіду, його обґрунтовують у ході об'єктивного аналітичного процесу. Процес вибору рішення має такі структурні елементи: формулювання проблемної ситуації, призначення децидента, встановлення мети виходу з проблемної ситуації, управління (як діяльність спрямована на досягнення мети), описування варіантів рішень, встановлення обмежень, умови, накладені станом зовнішнього середовища.

Нагромаджений практичний досвід щодо прийняття рішень показує, що часто найважчими і найважливішими є питання безпосередньо непов'язані з ППР, вони є скоріше організаційними, а саме [11]:

– уведення експертів і децидента в проблематику задач, які потрібно розв'язати;
– формування спільної мови комунікування для різних груп експертів і децидента;
– узгодження думок і поглядів різних груп експертів і децидента;
– виявлення справжніх цілей розв'язання та постановки задачі.

Будь-яке рішення характеризується поставленою метою і критерієм оптимальності або системою цілей, які повинні містити пріоритетні співвідношення, що показуватимуть відносну інтенсивність досягнення цільових функцій. Альтернативні стратегії, або очікувані варіанти дій дають можливість вибору оптимального рішення серед усіх можливих. Частковим випадком є вибір одиничного рішення при порівнянні дій лише з однією альтернативою [12].

Стан зовнішнього середовища – це сукупність зовнішніх чинників та їх майбутній розвиток, що характеризуються невизначеністю. Часто ця невизначеність пов'язана не зі свідомими діями, а з необізнаністю про середовище, в якому треба приймати рішення.

Чинник часу є невід'ємним атрибутом моделі прийняття рішень, оскільки важливими є не лише терміни вибору оптимального варіанту, а й кількість кроків та етапів цього процесу.

Методи прийняття рішень в умовах невизначеності є універсальними. Найбільш поширеними методами прийняття оптимальних рішень є [13]:

– платіжна матриця – суб'єкт має вирішити, яка стратегія найбільш сприятиме досягненню поставлених цілей. Особливість цього методу – обмежена кількість варіантів стратегії та невизначеність результату;

– метод теорії корисності ґрунтується на припущенні, що якщо переваги людей по відношенню до певних ситуацій задовольняють ряд аксіом, то їх поведінка може розглядатись як максимізація очікуваної корисності;

– метод теорії проспектів – передбачає ймовірнісний кінцевий результат. На жаль, цей метод не вирішує проблем, що виникають під час вивчення поведінки людей в задачах прийняття рішення;

– метод аналізу ієрархій – спирається на багатокритеріальну характеристику проблеми та використовує дерево критеріїв, що показує його наочність.

Евристичні методи поділяють на: метод компенсації (для попарного порівняння

ISSN 2663 - 4023

альтернатив) і метод зваженої суми оцінок критеріїв (для бальної оцінки кожної альтернативи).

Критерії, що їх використовують в умовах невизначеності під час ППР [14]:

1) критерій Вальда (максимін) – вибір альтернативи, яка з усіх несприятливих варіантів розвитку подій набуває найбільшого з мінімальних значень (значення ефективності краще з усіх гірших), застосовують суб'єкти, що не схильні ризикувати;

2) критерій "maximax" (максимакс) – вибір альтернативи, яка з усіх найсприятливіших ситуацій розвитку подій має найбільше з максимальних значень (значення ефективності найкраще), використовують суб'єкти схильні до ризику;

3) критерій Гурвіца (критерій "оптимізму-песимізму" або "альфа-критерій") побудований на взаємодії правил максимакса та максиміна, зв'язуванням максимуму мінімальних значень альтернатив. Оптимальне значення альтернативного рішення за критерієм Гурвіца визначається за формулою:

$$A_i = a * E_{MAXi} + (1 - a) * E_{MINi}\ , \qquad (1)$$

де A_i – середньозважена ефективність за критерієм Гурвіца для конкретної альтернативи;

a – альфа-коефіцієнт, що ідентифікує ризикову перевагу, від 0 до 1 (значення, наближені до 0, характерні для суб'єктів не схильних до ризику; значення, що дорівнює 0,5 – суб'єкти нейтральні до ризику; значення, наближені до 1 – суб'єкти схильні до ризику);

E_{MAXi} – максимальне значення ефективності по конкретній альтернативі;

E_{MINi} – мінімальне значення ефективності по конкретній альтернативі.

Критерій Гурвіца найчастіше використовують суб'єкти, яким необхідно максимально точно ідентифікувати ступінь своїх конкретних ризикових переваг, задаючи значення альфа-коефіцієнта;

4) критерій Севіджа передбачає вибір альтернативи, яка мінімізує величину максимальних втрат по кожному з можливих рішень і використовується суб'єктами, які не схильні до ризику.

Рішення – обґрунтований набір дій децидента, спрямованих на об'єкт чи систему управління, дає можливість привести об'єкт чи систему до бажаного стану чи досягнути поставленої мети. Рішення є одним із видів розумової діяльності і проявом волі людини. Характерними ознаками рішення є [14]:

можливість вибору з набору альтернативних варіантів – за відсутності альтернатив, відсутній і вибір, отже, відсутнє й рішення;

наявність мети – безцільний вибір не розглядається як рішення;

необхідність вольового акту децидента під час вибору рішення, так формується рішення. Класифікацію рішень див. у табл. 1.

Таблиця 1

Класифікація видів рішень

Ознака	Вид рішення		
Ступінь структуризації проблеми	Гарно структуроване	Погано структуроване	Не структуроване
Кількість етапів реалізації рішення	Статичне (один етап)	Динамічне (ітераційний підхід)	
Рівень поінформованості про стан проблеми	Умови визначеності	Умови ризику	Умови невизначеності
Кількість децидентів	Одна особа	Багато осіб	
Зміст рішення	Стратегічне	Тактичне	

Прийняття рішення – це процес вибору найбільш преференційного з множини допустимих рішень або упорядкування множини рішень. Прийняття рішень можливе на підставі знань про управління об'єктом, процеси, що відбуваються, чи можуть відбутись, а також за наявності множини чинників, що характеризують ефективність та якість прийнятого рішення. Модель прийняття рішень – це формальне подання поставленої задачі та ППР. Питання про формальну основу вибору, зокрема, про походження критерію оптимальності складає одну з фундаментальних проблем ТПР.

Є два основних параметри, що впливають на ефективність рішення: фактор якості рішення Q та фактор прийняття рішення людиною A. Ефективність рішення E може бути виражено формулою:

$$E \ \ Q * A. \qquad (2)$$

За умов, що один із зазначених факторів прямує до мінімуму, ефективність рішення зменшується. Фактор якості рішення Q пов'язаний із вибором кращої альтернативи з тих, що зумовлює проблемна ситуація з урахуванням умов прийняття рішень та можливостей виконавців рішення. Підвищення ефективності рішення головним чином слід спрямовувати на покращення фактору якості: підбір обмежень і критеріїв рішення, правильне формування множини допустимих альтернатив та на коректний вибір найкращого для умов задачі варіанту.

Під ППР розуміють послідовність процедур, що призводить до знаходження рішення. Він складається з таких основних етапів [5]: Виявлення проблемної ситуації; Постановка задачі прийняття рішення; Формулювання вимог до якості прийнятого рішення; Структуризація рішення до рівня критеріїв; Описування характеристик зовнішнього середовища; Прогнозування можливих результатів дії ППР із подальшим виявленням або конструюванням альтернативних варіантів рішень; Оцінювання якості варіантів рішень, порівняння їх між собою та вибір одного чи декількох найвідповідніших меті; Аналізування рішень, опрацювання плану реалізації та впровадження рішення.

Потреба у виділенні окремих етапів, що деталізує ППР, і їх контекст залежить від характеру проблеми, що розв'язується [5]: Виявлення й описання проблемної ситуації; Постановка задачі; Формулювання та структуризація мети вирішення проблемної ситуації; Виявлення та/чи розроблення альтернатив щодо досягнення цілі; Описування можливих станів та впливних дій зовнішнього середовища; Оцінювання можливості

виникнення конкретних станів зовнішнього середовища; Виявлення можливих результатів дій; Вибір критеріїв оцінювання відповідності результатів дій поставленій меті; Оцінювання очікуваного ефекту дій; Описування й оцінювання результатів реалізації альтернатив у конкретних умовах зовнішнього середовища; Порівняння окремих альтернатив за очікуваними ефектами дій (реалізаціями) і вибір найкращої; Прийняття рішень, тобто затвердження плану вирішення проблемної ситуації і його впровадження.

Зазвичай доводиться приймати рішення за умов, коли є невизначеності різних типів: розрізняють перспективну невизначеність (виникають непередбачені чинники) та ретроспективну (через нестачу інформації). Для ретроспективної невизначеності можливі три варіанти: інформацію можна відновити; можна замінити перспективною; не можна ні відновити, ні замінити.

Задачу прийняття рішення за умов невизначеності аналізують у такій послідовності:

1. Складають перелік доступних можливостей джерел інформації, проводять експерименти і виконують дії.
2. Складають перелік подій, які, скоріше за все, можуть трапитись.
3. Визначають послідовність виконуваних дій.
4. Вирішують, наскільки влаштовують наслідки різних дій.
5. Оцінюють кожну конкретну невизначеність події.

Досягнення в сфері захисту інформації не знімають потреби участі людини в технологічних процесах – потрібні люди, щоб аналізувати причини та наслідки інцидентів, робити висновки та підвищувати ефективність роботи засобів захисту. Люди є найціннішим активом у цій галузі діяльності: досвід, навички, креативність, – те що робить їх роботу по-справжньому ефективною [15].

У відомій концепції захисту інформації, запропонованій Hewlett Packard, NG SOC (англ. *Next Gen SOC або Next-Generation SOC (*Security Operations Center*), укр. Нова генерація Центру забезпечення безпеки*) є два ключові аспекти, які підвищують дієвість роботи центру: використання автоматизації діяльності персоналу стосовно реагування на інциденти та правильно побудована організаційна модель (модель команд та рівнів SOC), див. рис. 2.

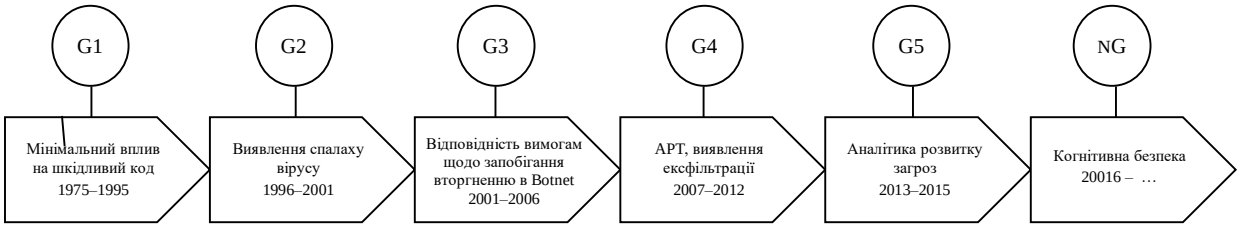

Рис. 2 Еволюція розвитку SOC

Автоматизація дає змогу підвищити продуктивність роботи та швидкість відгуку на інциденти, оскільки роботи, пов’язані з SOC є циклічними, а саме такі завдання є ідеальними для автоматизації (див. рис. 1–3). Окрім того, залишається час і енергія для розгляду складних інцидентів або проактивного пошуку загроз. Тобто, автоматизація потрібна не для того, щоб вилучити людей з процесу моніторингу, а щоб розширити їх можливості; фахівці є ключовою ланкою процесу моніторингу та реагування на інциденти. Також потрібно пам’ятати, що вкрай необхідно постійно вдосконалювати алгоритми – сьогоднішні порушники ІБ надзвичайно креативні та постійно змінюють свої методи, щоб залишитись непомітними.

Щоб ефективно вирішувати завдання моніторингу та оптимально реагувати на інциденти у сфері захисту інформації, необхідно контролювати всі ключові процеси SOC, починаючи від раннього виявлення та закінчуючи нейтралізацією подій. Для цього необхідно виділити в команді три лінії спеціалістів і додатково максимально автоматизувати завдання, що повторюються (див. рис. 3) [15].

Рис. 3 Організаційна структура SOC

Першу лінію вважають головною – вона відповідає за швидке реагування більшості інцидентів. Щоб скоротити час оброблення події і зменшити ймовірність появи помилок треба дотримуватись розроблених правил; саме тут оброблюють інциденти, які можна усунути протягом дуже короткого проміжку часу (зазвичай менше години). На другу лінію SOC передають ті випадки, для яких не розроблено стандартизованих інструкцій чи потрібно ізолювати реакцію об'єкта на подію або інцидент, чи навіть залучити інших фахівців для подальшого вивчення.

Друга лінія займається подіями, що потребують більш глибокого аналізування. Більшість подій потрапляє сюди від аналітиків першої лінії, але друга лінія також повинна відстежувати інциденти, пов'язані з критично важливими інформаційними активами, для розслідування так само потрібен структурований підхід, але в силу підвищеної складності проблем він може бути більш гнучким, ніж на першій лінії. На другій лінії вже починають опрацьовувати загрози.

Третя лінія переважно займається просунутим "хантінгом" – проактивним пошуком і ізоляцією складних загроз і прихованої активності, які виявили наявні засоби захисту, а також форензік. Взагалі більшість подій відсікається інструментами першої і другої ліній, і лише інциденти з ознаками суттєвих відхилень від нормальної поведінки передають на третю лінію.

Слід пам'ятати, що в сучасних умовах комп'ютери це лише одна зі складових інформаційної інфраструктури організації, а тому потрібно передбачати комплексний підхід до розв'язання проблеми захисту інформації [5].

У теорії захисту інформації для визначення категорій, аналізу та синтезу систем використовують два підходи – формальний і неформальний. Традиційно формальний підхід полягає у визначенні і підтвердженні Політики ІБ, де встановлено критерії та моделі у формальному вигляді. Побудова (синтез) гарантовано захищеної системи є однією з проблем теорії захисту. В класі відкритих систем цю проблему відносять до алгоритмічно нерозв'язних проблем. Формальний підхід теорії захисту інформації не може задовольнити всі вимоги, що виникають під час дослідження та створення СЗІ. Тому цей підхід доповнюється традиційним неформальним (описовим) підходом. Неформальний підхід – методи і механізми, які використовують для захисту інформації в автоматизованих системах (АС). У теорії захисту інформації цю проблему вирішують, застосовуючи метод ієрархічної декомпозиції складних систем, коли загальну складну

систему розподіляють на ієрархічні рівні [5], рис. 4. Вказані підсистеми вивчають із застосуванням характерних для кожного рівня методів аналізу.

Слід зазначити, що який би підхід не застосовувався, методи досліджень систем захисту загалом зведені до класичної побудови моделей об'єкту або внесення в об'єкт дослідження деякої структури, що має штучний характер, але полегшує дослідження [5]. На рис. 5 показано чинники, що впливають на побудову моделі захисту інформації.

1-й рівень	Політика безпеки
2-й рівень	Системи підтримки безпеки
3-й рівень	Механізми захисту
4-й рівень	Реалізація механізмів захисту

Рис. 4 Ієрархічна декомпозиція системи захисту

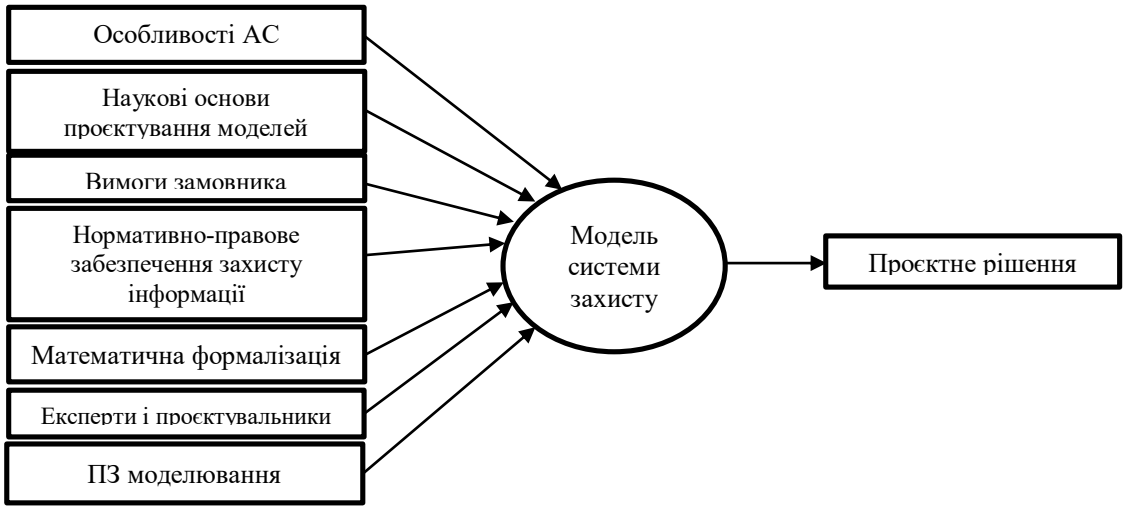

Рис. 5 Чинники, що впливають на побудову моделі системи захисту

Найбільш часто використовують оптимізаційні моделі прийняття рішень. Їх загальний вигляд такий:

$$F(X) \rightarrow max\, X \in A, \tag{3}$$

де X – параметр, який децидент може вибирати (керуючий параметр). Він може мати різну природу – число, вектор, множина тощо. Мета децидента: максимізувати цільову функцію □(□), вибравши відповідний □. За цього децидент повинен враховувати обмеження □ ∈ □ на можливі значення керуючого параметра □, знаючи, що цей параметр повинен належати множині □ [1, 3].

NG SOC (див. рис. 2) окрім традиційних функцій (управління журналами, кореляція подій, робота з інцидентами та відправка оповіщень) має нові можливості, такі як: довгострокове зберігання величезних обсягів даних, як структурованих, і неструктурованих; їх подальший аналіз за допомогою засобів BigData, включаючи методи машинного навчання, які дозволяють виявляти різні аномалії та шукати приховані загрози; поведінковий аналіз дій користувачів та вузлів мережі; координація

процесу реагування на інциденти ІБ; автоматизація операцій з реагування на обставини та їх нейтралізації.

Базові технології SOC нового покоління можна умовно поділити на кілька рівнів: рівень збору даних та зберігання; рівень моніторингу та аналізу даних; рівень автоматизації та реагування; рівень візуалізації та звітності.

Розширені аналітичні можливості NG SOC є ключем до вирішення проблеми виявлення прихованих загроз. Ці можливості реалізуються за допомогою засобів поведінкового аналізу, засобів статистичного аналізу та машинного навчання. І ці засоби дають змогу визначати взаємозв'язки між даними та виявляти різні відхилення, аномалії та тренди. В NG SOC використовується автоматизація реагування на інциденти [15]. Це уможливлює підвищення ефективності роботи центру загалом і знизити навантаження на персонал. Засоби візуалізації забезпечують наочність результатів проведеного аналізу даних у вигляді трендів та кореляцій та допомагають своєчасно розпізнавати проблемні ситуації. У NG SOC гнучке налаштування візуалізації даних дозволяє співробітникам швидше і точніше визначати закономірності та аномалії в роботі АС організації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Теоретичні основи побудови формальних моделей систем захисту інформації є надзвичайно складними, і незважаючи на інтенсивні дослідження у цій сфері, що проводяться, вони ще далекі від успіху. Тому практичного застосування отримали неформальні (описові) моделі, такі як: загальна модель захисту інформації, модель загроз інформації, модель порушника, модель аналізу систем розмежування доступу до ресурсів АС.

Ці моделі в найзагальнішому вигляді відображають процес захисту інформації як процес взаємодії дестабілізуючих чинників, що впливають на інформацію, і засобів захисту інформації, що перешкоджають дії цих чинників. Підсумком такого моделювання має бути визначення того чи іншого рівня захищеності інформації. Також вказані процеси в найзагальнішому вигляді можуть бути представлені як процеси розподілу і використання ресурсів, що виділяються на захист інформації. Основною спрямованістю є оцінка не просто загроз інформації як таких, а ще й оцінка тих втрат, які можуть мати місце при проявах різних загроз. Моделі цього напряму важливі ще і тим, що саме ними здебільше виявляються ті умови, за яких забезпечується вирішення завдань аналізу і синтезу систем (механізмів) розмежування доступу до різних видів ресурсів АС. Важливість цих моделей обумовлена й тим, що механізми розмежування доступу належать до найбільш суттєвих компонентів систем захисту інформації, і його вплив на ефективність функціонування таких систем в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Кушлик-Дивульська, О., Кушлик, Б. (2014). Основи теорії прийняття рішень.
2 Бідюк, П., Гожий, О., Коршевнюк, Л. (2012). *Комп'ютерні системи підтримки прийняття рішень: нав. пос.* НТУУ КПІ.
3 Орлов, А. (2005). *Теория принятия решений : уч.пос.* Экзамен.
4 Степанов, В. (2004). *Основы теории принятия решений : эксперим. уч. пос.* Клио.
5 Ковтунець, В.В., Нестеренко, О.В., Савенков, О.І. (2016). *Безпека систем підтримки прийняття рішень : навч. посіб.* Нац. ак. управ.
6 Shmelova, T., Sikirda, Yu. (2018). Models of Decision Making Operators of Socio-Technical System. *International Publisher of Progressive Information Science and Technology Research*, 33-75.
7 Sikirda Yu., Shmelova T. (2018). Analysis of the Development Situation and Forecasting of Development

of Emergency Situation in Socio-Technical Systems. *International Publisher of Progressive Information Science and Technology Research*, 76-107.

8 Подскребко, О. (2019). Розробка структури системи підтримки прийняття рішень з управління виробничою логістикою промислового підприємства. *Бізнес Інформ*, (4), 139–146. https://doi.org/10.32983/2222-4459-2019-4-139-146.

9 Очеретяний, А., Євтушенко, Г., Кузнецов, В. Розробка Android додатку для підтримки прийняття рішення на основі методу аналізу ієрархій. https://doi.org/10.32839/2304-5809/2019-1-65-63.

10 Набибекова, Г. (2014). Применение систем поддержки принятия решений в э-государстве. *Elektrondövlətquruculuğu problemləri,* I Respublikaelmi-praktikikonfransı, 4 dekabr. https://ict.az/uploads/konfrans/GOOGLE_SCHOLAR_e-gov/34G.Nabib.pdf.

11 Волошин, О.Ф., Мащенко, О.С. (2010). *Моделі та методи прийняття рішень: навчальний посібник.* Київський університет.

12 Трофимова, Л.А. (2012). *Методы принятия управленческих решений: уч.пос.* СПб ГУЭФ.

13 Бланк, І.А. Методи обгрунтування управлінських рішень в умовах ризику та невизначеності. http://econ.me.pn/metodyi-obosnovaniya-upravlencheskih-resheniy-18056.html.

14 Мединська, Т.М. Моделі і методи прийняття рішень в умовах невизначеності. http://dspace.wunu.edu.ua/jspui/bitstream/Мединська.pdf.

15 Знахарев, Д. Концепция создания SOC следующего поколения. http://AntiMalware.ru.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Oleksandr Avtushenko
Candidate of pedagogical sciences, associate professor, associate professor of the department
Institute of special communication and information protection
of National technical university of Ukraine
Igor Sikorsky Kyiv polytechnic institute, Kyiv, Ukraine
ORCID ID: 0000-0003-0910-7552
avtushenko_a@ukr.net

Vira Hyrda
senior engineer
Institute of special communication and information protection
of National technical university of Ukraine
Igor Sikorsky Kyiv polytechnic institute, Kyiv, Ukraine
ORCID ID: 0000-0002-3858-4086
gidraponka@ukr.net

Yuliia Kozhedub
Candidate of technical sciences, senior research
Institute of special communication and information protection
of National technical university of Ukraine
Igor Sikorsky Kyiv polytechnic institute, Kyiv, Ukraine
ORCID ID: 0000-0001-6181-5519
JuliaKozhedub@email.ua

Andrii Maksymets
senior engineer
Institute of special communication and information protection
of National technical university of Ukraine
Igor Sikorsky Kyiv polytechnic institute, Kyiv, Ukraine
ORCID ID: 0000-0003-3551-0628
andy.west.corp@gmail.com

ANALYSIS OF METHODS, METHODS, MECHANISMS, TOOLS THEORIES OF DECISION-MAKING FOR MODELING INFORMATION PROTECTION SYSTEM

Abstract. The article presents a detailed analysis of methods, methods, mechanisms, tools of decision theory for modeling information security systems. The basic terminological concepts are given, and their detailed definition is given. The combination of elements of decision theory with information security systems is shown. The connecting link for this is probability theory. The issue of decision-making procedure as a process is studied. Emphasis is placed on the qualitative parameters of the decision-making procedure that may be suitable for information protection purposes. Analogies have been made that indicate the applicability of decision theory methods to create a model of information security system. Implementation mechanisms are shown in decision-making algorithms. With the help of decision-making theory tools, it has been established that the modeling process can be formalized since both mathematical icons and verbalization. In general, the step-by-step process of designing an information security system is described. It is concluded that formalization as a type of symbolic modeling simultaneously with the application of decision theory is the best option for the descriptive part of the information security system. Modeling has been found to be the best scientific tool for combining theoretical calculations and the practical application of a wide range of research issues, including information security. To support the decision-making of the decision-maker, in other words the offender, in the field of information protection, it is important that the security officer or system administrator has experience and skills in regulated actions. Such actions are both well-known developments in this field of activity and a synthesis of already known algorithms to achieve the state of information security in general. Automation in decision-making is possible through the introduction of a decision support system that is widely used in automated systems: computer systems and networks, especially where there is a need to analyze significant data flows.

Keywords: information security; modeling; information security system model; decision making process; decision support systems, decision theory.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kushlyk-Divulskaya, O., Kushlyk, B. (2014). Fundamentals of decision theory.
2. Bidyuk, P., Gozhiy, O., Korshevnyuk, L. (2012). O Computer decision support systems: nav. pos. NTUU KPI.
3. Orlov, A. (2005). Theory of decision making: uch.pos. Exam.
4. Stepanov, V. (2004). Fundamentals of decision theory: experiment. account pos. Clio.
5. Kovtunets, V., Nesterenko, O., Savenkov, O. (2016). Security of decision support systems: textbook. way. Nat. ak. Management.
6 Shmelova, T., Sikirda, Yu. (2018). Models of Decision Making Operators of Socio-Technical System. International Publisher of Progressive Information Science and Technology Research, 33-75.
7 Sikirda Yu., Shmelova T. (2018). Analysis of the Development Situation and Forecasting of Development of Emergency Situation in Socio-Technical Systems. International Publisher of Progressive Information Science and Technology Research, 76-107.
8 Podskrebko, O. (2019). Rozrobka struktury systemy pidtrymky pryiniattia rishen z upravlinnia vyrobnychoiu lohistykoiu promyslovoho pidpryiemstva. Biznes Inform, (4), 139–146. https://doi.org/10.32983/2222-4459-2019-4-139-146.
9 Ocheretianyi, A., Yevtushenko, H., Kuznetsov, V. Rozrobka Android dodatku dlia pidtrymky pryiniattia rishennia na osnovi metodu analizu iierarkhii. https://doi.org/10.32839/2304-5809/2019-1-65-63.
10 Nabybekova, H. (2014). Prymenenye system podderzhky pryniatyia reshenyi v э-hosudarstve. Elektrondövlətquruculuğu problemləri, I Respublikaelmi-praktikikonfransı, 4 dekabr. https://ict.az/uploads/konfrans/GOOGLE_SCHOLAR_e-gov/34G.Nabib.pdf.
11 Voloshyn, O.F., Mashchenko, O.S. (2010). Modeli ta metody pryiniattia rishen: navchalnyi posibnyk. Kyivskyi universytet.
12 Trofymova, L.A. (2012). Metodы pryniatyia upravlencheskykh reshenyi: uch.pos. SPb HUЭF.
13 Blank, I.A. Metody obgruntuvannia upravlinskykh rishen v umovakh ryzyku ta nevyznachenosti. http://econ.me.pn/metodyi-obosnovaniya-upravlencheskih-resheniy-18056.html.
14 Medynska, T.M. Modeli i metody pryiniattia rishen v umovakh nevyznachenosti. http://dspace.wunu.edu.ua/jspui/bitstream/Medynska.pdf.
15 Znakharev, D. Kontseptsyia sozdanyia SOC sleduiushcheho pokolenyia. http://AntiMalware.ru.