КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.636
УДК 004/8

Ткач Володимир Олександрович
старший науковий співробітник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0003-0013-7368
Tkachwolodymyr@gmail.com

Шемендюк Олександр Віталійович
начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-5594-2973
1o2l3d@gmail.com

Чередниченко Олексій Юрійович
старший науковий співробітник науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-0816-8321
n0ize@ukr.net

ДОСЛІДЖЕННЯ ПИТАНЬ З ОЦІНКИ І УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ТА ФОРМУВАННЯ ПОКАЗНИКІВ РІВНЯ ЗАХИЩЕНОСТІ

Анотація. Відомо, що у сфері управління сектору безпеки і оборони включаються різні ресурси — інформація, особовий склад (персонал), планування, підготовка, ведення бойових дій (операцій), логістика та оперативне забезпечення. Загальновідомим фактором підвищення їх життєво-здатності є ефективне використання інформаційних систем. У зв'язку з появою нових загроз, що постійно змінюються і циркулюють в інформаційних системах, виникла проблема щодо оцінювання і управління ризиками інформаційної безпеки в секторі безпеки і оборони та питання формування показників рівня захищеності інформації. У статті запропоновані: концепція RME, доцільність її впровадження, визначення ризику інформаційної безпеки, розрахунок очікуваного значення результату ризикованої діяльності та що необхідно визначати під час управління ризиками інформаційної безпеки, методика управління ризиками інформаційної безпеки, методи оцінювання ризиків як якісні так і кількісні та порядок визначення очікуваного розміру шкоди(збитку) військової інформації, сформовані інженерні заходи захисту інформації та заходи рівня кваліфікації і надійності персоналу та їх оцінки. Зазначимо, що вказані вище задачі можна досягти за рахунок застосування успішного та ефективного управління ризиками, уточнення органам управління порядку оцінювання інформаційної захищеності, обов'язків з визначення та застосування процесу оброблення ризиків інформаційної безпеки. Передбачається, що запропоновані дослідження з питання оцінки і управління ризиками інформаційної захищеності, формування рівня захищеності інформації, дозволять визначити, найбільш доцільний підхід з питань оцінювання системи захисту інформації, які можуть бути враховані в практичній роботі. Реалізація запланованого підходу дозволить значно покращити процес оцінювання ризиків інформаційної безпеки, порівнювати різні шкоди і ймовірності, формувати показники та критерії рівня інформаційної захищеності і, як наслідок, може стати основою для оцінки і управління ризиками та формування показників рівня захищеності інформації.

Ключові слова: інформаційна безпека; системи управління інформаційною безпекою; оцінки і управління ризиками; методики оцінки та управління ризиками; формування показників захищеності.

ВСТУП

Постановка проблеми. У зв'язку з появою нових загроз, які постійно змінюються в інформаційних системах, постає наукове завдання щодо оцінки та управлінням ризиками інформаційної безпеки і формування показників рівня захищеності інформації.

Аналіз останніх досліджень і публікацій. Відомо багато прикладів проведення досліджень і публікацій з питань оцінки і управління ризиками інформаційної безпеки (ІБ) в інформаційних системах (ІС) та забезпечення високого рівня інформаційної безпеки, основні із них наведено нижче.

У цій статі [1] проведено аналіз моделей оцінки ризиків інформаційної безпеки для побудови системи захисту інформації.

У двотомному підручнику [2] розглянуті питання управління інформаційною безпекою системи захисту інформації.

У роботі [3] проведено аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки.

У стандарті [4] (ISO/IES 27000:2009) визначені системи керування інформаційною безпекою.

У стандарті [5] (ISO/IEC 27035) розкрито питання управління інцидентами інформаційної безпеки.

У стандарті [6] (ISO/IEC 27005:2018) розкрито питання щодо інформаційної технології, методів і засобів забезпечення безпеки та менеджменту ризиків інформаційної безпеки.

У посібнику [7] вчені Ландолл та Кевін Генрі дослідили питання управління та аналіз ризиків і видали довідник з управління безпекою.

У роботі [8] К. Дж. Альбертс, С. Г. Беренс, Р. Д. Петія, В. Р. Вілсон проведено аналіз з операційно-критичної оцінки загроз, активів і вразливостей.

Керівництво [9] було розроблено з управління ризиками для систем інформаційних технологій, та рекомендації Національного інституту Стандартів і технологій.

У публікації [10] описується структура управління ризиками (RMF) і надаються вказівки щодо застосування RMF до інформаційних систем і організацій.

У роботі [11] розглянуто питання з концепції оцінки ризиків кібербезпеки інформаційної системи об'єкта критичної інфраструктури.

У науковій праці [12] проведено аналіз з питань формування системи показників оцінки рівня інформаційної безпеки підприємства.

У науковій статті [13] розглянуто питання, що стосуються оцінки засобів захисту інформаційних ресурсів.

У роботі [14] розглянуто питання з методів кількісної оцінки стійкості системи зберігання даних.

У роботі [15] розглянуту питання економічної оцінки конфіденціальної інформації організації.

У статті [16] було розглянуті терміни «інформація» та «цінність інформації» у спеціалізованому визначенні для використання у військовій справі.

Завдяки аналізу вище зазначених публікацій і досліджень, у зв'язку з появою нових загроз, що постійно змінюються в інформаційних системах та відсутністю єдиного підходу з оцінки ефективності системи захисту інформації запропоновано більш ефективний підхід оцінки та управління ризиками інформаційної безпеки (ІБ) та з питання формування показників рівня інформаційної захищеності.

Мета статті. Метою статті є оцінювання ризиків інформаційної безпеки (ІБ), як з питань оцінки управління ризиками інформаційної безпеки (ІБ) сектору безпеки та оборони (СБО) так і з формування рівня захищеності інформації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Завданнями дослідження є:

- запропонувати СБО методику управління ризиками;
- методику оцінювання та їх обчислення;
- методи оцінки ризиків та формування показників оцінювання рівня інформаційної захищеності.

Вивчаючи питання оцінки і управління ризиками інформаційної безпеки [1] – [2], формування показників рівня захищеності інформації ми звернули увагу на активну дію міжнародних установ [3] – [6], які підтверджують важливість питань забезпечення інформаційної безпеки в інформаційних системах та регулярного удосконалення моделей, методів інформаційних механізмів безпеки інформаційних технологій.

Визначальним підходом до забезпечення інформаційної безпеки (ІБ) в ІС є стратегія захисту на підгрунті RISK — Based Protection Strategy [8]. Програми управління ризиками передбачають побудову системи забезпечення інформаційної безпеки. Ці програми ІБ об’єднані у організаційну і технічну інфраструктуру. Вони мають бути впроваджені, як складові частини загального управління в цілому. Значення управління ризиками відносно ІБ під час функціонування та використання ІС є надзвичайно важливим для досягнення СБО стратегічних цілей та завдань. Виходячи з підходів NIST США (Національний Інститут Стандартів і Технологій) розроблює та запроваджує методологію забезпечення ІБ, структуру управління ризиками (RMF) [7] – [10]. Концепція RMF дозволяє наступне:

- управляти організаційними ризиками;
- забезпечувати успіх своїх програм;
- впроваджувати різноманітний структурний погляд до управління ризиками пов’язаними із впровадженням ІС у процеси різних структурних підрозділів.

Покладаючись на зазначену концепцію вважаємо доцільно її впровадити під час проведення досліджень питань оцінки управління ризиками інформаційної безпеки та формування показників рівня захищеності інформації. Такими цілями можуть бути наступні:

- забезпечення одного і того ж процесу налаштування ІБ у відповідності до діючих ризиків;
- установити цілісну загальну систему з підходу до управління ризиками безпеки;
- впровадити єдину методику класифікації (категоризації) ІС та заходи безпеки, які поширюються на всі системи;
- впровадження в режимі реального часу безпечних послідовних дій моніторингу безпеки;
- впровадження систем, які працюють автоматично для забезпечення органів управління необхідною інформацією з метою прийняття ефективних та економічно обгрунтованих рішень на основі ризиків ІС, які підтримують завдання та функції СБО;

– забезпечення об’єднання правил безпеки шляхом побудови захисту в єдину архітектуру;
– об’єднання ряду послідовних дій з управління ризиками на рівні ІС;
– встановлення відповідальності і наукового дослідження з супроводження та впровадження заходів безпеки в їх інформаційних системах.

Ризик ІБ — R це потенційна можливість використання активів конкретної загрози для заподіяння шкоди СБО. Вони характеризуються двома параметрами: втратами які можуть здійснитися та ймовірністю втілення їх реалізації. Аналізуючи ці дві характеристики дозволить порівнювати ризики з різними величинами шкоди і ймовірності, щоб вони мали зрозумілий вигляд для осіб, які приймають рішення з мінімізації ризиків в СБО. Аналіз ризиків ІБ дозволяє встановлювати необхідну і достатню сукупність заходів для зниження ризиків ІБ і відпрацювання структури її та максимально ефективну діяльність спрямовану на пониження саме її ІБ.

Управління ризиком полягає у пошуку компромісу між витратами на зменшення імовірності виникнення небезпечної події або збитку від неї і тією вигодою, яку приносить використання небезпечних технологій, матеріалів, продуктів тощо.

Очікуване значення результату небезпечної (ризикованої) діяльності є середньо виваженим усіх можливих результатів і розраховується за формулою (1) [11].

$$E = \sum_{i=1}^{n} P_i \times X_i \quad (1)$$

де *P, X* — відповідно ймовірність і значення *i*-го результату, *n* — кількість можливих результатів.

На наш погляд під час управління ризиками ІБ необхідно визначати наступне:

– загальну кількість способів захисту інформації;
– організацію проведення аудиту;
– можливість не допущення або зменшення непотрібних ефектів;
– шляхи постійного вдосконалення ІБ;
– ризики та можливості, на які необхідно зосереджувати увагу щоб система управління ІБ цього сектору можна досягти запланованого рівня.

Органи управління СБО повинні планувати дії, які стосуються цих ризиків та можливостей шляхом інтегрування й упровадженням їх до послідовних змін системи управління ІБ та оцінювати ефективність цих дій.

Для більш ефективного, своєчасного та якісного планування управління ризиками ми пропонуємо використовувати методику управління ризиками [4], що викладена на рис. 1, виходячи з того, що виявлення різних ризиків — це імовірність того, що відбуваються події які небажані і можливо погано вплинуть на те щоб досягти мети СБО. Обчислення ризику здійснюється за формулою (2) [11].

$$R = Rp * Rз, \quad (2)$$

де *R* — ризик ІБ, *Rp* — реалізація ризику ІБ, *Rз* — збиток ІБ.

При цьому вмовірність реалізації ризиків *Ppp* обчислюється за формулою (3) [11].

$$Rpp = Rз * Ry \quad (3)$$

де *Rз* — реалізація загрози ІБ, *Ry* — реалізацію уразливості ІБ.

На етапі обчислення ризиків для кожного інформаційного активу визначаються вимоги щодо забезпечення ІБ за шкалою від «1» до «7», де значення «1» відповідає мінімально необхідному набору заходів забезпечення ІБ, а значення «7» відповідає максимальному. На рис. 1 представлено методику управління ризиками ІБ.

ISSN 2663 - 4023

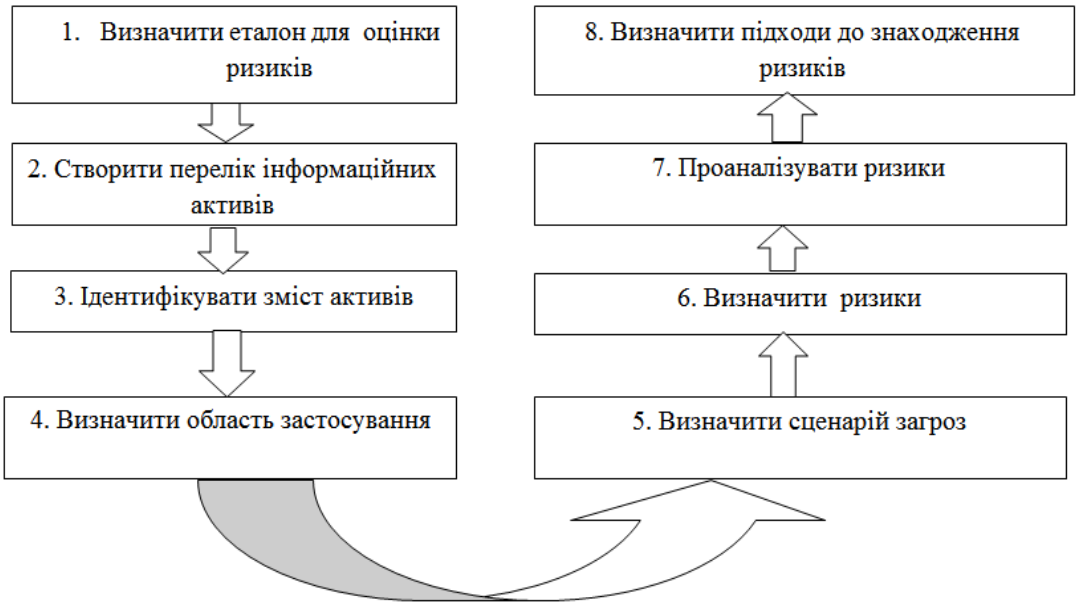

Рис. 1. Методика управління ризиками ІБ

Перевага цієї методики зводиться до того, що вона найбільш проста для проведення заходів з оцінки ризиків (ОР). До показників зазначеної методики відносяться наступне:

- спроможність пристосування методу ОР до бажання, всіх військових формувань та органів, в залежності від її типу і розміру;
- наявність умов одержувати, в підсумку, результати якісних та кількісних показників;
- програми, які втілюють положення методики;
- гнучке реагування під час її застосування.

Отже використовуючи методику управління ризиками інформаційної безпеки посадові особи, на наш погляд, повинні визначати та застосовувати наступний хід оцінювання ризиків ІБ. Встановлювати і підтримувати еталони ризиків ІБ, які містять наступні заходи:

- аналіз критеріїв визначення ризиків;
- еталони для ризиків ІБ;
- гарантію того, що оцінки ризиків ІБ які повторюються призводять до послідовних, ефективних та порівняльних результатів;
- ототожнення ризиків ІБ;
- хід оцінювання ризиків ІБ для ідентифікації ризиків, поєднаних з властивістю, яка не підлягає розголосові, цілісності і доступності в межах сфери застосування системи управління інформаційною безпекою (СУІБ) здійснює аналіз ризиків ІБ;
- оцінює можливі результатів визначення ідентифікованих ризиків;
- оцінює фактичну ймовірність ризиків, які можуть вплинути на здатність СБО виконувати завдання і функції для досягнення мети (місії) та цілей;
- визначає рівні ризику тобто добуток від ймовірності виникнення небезпеки на очікуваний розмір шкоди (збитку), що може завдати реалізована небезпека;
- оцінює потенційну можливість використання вразливостей активів конкретної загрози для заподіяння шкоди військовим формуванням та їх органів. При цьому порівнює результати аналізу ризиків з визначеними

еталонами та визначає пріоритети проаналізованих ризиків для їх опрацювання. Але необхідно зазначити, що зміст та склад зазначених послідовних дій залежить від використання в СБО викладеної нами методики згідно рис. 1.

Методи оцінювання ризиків можуть бути якісні, кількісні та комбіновані. Якісна оцінка застосовується для того щоб отримати добуток від ймовірності виникнення небезпеки на очікуваний розмір шкоди (збитку), що може завдати реалізована загроза — Rз. (Згідно з ДСТУ 2293-99) (4) [12] – [14]

$$Rз = P*Z \quad (4)$$

де *P* — ймовірність виникнення небезпеки, *Z* — очікуваний розмір шкоди (збитку), що, може завдати реалізована небезпека.

Оскільки ймовірність — величина безрозмірна, ризик має вимірюватися в одиницях шкоди (збитку), заподіяної небезпекою. Пропонується розглянути комплексний підхід для оцінки військової інформації (ВІ) СБО. Для зручності використовується вектор Z [15], [16], створений з компонентів актуальних оцінок ВІ, кожний з яких може стати надважливим. Розглянемо вектор компонентів цінності ВІ — {*Z0, Z1, Z2, Z3, Z4, Z5*} і використати наступні компоненти вектора оцінки ВІ:

- *Z0* — ЕО вартості вхідних даних для створення ВІ;
- *Z1* — ЕО вартості здобутків або втрат під час втілення сценарію, закладеного у ВІ;
- *Z2* — ЕО вартості інсайдерського заволодіння, купівлі або викрадення ВІ;
- *Z3* — ЕО вартості технічного перехоплення ВІ;
- *Z4* — ЕО вартості технічного захисту ВІ;
- *Z5* — ЕО вартості створення ВІ.

Розглянемо всі компоненти вектора ВІ — {*Z0, Z1, Z2, Z3, Z4, Z5*}, які потрібно розраховувати під час життєвого циклу (далі — ЖЦ) ВІ [16] згідно з нижче наведеною з компонентів ВІ.

Z0 — вхідний компонент вектора ВІ, який визначає витрати, необхідні для отримання вхідної інформації. Вхідна інформація згідно з формулою (5) складається з наступних складових:

$$Z_0 = C_З + C_{РД} + C_{НДР,\ ДКР} \quad (5)$$

де $C_З$ — кошторис створення задуму, $C_{РД}$ — кошторис затрат на здобуття розвідданих, $C_{НДР,\ ДКР}$ — кошторис затрат на проведення НДР та ДКР.

Z1 — перший компонент вектора ВІ СБО — це сумарна вартість в доларовому еквіваленті всіх матеріальних ресурсів та дій з ними, які заплановані у ВІ згідно з формулами (6), (7).

Масив інформації $V_{ВІ1}$ визначають описом суб'єктів СБО та описом запланованих дій з ними за формулою (6):

$$V_{ВІ1} = f\,(OBT_n,\ OC_S,\ Км^2,\ O_l,\ d_{n,s}) \quad (6)$$

Цінність ВІ — *Z1* визначимо сумою вартості всіх суб'єктів сценарію ВІ та вартості дій з ними в доларовому еквіваленті [15] – [16] згідно з формулою (7):

$$Z_1\,(t) = \sum C_{OBTn}\,(t) + \sum C_{\ OCs}(t) + \sum CКм^{\,2}(t) + \sum C_{Ol}(t) + \sum d_{n,s}(t) \quad (7)$$

де $V_{ВІ1}$ — масив ВІ, *t* — час здійснення оцінки ВІ, *C* — коштовність суб'єктів ВІ, OBT_n — перелік зразків *n* ОВТ, задіяних у сценарії ВІ, OC_S — перелік особового складу *s*, задіяного у ВІ, $Км^2$ — обсяги територій, задіяні у ВІ, O_l — підприємства, розміщені на територіях, задіяних у ВІ, $d_{n,s}$ — дії з OBT_n та OC_S.

Z2 — другий компонент вектора ВІ СБО, визначений сучасними підходами до оцінки вартості інформації, придатними для військової справи. Це дуже важливий

варіант сценарію, який враховує витрати противника в доларовому еквіваленті, необхідні для інсайдерського заволодіння ВІ згідно з формулою (8):

$$Z_2 = C_{СУ} + C_{ОВД} \quad (8)$$

де $C_{СУ}$ — вартість утримання противником спеціальної установи, $C_{ОВД}$ — затрати противника на операцію з отримання ВІ.

Z3 — третій компонент вектора ВІ СБО визначено необхідністю враховувати загрози технічного, кібернетичного або криптографічного перехоплення ВІ противником. Компонент враховує витрати противника в доларовому еквіваленті, необхідні для заволодіння ВІ технічним шляхом згідно з формулою (9):

$$Z_3 = C_T + C_K + C_{Kp} \quad (9)$$

де C_T — вартість технічного перехоплення ВІ, C_K — вартість кібернетичного перехоплення ВІ, C_{Kp} — вартість криптографічного розкриття перехопленої ВІ.

Z4 — четвертий компонент вектора ВІ СБО визначено необхідністю враховувати затрати в доларовому еквіваленті, необхідні на технічний, кібернетичний та криптографічний захист ВІ згідно з формулою (10):

$$Z_4 = C_{TЗ} + C_{KЗ} + C_{KpЗ} \quad (10)$$

де $C_{TЗ}$ — вартість технічного захисту ВІ, $C_{KЗ}$ — вартість кібернетичного захисту ВІ, $C_{KpЗ}$ — вартість криптографічного захисту ВІ.

Z5 — п’ятий компонент вектору ВІ СБО визначає витрати в доларовому еквіваленті, необхідні для створення ВІ в штабі згідно з формулою (11):

$$Z_5 = C_{Ш} + C_{ОС} + C_З \quad (11)$$

де $C_{Ш}$ — вартість роботи інфраструктури штабу, $C_{ОС}$ — вартість роботи особового складу штабу, $C_З$ — вартість збереження ВІ.

Натомість об’єкту оцінки надається показник в порядку надання їм переваги за трибальною (низький, середній високий), п’ятибальною чи десятибальною шкалою (0…10). Для того щоб зібрати дані під час якісної оцінки ризиків необхідно залучити опитування цільових груп, інтерв’ювання, анкетування.

В межах кількісної оцінки, ризик — $R_К$ розглядається як комплексна величина і він залежить від таких показників — загрози, вразливості, збитки (12).

$$R_К = \lambda * P_t * P_v(z) \quad (12)$$

де z — витрати на забезпечення захисних заходів, λ — величина збитків від порушення безпеки будь-якої інформації, яка має цінність для СБО, P_t — імовірність виникнення загрози ІБ, $P_v(z)$ — функція ймовірності реалізації загроз для будь-якої інформації в залежності від витрат.

Кількісна оцінка ризиків може визначатися декількома етапами:

- визначити цінність будь-якої інформації;
- встановити кількісну оцінку потенційних збитків в залежності від реалізації тієї чи іншої загрози відносно будь-якої інформації;
- визначити ймовірність реалізації узятої окремо загроз ІБ.

Отже, величина збитків, залежить як від інформації що підлягає захисту так і від заданої імовірності здійснення загрози. Ці ймовірності можуть бути суттєво знижені завдяки надання інвестицій в ІБ активу, використовуючи опрацювання і аналіз кількісних даних, опитування персоналу. В ході знаходження ймовірності, тобто числової характеристики можливості того, що випадкова подія відбудеться в умовах, які можуть бути відтворені необмежену кількість разів, необхідно:

- підрахувати частоту появлення випадків поєднаних з реалізацією загроз ІС за визначений період (наприклад — за один рік);

– визначити загальний можливий збиток від кожної загрози, щодо кожного активу за визначений період.

Це розраховується шляхом добутку разової шкоди від виявлення загрози на частоту виявлення цієї загрози та проводиться аналіз даних, які були отримані щодо збитку для кожної загрози.

Ідентифікація еталонів ризику означає — прийняти рішення відносно характеру можливих наслідків і способу їх вимірювання. При визначенні еталонів необхідно визначити, за якими еталонами будуть прийматися рішення щодо необхідності оброблення ризику та еталони, за якими будуть прийматися рішення відносно допустимості або прийняття ризику.

Наявні на сьогодні методи оцінки ризиків в переважній більшості засновані на збиранні, організуванні, аналізі, інтерпретуванні та представленні даних, тобто на статистичних підходах. Після того, коли буде завершено їх загальне оцінювання проводять оброблення ризику, це передбачає прийняття заходів, які дозволяють зменшити ймовірність виникнення ризиків та їх вплив на ІС.

Проведені дослідження дозволяють сформувати критерії вибору методів оцінки і управління ризиками ІБ [5] – [7]. Поряд з сформуванням питань з оцінки і управління ризиками ІБ, необхідно сформувати показники оцінювання рівня захисту інформації. Питанню формування показників та критеріїв оцінювання рівня ІБ присвячені роботи не одного науковця, при цьому зазначимо, що вони в деякій мірі відображають свої підходи до оцінювання рівня захисту інформації по різному і розглядують до чотирьох напрямків діяльності інформаційної безпеки. Сьогодні, всі заходи які впливають на рівень ІБ, в межах інформації зростають у зв’язку з появою нових видів загроз в інформаційному просторі нашої держави, зокрема і військового характеру. Ми ж зупинимося на заходах інженерного захисту інформації та на рівні кваліфікації і надійності особового складу (персоналу) за напрямками.

Інженерні заходи захисту інформації, це заходи, які попереджають руйнування носія інформації внаслідок навмисних дій або природного вплив.

Оцінка з інженерного захисту інформації залежить від заходів вказаних в табл. 1.

Таблиця 1

Інженерні заходи захисту інформації

№ п/п	Інженерні заходи захисту інформації
1	Перевірка оснащення охоронною сигналізацією та відповідність їх типів і видів встановленим вимогам.
2	Перевірка наявності автоматичної пожежної сигналізації
3	Перевірка справності різних замків, ключів згідно встановлених норм.
4	Наявність попереджувальних знаків
5	Перевірка наявності внутрішніх засовів, гратів згідно встановленим нормам
6	Перевірка встановлених таких засобів захисту, як електронних, оптичних, акустичних.
7	Перевірка відповідності мінімальної площі приміщень.
8	Перевірка наявності та відповідності нормам площі робочого місця з обслуговування, ремонту та налагодженні ПЕОМ.
9	Наявність та відповідність стін, перегородок визначеним нормативним даних.
10	Відповідність встановлених дверей до норм та їх порядок укріплення.
11	Перевірка заземлення та відповідність їх встановленим нормам.
12	Перевірка справності електропроводки, виключателів, розеток згідно встановлених норм.

Враховуючи кожен із зазначених заходів та встановивши факт його виконання можна оцінити рівень інженерного захисту інформації користуючись табл. 2.

Таблиця 2

Оцінка рівня інженерного захисту інформації

Пункт заходу	1	2	…	11	12
Фактичне виконання	+	–	+	+	–
Оцінка(Scientific assessment) S_a	1	0	1	1	0

Згідно зазначеного експертного оцінювання — нормована оцінка інженерного забезпечення захисту інформації $K_з$ знаходиться за формулою (13) [11] – [13]

$$K_з = \frac{\sum_{i=1}^{N\text{ci}} S_a}{N_c} \quad (13)$$

де $K_з$ — оцінка інженерного забезпечення захисту інформації, N_c — кількість перевірених пунктів, S_a — наукова оцінка фактів виконання пунктів заходу.

Крім експертного оцінювання засобів інженерного захисту інформації важливо визначити і нормативну оцінку рівня кваліфікації надійності персоналу. Ця оцінка залежать від спроможності її персоналу якісно виконувати заходи з порушень інформаційної безпеки вказаних в табл. 3.

Таблиця 3

Заходи порушень ІБ, що залежать від спроможності персоналу

№п/п	**Заходи**
1	Компрометація облікового запису системи (сервісу), в тому числі в результаті крадіжки паролю зловмисником.
2	Компрометація системи, в тому числі в результаті експлуатації вразливості або роботи ШПЗ, що дозволяє віддалене керування.
3	Несанкціоноване підключення пристрою до інформаційно-комунікаційної системи, в тому числі цифрової радіостанції до системи цифрового радіозв'язку.
4	Порушення порядку доступу до інформації в системі, в тому числі в результаті експлуатації вразливості або роботи ШПЗ.
5	Відмова в обслуговуванні або порушення сталого функціонування сервісу (об'єкта ІТС) в результаті DoS-, DDoS-атаки, помилкових дій користувачів, відключення електричної енергії тощо.
6	Виявлення шкідливого програмного засобу, що не дозволяє віддалене керування та не несе загрози цілісності і конфіденційності та/або доступності інформації.
7	Виявлення спроб використання зловмисником вразливостей програмного забезпечення, невдалих спроб автентифікації в системі, в тому числі в системі цифрового радіозв'язку.
8	Розсилання зловмисником повідомлень з метою крадіжки пароля Користувача.
9	Несанкціонований доступ до ресурсів системи шляхом використання прав іншого об'єкта (несанкціоноване використання NAT, підміна MAC-адреси).
10	Несанкціоноване використання програмного забезпечення, що втручається в роботу комплексу засобів захисту.
11	Порушення порядку використання ресурсів (використання не за призначенням, у несанкціонованих цілях), в тому числі обробка інформації в АС без створення КСЗІ з підтвердженою відповідністю, обробка інформації з обмеженим доступом в АС, що призначена для обробки відкритої інформації, передача інформації з обмеженим доступом в мережі Інтернет, в автоматизованій системі управління Збройних Сил України «Дніпро», по відкритих телефонних мережах.
12	Відсутність критичного оновлення безпеки програмного забезпечення (прошивки телекомунікаційного обладнання).
13	Порушення порядку підключення автоматизованої системи до мережі Інтернет.

14	Порушення встановлених правил розмежування доступу, в тому числі використання пароля (SNMP community, ключа шифрування системи цифрового радіозв'язку) понад встановлений термін або такого, що не відповідає визначеним вимогам безпеки.
15	Використання свідомо уразливого протоколу, режиму роботи, налаштувань обладнання або програмного забезпечення при передачі паролів, іншої чутливої інформації.
16	Несанкціоноване використання програмного забезпечення, що збільшує ризик порушення безпеки інформації, в тому числі отриманого з недостовірних джерел.
17	Помилкові дії або бездіяльність користувача, що призводять до збільшення ризику порушення безпеки інформації цифрових систем радіозв'язку, а саме: робота передавача на випромінювання в період радіомовчання, робота радіозасобів без зміни радіоданих під час переміщення пунктів управління (вузлів зв'язку), спотворення форми сигналу на виході передавача.
18	Використання та поширення конфіденційної інформації правопорушником про особу.
19	Збір інформації правопорушником про склад інформаційно-комунікаційних систем, існуючих вразливостей, в тому числі нетехнічними засобами.

Враховуючи кожен із зазначених в табл. 3 заходів можна оцінити рівень кваліфікації надійності персоналу користуючись табл. 4.

Таблиця 4

Оцінка рівня кваліфікації персоналу

Пункт заходу	1	2	3	...	15	18
Факт виконання	+	+	+	+	+	+
Оцінка (Scientific assessment) C_i	1	0	1	0	1	1

Оцінка рівня надійності персоналу розраховується за формулою (14) [12] – [13].

$$K_н = 0.2\,\frac{\sum_{i=0}^{n_{ci}} c}{N_c} + K_{ДРн} + K_{НПн} + K_{ППн} + K_{КПн} \qquad (14)$$

де N_c — кількість перевірених пунктів згідно таблиці 2, $K_{ДРн}$ — нормативний коефіцієнт досвіду роботи персоналу, $K_{НПн}$ — нормативний коефіцієнт надійності персоналу, $K_{ППн}$ — нормативний коефіцієнт підготовленості персоналу до розпізнання загроз інформаційної безпеки, $K_{КПн}$ — нормативний коефіцієнт компетентності персоналу.

$$K_{ДР_н=}\ \frac{n}{N} \qquad (15)$$

де n — чисельність фахівців які мають доступ до інформаційних систем, що працюють більше одного року на конкретній інформаційній системі, N — загальна кількість фахівців які мають доступ до баз даних на конкретній інформаційній системі.

$$K_{НП_н=\,1-}\ \frac{n_{в_i}}{N_{вс},} \qquad (16)$$

де $n_{нд}$ — численність персоналу відстороненого від роботи за витік інформації, $N_{вс}$ — загальна чисельність персоналу.

$$K_{ПП_н=\,1-}\ \frac{n_н}{N_д} \qquad (17)$$

де $n_{нд}$ — численність персоналу ненавмисні дії яких призвели до витоку інформації, $N_д$ — загальна чисельність персоналу що мають доступ до закритої інформації.

$$K_{КП_н=}\ \frac{n_{із}}{N_{із}} \qquad (18)$$

де $n_{із}$ — кількість інформаційних атак, що відвернуті через дії персоналу, який забезпечує інформаційну безпеку, $N_{із}$ — загальна кількість атак за певний проміжок часу.

Таким чином після тестування заходів вказаних в табл. 1, 3 від яких залежить інформаційна безпека і отримання нормативних оцінок табл. 3, 4 можна визначити комплексний показник інформаційної безпеки.

$$\sum_{i=1}^{n} W_i \, К_i \qquad (19)$$

де W_i — заходи від яких залежить інформаційна безпека $\sum_{i=1}^{n} W_i=1$, $K_i=[0,1]$ — оцінки рівня кваліфікації і надійності персоналу від 0,1.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі було досліджено та запропоновані — розрахунок очікуваного значення результату ризикованої діяльності та що необхідно визначати під час управління ризиками інформаційної безпеки, запропонована методика управління ризиками інформаційної безпеки, методи оцінювання ризиків як якісні так і кількісні та порядок визначення очікуваного розміру шкоди (збитку) військової інформації, сформовані інженерні заходи захисту інформації та заходи рівня кваліфікації і надійності персоналу та їх оцінки.

Дослідження дозволяють якісно оцінити ризики ІБ як з питань оцінки управління ризиками інформаційної безпеки СБО так і з формування рівня захищеності інформації.

В подальших дослідженнях доцільно провести порівняльний аналіз методів управління ризиками ІБ і на основі цього аналізу можливо було б стверджувати, що найбільш оптимальним варіантом для управління ризиками ІБ в межах забезпечення неперервності функціонування ІБ є адаптація та удосконалення відомих на сьогодні методів шляхом їх логічного поєднання з урахування переваг та мінімізації цих методів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Замула, А. А., Северинов, А. В., & Корниенко, М. А. (2017). Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. *Наука і техніка Повітряних Сил Збройних Сил України, 2(15),* 47–52.
2. Єжова, Л.Ф. (2010). *Управління інформаційною безпекою.* В 2-х томах. Том. 1. К.: Вид. ДУІКТ.
3. Замула, О. А. (2014). Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки. Збірних наукових праць. *Системи обробки інформації, 2(92),* 53–56.
4. *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC 27000:2009). (2009).
5. *Information technology. Security techniques. Information security incedent management* (ISO/IEC 27035). (2011).
6. *Information technology – Security techniques. Information security risk management* (ISO/ IEC 27005:2018). (2018).
7. Henry, K. (2017). Risk management and analysis. *Information Security Management Handbook, Part 1(28),* 321–329.
8. Alberts, C. J. (2018). Operationally Critical Threat, Asset and Vulnerability Evaluation.
9. *Guide for Conducting Risk Assessments. National Institute of Standards and Technology)* (200.332). (б. д.). Gaithersburg: National Institute of Standards and Technology.
10. *Risk Management Framework for Information Systems and Organizations.* (б. д.). NIST Special Publication 800-37, Revision 2. https://doi.org/10.6028/NIST.SP.800-37r2
11. Горбенко, А. Д., Замула, О. А., & Осипенко, Ю. С. (2022). Концепція оцінки ризиків кібербезпеки інформаційної системи об'єкта критичної інфраструктури. *Радіотехніка, (2)209,* 118–129. https://doi.org/10.30837/rt.2022.2.209.12

12. Журавель, М. Ю., Полозова, Т. В., & Стороженко, О. В. (2014). Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*, *33*, 171–177.
13. Кононова, В. О., Харкянен, О. В., Грибков, О. В. (2014). Оцінка засобів захисту інформаційних ресурсів. *Вісник Національного університету «Львівська політехніка». Компютерні системи та мережі, 806*, 99–105.
14. Гріньків, В. О. (2019). Методи кількісної оцінки стійкості системи зберігання даних. *Збірник наукових праць ВІТІ, 3,* 16–22.
15. Раимов, А. В. (2017). Экономическая оценка конфиденциальной информации организации. *Финансы и управление*, *1*, 1–9
16. Куцаєв, В. В., Орда, М. В., Зіборєва, О. Б., Головко О. Є., & Гришенко, Н. О. (2021). Цінність військової інформації. *Збірник наукових праць ВІТІ. МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку»*, *3*, 172–176.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Volodymyr Tkach
Senior Researcher, Research Department
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0003-0013-7368
Tkachwolodymyr@gmail.com

Oleksandr Shemendiuk
Head of Research Department
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-5594-2973
1o2l3d@gmail.com

Oleksiy Cherednychenko
Senior Researcher, Research Laboratory
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-0816-8321
n0ize@ukr.net

RESEARCH ON ISSUES OF INFORMATION SECURITY RISKS ASSESSMENT AND MANAGEMENT IN THE SECURITY AND DEFENSE SECTOR AND FORMATION OF SECURITY LEVEL INDICATORS

Abstract. It is known that the management of the security and defense sector includes various resources — information, personnel (staff), planning, training, conducting combat operations (operations), logistics and operational support. A well-known factor in increasing their viability is the effective use of information systems. In connection with the emergence of new threats that are constantly changing and circulating in information systems, a problem arose regarding the assessment and management of information security risks in the security and defense sector and the issue of forming indicators of the level of information security. The article proposes: the concept of RME, the feasibility of its implementation, the definition of information security risk, the calculation of the expected value of the result of risky activities and what needs to be determined when managing information security risks, the methodology for managing information security risks, methods for assessing risks, both qualitative and quantitative, and the procedure for determining the expected amount of damage (loss) to military information, engineering measures for information protection and measures for the level of qualification and reliability of personnel and their assessment. It should be noted that the above tasks can be achieved through the application of successful and effective risk management, clarification of the management bodies of the procedure for assessing information security, responsibilities for determining and applying the process of processing information security risks. It is assumed that the proposed studies on the assessment and management of information security risks, the formation of the level of information security, will allow determining the most appropriate approach to assessing the information protection system, which can be taken into account in practical work. The implementation of the planned approach will significantly improve the process of assessing information security risks, compare different harms and probabilities, form indicators and criteria for the level of information security and, as a result, can become the basis for assessing and managing risks and forming indicators for the level of information security.

Keywords: information security; information security management systems; risk assessment and management; risk assessment and management methodologies; formation of security indicators.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zamula, A. A., Severinov, A. V., & Kornienko, M. A. (2017). Analysis of models of information security risk assessment for building an information security system. *Science and Technology of the Air Force of the Armed Forces of Ukraine, 2(15),* 47–52.
2. Yezhova, L. F. (2010). *Information Security Management.* In 2 volumes. Vol. 1. Kyiv: Publishing House of DUICT.
3. Zamula, O. A. (2014). Analysis of international standards in the field of information security risk assessment Collected scientific works. *Information processing systems, 2(92),* 53–56.
4. *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC 27000:2009). (2009).
5. *Information technology. Security techniques. Information security incedent management* (ISO/IEC 27035). (2011).
6. *Information technology – Security techniques. Information security risk management* (ISO/ IEC 27005:2018). (2018).
7. Henry, K. (2017). Risk management and analysis. *Information Security Management Handbook, Part 1(28),* 321–329.
8. Alberts, C. J. (2018). Operationally Critical Threat, Asset and Vulnerability Evaluation.
9. *Guide for Conducting Risk Assessments. National Institute of Standards and Technology)* (200.332). (б. д.). Gaithersburg: National Institute of Standards and Technology.
10. *Risk Management Framework for Information Systems and Organizations.* (n. d.). NIST Special Publication 800-37, Revision 2. https://doi.org/10.6028/NIST.SP.800-37r2
11. Gorbenko, I., Zamula, O., & Osipenko, Y. (2022). The concept of assessing the risks of cybersecurity of the information system of the critical infrastructure object. *Radiotekhnika, 2(209),* 118–129. https://doi.org/10.30837/rt.2022.2.209.12
12. Zhuravel, M. Yu., Polozova, T. V., & Storozhenko, O. V. (2014). Formation of a system of indicators for assessing the level of information security of an enterprise. *Bulletin of the Economy of Transport and Industry, 33,* 171–177.
13. Kononova, V. O., Kharkyanen, O. V., & Hrybkov, O. V. (2014). Assessment of means of protecting information resources. *Bulletin of the National University "Lviv Polytechnic". Computer systems and networks, 806,* 99–105.
14. Grinkov, V. O. (2019). Methods for quantitative assessment of the stability of a data storage system. *Collection of scientific works of VITI, 3,* 16–22.
15. Raimov, A. V. (2017). Economic assessment of confidential information of the organization. *Finance and management, 1,* 1–9.
16. Kutsaev, V. V., Orda M. V., Ziboreva, O. B., Golovko, O. E., & Grishenko, N. O. (2021). The value of military information. Collection of scientific papers of MITIT. *INTERNATIONAL SCIENTIFIC AND TECHNICAL CONFERENCE "Systems and technologies of communication, informatization and cybersecurity: current issues and development trends", 3,* 172–176.