ISSN 2411-3816

УДК 004.621.3:519.816

С.В. Зибін,
кандидат технічних наук, доцент
Державного університету телекомунікацій, м. Київ

КРИТЕРІЇ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НЕВИЗНАЧЕНОСТЕЙ. КРИТЕРІЙ РИЗИКУ

Розглядається задача підвищення ефективності процесів формування системи інформаційної безпеки. Описано основні критерії оцінки ефективності процесів формування системи інформаційної безпеки в умовах обмежень і невизначеностей. Інтегральний критерій ефективності складається з підкритеріїв: оперативності, якості, безперервності, надійності, однозначності, ризику.

У статті пропонується використовувати критерій ризику реалізації загроз для оцінки ефективності. Запропонована методика аналізу ризиків дозволяє визначити ефективність прийнятих або запланованих рішень. Крім того, значення ймовірності реалізації загрози залежить від рівня ешелонування захисту.

Результат застосування СППР – підвищення ефективності прийнятих рішень і зниження витрат при створенні і експлуатації систем захисту інформації.

Ключові слова: *інформаційна безпека, автоматизована інформаційна система, захист інформації, система підтримки прийняття рішень, багатокритеріальна оптимізація, система керування, моделювання процесів, інформаційний вплив, керуюче рішення, комплексна система захисту інформації.*

Рассматривается задача повышения эффективности процессов формирования системы информационной безопасности. Описаны основные критерии оценки эффективности процессов формирования системы информационной безопасности в условиях ограничений и неопределенностей. Интегральный критерий эффективности состоит из подкритериев: оперативности, качества, непрерывности, надежности, однозначности, риска.

В данной статье предлагается использовать критерий риска реализации угроз для оценки эффективности. Предложенная методика анализа рисков позволяет определить эффективность принятых или планируемых решений. Кроме того, значение вероятности реализации угрозы зависит от уровня эшелонирования защиты.

Результатом применения СППР является повышение эффективности принимаемых решений и снижение затрат при создании и эксплуатации систем защиты информации.

Ключевые слова: *информационная безопасность, автоматизированная информационная система, защита информации, система поддержки принятия решений, многокритериальная оптимизация, система управления, моделирование процессов, информационное воздействие, управляющее решение, комплексная система защиты информации.*

The task of increasing processes effectiveness of forming an information security system is considered. The main criteria for assessing the processes of effectiveness of

forming an information security system in conditions of limitations and uncertainties are described. The integral criterion of effectiveness consists of sub-criteria: efficiency, quality, continuity, reliability, uniqueness, risk.

In this paper, the author suggests using a risk criterion for implementing threats to assess effectiveness. The offered method of risk analysis allows to determine the efficiency of the adopted or planned solutions. In addition, the probability of realizing the threat depends on the level of security separation.

The result of the DSS application is to increase the efficiency of the taken decisions and reduce costs in the creation and operation of information security.

Keywords: *information security, automated information system, information protection, decision support system, multi-criteria optimization, control system, process modeling, information impact, control solution, integrated information security system.*

Вступ

Для оцінки ефективності функціонування систем підтримки прийняття рішень (СППР) необхідно визначити показник, за чисельною величиною якого можна зробити висновок про те, наскільки результат є хорошим або рішення приємним. Цей показник називається критерієм ефективності.

На основі аналізу ряду робіт [1; 2] можна визначити основні вимоги до критерію ефективності. Критерій повинен бути:

- несуперечним і комплексним;
- залежати від структури системи, значень її параметрів, характеру впливу зовнішнього середовища, зовнішніх і внутрішніх факторів;
- повним, тобто відображати основні види витрат;
- представницьким, відображати основну мету управління;
- допускати порівняння одержуваного ефекту з витратами сил і засобів;
- забезпечити чітке уявлення фізичного сенсу кожного з порівнюваних варіантів і ступеня досягнення поставленої мети в кожному з них.

Основна частина

Аспекти розробки та застосування СППР детально розглянуто у роботах [3–5]. Проаналізовано історію їх розвитку, галузі застосування, наведено опис найпоширеніших СППР. Необхідними умовами ефективності рішень, що приймаються, є своєчасність, комплексність та оптимальність. Перша з наведених умов є обмеженням, а інші – визначальними фундаментальними умовами. Вимога комплексності передбачає необхідність якомога повнішого та всебічного урахування впливу на рішення внутрішніх і зовнішніх факторів та їх взаємозв'язків.

Значний внесок у вирішення проблем застосування систем підтримки прийняття рішень зробили такі відомі зарубіжні та вітчизняні вчені, як Фішберн П., Кіні Р., Райфа Р., Сааті Т., Руа Б., Заде Л., Герасимов Б.М., Тоценко В.Г., Ларічев О.І., Бідюк П.І., Подіновський В.В., Волошин О.Ф., Наконечний О.Г., Згуровський М.З., Зайченко Ю.П., Панкратова Н.Д. та багато інших. Методи та засоби забезпечення захисту інформації розглянуті у [6–8]. Комплексне дослідження аспектів задач прийняття рішень має велику теоретичну і прикладну значимість і є актуальним.

Критерій повинен просто і швидко обчислюватися, має бути зрозумілий його зміст. Він повинен мати властивість насичення. В узагальненому критерії неприпустимо дублювання одного і того ж показника, оскільки це веде до завищення

ISSN 2411-3816

його ролі в порівнянні з іншими. Критерій повинен мати мінімальну розмірність. Нині критерії широко застосовуються для оцінки ефективності використання коштів, а також ступеня виконання поставленого завдання. Найбільш часто вживаними є дві групи критеріїв: оперативна і економічна. За своєю значимістю залежно від сутності системи вони можуть бути головними і допоміжними.

Як правило, як головний критерій вибирається оперативний, оскільки він дозволяє оцінити ступінь досягнення мети або ступінь виконання поставленого завдання.

$$K_{оп} = \frac{F}{F_H}, \qquad (1)$$

де: $K_{оп}$ – оперативний критерій;

F і $F_н$ – фактичне і нормативне значення показника ефективності.

Такий вид критерію широко використовується при оцінці ефективності різних систем управління.

Економічні критерії дозволяють оцінити кількість ресурсів для досягнення поставленої мети. У процесі планування і знаходження рішення критерії можуть виражатися в тимчасових показниках – в затратах, енерговитратах. Порівняння загальноприйнятих критеріїв оцінки вказує на необхідність їх трансформації з урахуванням специфіки СППР.

Аналіз методів оцінки ефективності функціонування СППР дозволяє зробити такі висновки:

- існуючі критерії різнотипні і не становлять стрункої системи; вибір найкращого критерію викликає певні труднощі;
- відсутні чіткі рекомендації для вибору інтегрального критерію;
- критерії є простими і, як наслідок, відсутні складні критерії.

Все це визначає необхідність розробки критеріїв оцінки ефективності функціонування СППР. При оцінці ефективності функціонування СППР істотне значення має визначення цілей оцінки. Можна ставити питання про оцінку ефективності її функціонування. Побудова системи критеріїв оцінки ефективності управління проводилася на основі визначення цілей і побудови «дерева» цілей СППР (рис. 1), тобто критерії створюються таким же чином, як і мета, на основі певного формального підходу.

За ступенем формалізації цілі повинні бути чітко сформульованими і піддаватися формалізованому опису. Вони мають виражати лише загальний напрямок дій системи. При наявності на одному рівні кількох характеристик цільового стану системи можливі два підходи: перший – метою діяльності системи є одна з найбільш важливих характеристик, другий – при неможливості виділення головної характеристики як цілі приймаються декілька з них. Оптимальному стану СППР буде відповідати їх оптимальне співвідношення.

На кожному рівні СППР існують цілі, властиві лише цьому рівню. Цілі вищого рівня містять більше невизначеності, менш структуровані і не можуть бути використані для вибору конкретного способу дій. Тому загальна мета підлягає декомпозиції на підцілі до тих пір, поки вони не будуть настільки конкретними, щоб їх можна було б реалізувати в процесі управління.

ISSN 2411-3816

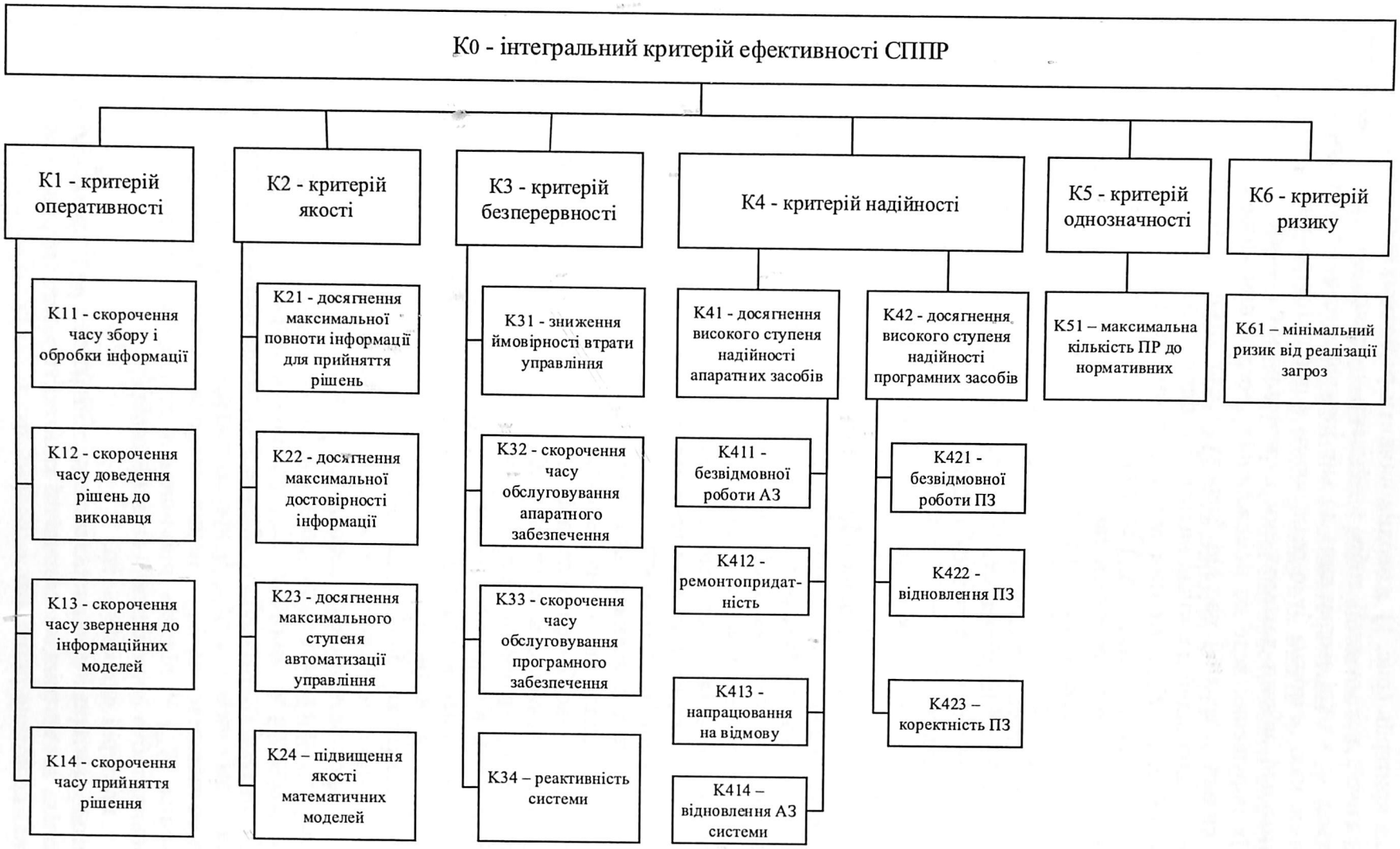

Рис. 1. Критерії оцінювання ефективності

Аналіз критеріїв (рис. 1) дозволив виявити ряд закономірностей. Загальна мета K_0 підлягає декомпозиції, тобто розбивається на підцілі, які, у свою чергу, розбиваються на підцілі зверху вниз до тих пір, поки вони не будуть настільки конкретними, щоб їх можна було реалізувати в процесі управління.

Вертикальні зв'язки декомпозиції є необхідними і найбільш важливими, оскільки їх порушення веде до неможливості досягнення кінцевої мети. Вони найбільш сильні у верхній частині "дерева" і слабшають у міру декомпозиції цілей вниз. Аналіз цілей дозволив визначити підцілі і розподілити їх у порядку переваги $(K_1, K_2, \ldots, K_n)$. Кожна мета розбивається ще раз на підцілі $(K_{11}, \ldots, K_{1n}, K_{21}, \ldots, K_{2k}, \ldots, K_{l1}, \ldots, K_{ln})$ зверху вниз по вертикальних зв'язках.

Дерево цілей може включати такі цілі та їх показники.

K_0 – це інтегральний показник ефективності, який складається з $(K_1, K_2, \ldots, K_n)$ критеріїв.

– критерій оперативності.

Метою критерію оперативності є підвищення оперативності прийнятих рішень. Критерій оперативності складається з критеріїв (підцілей) $K_{11}, K_{12}, K_{13}, K_{14}$. K_{11} – підціль скорочення часу збору і обробки інформації. K_{12} – підціль скорочення часу доведення рішень до виконавця. K_{13} – підціль скорочення часу звернення до інформаційних моделей. K_{14} – підціль скорочення часу прийняття рішення.

K_2 – критерій якості рішень або критерій обґрунтованості рішень.

Метою критерію є підвищення обґрунтованості прийнятих рішень. Критерій обґрунтованості рішень складається з критеріїв (підцілей) K_{21}, K_{22}, K_{23}. K_{21} – підціль досягнення максимальної повноти інформації для прийняття рішень. K_{22} – підціль досягнення максимальної достовірності інформації. K_{23} – підціль досягнення максимального ступеня автоматизації функцій органів управління. K_{24} – підціль підвищення якості математичних моделей.

K_3 – критерій безперервності.

Метою критерію є забезпечення безперервності роботи системи інформаційної безпеки. K_{31} – підціль зниження ймовірності втрати управління при виході з ладу обладнання та засобів автоматизації. K_{32} – підціль скорочення часу технічного обслуговування апаратного забезпечення. K_{33} – підціль скорочення часу технічного обслуговування програмного забезпечення. K_{34} – підціль реактивності системи, тобто забезпечення високого ступеня ймовірності розв'язання завдань управління інформаційною безпекою при заданих часових обмеження.

K_4 – критерій надійності.

Метою критерію є підвищення надійності функціонування системи. K_{41} – підціль досягнення високого ступеня надійності апаратних засобів. K_{411} – підціль підвищення часу безвідмовної роботи апаратного забезпечення. K_{412} – підціль підвищення ступеня ремонтопридатності обладнання. K_{413} – підціль підвищення часу напрацювання на відмову. K_{414} – підціль скорочення часу відновлення технічної складової системи. K_{42} – підціль досягнення високого ступеня надійності програмного забезпечення. K_{421} – підціль підвищення часу безвідмовної роботи програмного забезпечення. K_{422} – підціль скорочення часу відновлення програмного забезпечення. K_{423} – підціль підвищення ступеня коректності програмного забезпечення, тобто відповідності специфікаціям.

K_5 – критерій однозначності.

Метою критерію є підвищення однозначності при управлінні системою K_{51} – підціль досягнення максимальної кількості прийнятих рішень до кількості рішень, які необхідно прийняти за певний час.

K_6 – критерій ризику.

Метою критерію є зменшення ризиків реалізації загроз інформаційній безпеці.

Достатньо загальноприйнятими показниками ефективності ергатичних систем управління є оперативність прийнятих рішень і їх якість [9].

При оцінці ефективності СППР можна використовувати критерій ризику інформаційної безпеки.

Найбільш поширена оцінка інформаційних ризиків має вигляд:

$$R = pC,$$

де R – інформаційний ризик;

p – ймовірність порушення інформаційної безпеки;

C – вартість інформаційних ресурсів.

При побудові системи захисту досить складно розрахувати загальне значення ймовірності порушення безпеки, але можна знайти значення ймовірності реалізації окремих загроз. Відповідно, загальне значення ризику можна знайти як суму значень ризиків від реалізації всіх загроз:

$$R = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} (p_i L_i) \ , \qquad (2)$$

де R_i – інформаційний ризик від реалізації i-ї загрози;

p_i – ймовірність реалізації i-ї загрози;

L_i – збиток від реалізації i-ї загрози.

Кожен вид загроз у системі підтримки прийняття рішень в умовах обмежень і невизначеностей може бути представлений у вигляді сукупності таких об'єктів:

$$T = \langle N, S, V, W, O, A \rangle, \qquad (3)$$

де N – вид загроз;

S – множина можливих джерел загроз цього виду;

V – множина можливих вразливостей, пов'язаних з цим видом загроз;

W – множина можливих способів реалізації загроз цього виду;

O – можливих об'єктів впливу загроз цього виду;

A – можливих деструктивних дій при реалізації загроз цього виду.

Зміст перерахованих множин для кожного виду загроз визначається експертами і міститься в базі знань.

Множини *S, V, O, A* складаються шляхом вибору з множини допустимих для цього виду загроз значень, які визначаються експертами, відповідно до властивостей і умов функціонування СППР. Множина W формується залежно від складу інших множин. Водночас множина A складається з п'яти підмножин, відповідно до критеріїв захищеності інформації [10]:

$$A = \langle A_к, A_ц, A_д, A_с, A_г \rangle,$$

де $A_к$ – множина деструктивних дій, спрямованих на порушення конфіденційності;

$A_ц$ – множина деструктивних дій, спрямованих на порушення цілісності;

$A_д$ – множина деструктивних дій, спрямованих на порушення доступності;

ISSN 2411-3816

A_c – множина деструктивних дій, спрямованих на спостережності;
$A_г$ – множина деструктивних дій, спрямованих на гарантованості.

Більшість відомих методик аналізу ризиків припускають введення значення ймовірності реалізації загрози p_i експертом [11–14]. Використання статистичних даних не дозволяє визначити, як змінюється значення при впровадженні того чи іншого механізму захисту. Саме тому пропонується метод обчислення ймовірностей на основі відомостей, що містяться в описі загрози (3).

Ключовим при обчисленні ймовірності реалізації загрози є множина можливих способів її реалізації. Чим більше можливих способів реалізації загрози, тим вище ймовірність того, що зловмисник спробує реалізувати цю загрозу. Множина W формується відповідно до того, які можливі джерела загрози, які уразливості і об'єкти присутні в СППР. Таким чином, ймовірність реалізації i-ї загрози безпеці може бути знайдена за формулою (4)

$$p_i = \left(\sum_{k=1}^{m} \alpha_k p_{r_k} \right) / m , \tag{4}$$

де p_{r_k} – ймовірність успішного використання зловмисником k-го варіанту реалізації i-ї загрози;

α_k – коефіцієнт достовірності, що визначає ступінь впевненості в тому, що зловмисник може скористатися k-м варіантом реалізації i-ї загрози;

m – кількість можливих способів реалізації i-ї загрози.

За відсутністю статистичної або іншої інформації коефіцієнти α_k вважаються однаковими за ймовірністю. Коефіцієнт α_k приймає два можливих значення: $\alpha_k = 0$, якщо відсутні об'єктивні передумови для використання варіанта загрози, який аналізується, і $\alpha_k = 1$, якщо такі передумови існують.

Кожен варіант реалізації загрози може бути повністю перекритий певним набором протидій. При цьому ймовірність успішного використання варіанта реалізації загрози залежить від того, яку кількість можливих контрзаходів реалізовано, і може бути розрахована за такою формулою:

$$p_{r_k} = 1 - \frac{K_{r_k}}{K_{u_k}} , \tag{5}$$

де K_{r_k} – кількість контрзаходів, що було виконано, які перекривають k-й варіант реалізації загрози;

K_{u_k} – загальна кількість контрзаходів, що перекривають k-й варіант реалізації загрози.

Розрахунок розміру збитків від реалізації i-ї загрози безпеки проводиться за такою формулою:

$$L_i = \left(\omega_к + \omega_ц + \omega_д + \omega_с + \omega_г \right) C , \tag{6}$$

де $\omega_к$, $\omega_ц$, $\omega_д$, $\omega_с$, $\omega_г$ – коефіцієнти значимості, що визначають значимість забезпечення відповідних критеріїв: конфіденційності, цілісності, доступності, спостережності і гарантованості;

C – вартість інформаційних ресурсів.

Розрахунок розміру збитку може бути здійснено відповідно до формули (6) окремо для кожного інформаційного ресурсу.

Нині інформаційно-аналітична підтримка неможлива без використання різноманітних мереж. Тому виконаємо розрахунок значення ризику для загрози "Аналіз мережевого трафіку".

Метою атак подібного типу є прослуховування каналів зв'язку і аналіз даних, що передаються, та службової інформації з метою вивчення топології та архітектури побудови системи, отримання критичної інформації користувачів. Атакам цього типу піддаються такі протоколи, як FTP і Telnet.

Передувати атакам аналізу мережевого трафіку може мережева розвідка. Це збір інформації про мережу за допомогою загальнодоступних даних і додатків. Мережева розвідка проводиться у формі запитів DNS, луна-тестування (Ping Sweep) і сканування портів. У результаті видобувається інформація, яку можна використовувати для злому. Зауважимо, що повністю позбавитися від мережевої розвідки неможливо.

Для загрози "Аналіз мережевого трафіку" в загальному випадку визначено шість можливих варіантів реалізації P1–P6 (m = 6):

P1: Використання шкідливої програми;

P2: Впровадження програмно-апаратної закладки;

P3: Перехоплення інформації, переданої по внутрішніх каналах зв'язку, з використанням вразливостей протоколів канального рівня;

P4: Перехоплення інформації, переданої по внутрішніх каналах зв'язку, з використанням вразливостей протоколів мережевого рівня;

P5: Перехоплення інформації, переданої по зовнішніх каналах зв'язку, з використанням вразливостей протоколів мережевого рівня;

P6: Використання вразливостей прикладного та спеціального програмного забезпечення.

Найбільш легким для уразливості місцем будь-якої обчислювальної, розподіленої системи є засоби бездротового доступу. Припустимо, що обчислювальна система побудована з використанням комутаторів, без використання мереж бездротового доступу, з використанням передачі даних по зовнішніх каналах зв'язку. Статистична інформація відсутня. В цьому випадку об'єктивні передумови для використання варіанту P3 відсутні, а коефіцієнти мають значення:

$$\alpha_3 = 0, \alpha_1 = \alpha_2 = \alpha_4 = \alpha_5 = \alpha_6 = 1.$$

Для перекриття решти варіантів реалізації загрози (P1, P2, P4, P5, P6) застосовуються такні контрзаходи:

Для P1: засоби антивірусного захисту.

Для P2: засоби забезпечення цілісності і фізична охорона внутрішніх каналів зв'язку.

Для P4: засоби виявлення вторгнень по внутрішніх каналах зв'язку.

Для P5: засоби виявлення вторгнень по зовнішніх каналах зв'язку.

Для P6: засоби забезпечення цілісності та засоби аналізу захищеності.

Якщо нереалізовані перераховані контрзаходи, то ймовірність успішного використання всіх варіантів реалізації загрози дорівнює 1. У цьому випадку ймовірність реалізації загрози визначається за формулою (4):

ISSN 2411-3816

$$p_i = \frac{1+1+1+1+1}{6} = \frac{5}{6} = 0,8333$$

При використанні засобів забезпечення цілісності, ймовірності успішного використання варіантів реалізації загрози приймають значення:

$$p_{r_1} = p_{r_4} = p_{r_5} = 1, \quad p_{r_2} = p_{r_6} = 0,5.$$

Тоді ймовірність реалізації загрози приймає значення: $p_i = 0,6667$.

Таким чином, існує можливість розрахувати значення ймовірності реалізації загрози при використанні різних засобів захисту і їх варіацій.

Далі експертам необхідно визначити значення вагових коефіцієнтів, що визначають значимість забезпечення відповідних критеріїв.

За характером впливу аналіз мережевого трафіку є пасивним впливом. Здійснення цієї атаки без зворотного зв'язку веде до порушення конфіденційності інформації всередині одного сегмента мережі на канальному рівні моделі OSI (Open Systems Interconnection Basic Reference Model). Відповідно, будемо враховувати тільки ваговий коефіцієнт конфіденційності.

Оскільки сума значущих коефіцієнтів не може перевищувати одиницю і при цьому вартість інформаційних ресурсів можна вважати постійною (або незмінною впродовж певного проміжку часу), і, як наслідок, не враховувати при відносному порівнянні, тоді значення ризику не може перевищувати значення ймовірності реалізації загрози. У табл. 1 наведені приклади розрахунку максимального, відносного значення ризику реалізації загрози при застосуванні різних контрзаходів з інформаційного захисту.

Запропонована методика аналізу ризиків дозволяє визначити ефективність прийнятих або запланованих рішень. Крім того, значення ймовірності реалізації загрози залежить від рівня ешелонування захисту.

Таблиця 1

Засоби протидії	Ймовірність реалізації загрози
Відсутні	0,8333
Засоби антивірусного захисту	0,5
Засоби забезпечення цілісності від внутрішніх порушників	0,54
Засоби забезпечення цілісності від зовнішніх порушників	0,25
Фізична охорона внутрішніх каналів зв'язку	0,58
Засоби виявляння порушень безпеки	0,5
Засоби аналізу захищеності	0,58
Засоби антивірусного захисту і засоби забезпечення цілісності	0,33
Засоби антивірусного захисту, засоби забезпечення цілісності від внутрішніх порушників, фізична охорона внутрішніх каналів зв'язку, засоби аналізу захищеності.	0,23

Методика не враховує ефективність перекриття способів протидії загрозам. Крім того, відсутня методика визначення вартості інформаційних ресурсів. Проте ця методика дозволяє оцінити ефективність і коректність рішень, що генеруються за результатами тестування прототипу СППР.

Модуль аналізу ризиків та оцінки ефективності є основним компонентом системи підтримки прийняття рішень, яка розробляється.

Результатом застосування СППР є підвищення ефективності прийнятих рішень і зниження витрат при створенні і експлуатації систем захисту інформації.

Висновок

Пропонуємо використовувати методику оцінювання ефективності прийнятих рішень і аналізу ризиків інформаційної безпеки. Ця методика аналізу ризиків дозволяє визначити ефективність прийнятих або запланованих рішень. До того ж значення ймовірності реалізації загрози залежить від рівня ешелонування захисту.

Методика не враховує ефективність перекриття способів протидії загрозам. Крім того, відсутня методика визначення вартості інформаційних ресурсів. Проте ця методика дозволяє оцінити ефективність і коректність рішень, що генеруються за результатами тестування прототипу СППР.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Багриновский М.А.* и др. Имитационные системы. Принятие экономических решений. Москва: Наука, 2001. 121 с.
2. *Длин А.М.* Математическая статистика в технике. Москва: Наука, 1980. 466 с.
3. *Бідюк О.П. , Гожий О.П., Коршевнюк Л.О.* Комп'ютерні системи підтримки прийняття рішень: навчальний посібник. Миколаїв: Вид-во ЧДУ ім. Петра Могили, 2012. 380 с.
4. *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных странах: учебник. 2-ое изд., перераб. и доп. Москва: Логос, 2002. 392 с.
5. *Саати Т.Л.* Принятие решений при зависимостях и обратных связях. Аналитические сети. Москва: Издательство ЛКИ, 2008. 360 с.
6. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации; под ред. Ю.С. Ковтанюка. Киев: ЮНИОР, 2003. 504 с.
7. *Браиловский Н.Н., Зыбин С.В., Хорошко В.А.* Модели управления в системах обеспечения информационной безопасности государства. Інформатика та математичні методи в моделюванні. Одеса. ОНПУ, Т. 4. № 4. 2014. С. 304–311.
8. *Зибін С.В., Хорошко В.А.* Підтримка прийняття рішень при формуванні програм інформаційної безпеки держави: оцінка ефективності програм. Інформатика та математичні методи в моделюванні. Одеса. ОНПУ, Т. 5. № 2. 2015. С. 122–129.
9. Введение в эргономику; под ред. В.П. Зинченко. Москва: Сов. Радио, 1974. 352 с.
10. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".
11. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации К.: Юниор, 2003. 504 с.
12. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. Киев: ООО "ТИД "ДС", 2002. 688 с.
13. *Згуровский М.З., Коваленко Н.И., Кондрак К.,* и др. Информационный подход к анализу и управлению проектными рисками. Проблемы управления и информатики. 2000. № 4, С. 148–156.
14. *Грачева М.В.* Анализ проектных рисков. Учебное пособие для вузов. Москва: ЗАО "Фин-статинформ", 1999. 216 с.

Отримано 21.11.2017
Рецензент Корченко О.Г., д.т.н., проф.