УДК 004.056

Алексєєв М. М.

Національний університет оборони України імені Івана Черняховського, Київ

Методика кількісного оцінювання інформаційних ризиків із застосуванням онтології факторного аналізу

Резюме. У статті розглянуто методику кількісного оцінювання інформаційних ризиків. У системі забезпечення кібернетичної безпеки ризик, головним чином, асоціюється з "втратою даних". Запропоновано модель ризику під час використання онтології факторного аналізу інформаційних ризиків. У процесі побудови моделі ризику використано такі складові, як частота події, що викликає втрати, та магнітуда втрати.

Ключові слова: факторний аналіз; інформаційні ризики; розрахунок ризику; частота події, що викликає втрати; магнітуда втрати.

Постановка проблеми. На відміну від вже звичної схеми розвитку загроз (наприклад, у військовій сфері), розвиток кіберзагроз відбувається за іншою логікою. У момент виявлення впливу загрози вона вже може спричинити суттєві негативні наслідки. До того ж оперативність роботи системи кібернетичної безпеки, зазвичай, суттєво відстає від темпів зростання матеріальних і нематеріальних збитків від реалізації загрози.

Крім того, до кіберзагроз дуже важко застосовувати концепції стримування та запобігання, оскільки під час підготовки і здійснення кібератак, насамперед, забезпечується анонімність атакуючого. Отже, виникає об'єктивна необхідність проактивного, тобто випереджувального вживання заходів з нейтралізації кіберзагроз.

Для нейтралізації кіберзагроз у світовій практиці успішно використовується теорія управління ризиками, або ризик-менеджменту, яка, на жаль, ще рідко застосовується в українських реаліях. Відповідно до кращих сучасних практик кіберзахисту, оптимальна безпека досягається за допомогою безперервного процесу ідентифікації, оцінювання ризиків та постійної підтримки процесів безпеки у поєднанні з усуненням вразливих місць.

Аналіз останніх досліджень і публікацій. Набуття спроможностей фахівцями ЗС України з ефективного реагування на сучасні кіберінциденти та виклики є актуальним завданням сьогодення. З цією метою 27 січня 2020 року у Військовому інституті телекомунікацій та інформатизації імені Героїв Крут розпочались трьохмісячні початкові курси з кіберзахисту для офіцерів підрозділів та частин військ зв'язку ЗС України. Планується, що курс донесе до слухачів результати досліджень та досвід європейських організацій SANS, MITRE, NIST у забезпеченні кібербезпеки на об'єктах критичної інфраструктури держави, зміцненні у військах єдиного розуміння принципів побудови системи кібербезпеки і основ кіберзахисту [1].

Питання створення, розвитку та захисту кібернетичного простору військової сфери України досліджувалися В. Кацалапом, П. Сніцаренком, Ю. Саричевим, О. Устименком [2–4]. Модель оцінювання вразливостей систем з критичною кібернетичною інфраструктурою досліджували В. Телелим, Ю. Даник та А. Зінченко [5].

Крім того, науковцями Центру воєнно-стратегічних досліджень під час розроблення військового стандарту "Інформаційна безпека держави у воєнній сфері. Терміни та визначення" визначено сутність понять "загроза інформаційна", "загроза кібернетична" [6], а під час розроблення військового стандарту "Воєнна безпека. Стратегічне планування. Терміни та визначення" визначено сутність понять "живучість", "захист", "кібербезпека", "кіберзахист" [7].

Проте у вказаних джерелах недостатньо уваги приділено розробленню підходів щодо оцінювання інформаційних ризиків для формування випереджальних заходів забезпечення кіберзахисту.

Стаття присвячена удосконаленню методики кількісної оцінки ризиків, яка використовує методи факторного аналізу інформаційних ризиків (ФАІР) шляхом їх декомпозиції, математичний апарат імітаційного моделювання, та дає змогу приймати більш виважені та обґрунтовані рішення щодо попередження настання

негативних наслідків у разі реалізації визначених кібернетичних загроз.

Метою статті є висвітлення методики кількісного оцінювання інформаційних ризиків із застосуванням онтології факторного аналізу.

Виклад основного матеріалу. Факторний аналіз інформаційних ризиків (ФАІР) дає змогу впровадити добре обґрунтовану логічну схему кількісного оцінювання ризику. В основу її покладені такі елементи.

1. *Онтологія факторів*, з яких складається ризик, та їх взаємовідносини. Ця онтологія визначає фундаментальне розуміння ризику, без якого не можливі подальші дії. Вона також впроваджує набір стандартних дефініцій для таких ключових термінів, як ризик, загроза, вразливість та ін.

2. *Методи вимірювання* основних факторів, які впливають на ризик.

3. *Обчислювальний апарат*, необхідний для того, щоб розрахувати ризик, використовуючи математичну імітацію взаємовідносин між факторами, які вже були виміряні.

4. Конструкція моделі, яка дає змогу побудувати та проаналізувати ризикові сценарії практично будь-якого розміру та складності, використовуючи онтологію, вимірювання та відповідний обчислювальний апарат.

Безумовно головним ключовим терміном ФАІР є *"ризик",* який визначається як імовірна частота та ймовірна магнітуда майбутніх втрат. Тобто як часто трапляються втрати та яким може бути результат цих втрат.

До того ж необхідно розуміти, що одним із проблемних питань під час визначення складових ризику, є різниця між такими дефініціями, як імовірність та частота. Автори ФАІР [8] наполягають на тому, що для прийняття якісного рішення під час оцінювання ризику визначальним є прив'язка його параметрів до шкали часу. Тобто підрахунок конкретний подій у визначений часовий проміжок (зазвичай – 1 рік) несе більше корисного навантаження ніж імовірність згаданої події, оскільки у безкінечності ймовірність будь-якого реального ризику зростає до 100 %.

З іншого боку, частота також має свій ліміт. Її не можна використовувати, коли подія відбувається лише один раз. Водночас, є достатньо легкий спосіб визначання частоти, маючи значення ймовірності. Наприклад, якщо ймовірність події дорівнює 5 %, то у масштабі часу "рік" це еквівалентно частоті 1 раз у 20 років.

Іншим важливим елементом ФАІР є "*загроза*", яка визначається як об'єкт, субстанція, людина тощо, яка здатна діяти у спосіб, який може призвести до нанесення шкоди. Ключовим є той факт, що актор (агент) має потенцію для створення передумов до настання події з негативними наслідками (викликати втрати). Наприклад, калюжа на підлозі не є загрозою у цьому розумінні, вона лише збільшує ймовірність настання негативних наслідків (випадкового падіння, або удару електричним струмом).

Наступним ключовим терміном є "*вразливість*". Не зважаючи на прийняте визначення вразливості як "слабкість системи, що може бути використана загрозою", у ФАІР, подібно терміну "ризик", вразливість розглядається як значення, але не конкретна річ. Не можна вказати на щось і заявити, що це є вразливість. Усе, на що ми здатні, це вказати на конкретну політику безпеки та зазначити, що відповідні умови (обставини) збільшують нашу вразливість.

Повертаючись до онтології ФАІР слід зазначити, що вона репрезентує модель роботи ризику, визначаючи головні фактори, які його формують, та взаємовідносини між ними. Так само ці взаємовідносини можуть бути описані математично, що дає змогу вирахувати ризик вимірюючи та оцінюючи відповідні фактори, з яких він складається.

Також додатковою перевагою запровадження онтології ФАІР є той факт, що послідовні та логічні дефініції, з яких вона складається, здатні якісно поліпшити та спростити комунікації як між фахівцями з управління ризиками, так і з посадовцями, які безпосередньо відповідають за прийняття рішення.

У системі забезпечення кібернетичної безпеки ризик, головним чином, асоціюється з "втратою даних". З огляду на викладене, ризик складається з імовірної **частоти** та ймовірної **магнітуди** майбутніх втрат. До того ж імовірнісний характер складових ризику в більшості випадків пов'язаний з недосконалістю моделей, що використовуються та недостатньою кількістю та якістю вхідних даних.

Зважаючи на наведене, першими двома факторами визначаються: *частота події, яка викликає втрати* (ЧПВВ) та *магнітуда втрати* (МВ).

У цьому випадку ЧПВВ – це як часто, у визначений період часу, може бути

матеріалізована втрата внаслідок дій загрозливого агента. До того ж, як вже зазначалось, у практиці ФАІР визначений період часу, зазвичай, становить 1 рік.

Як приклад ЧПВВ можуть бути такі:

вихід з ладу дата-центру внаслідок екстремальних погодних умов;

знищення або пошкодження бази даних;

виток (викрадення) чутливих персональних даних клієнтів.

ЧПВВ може бути розрахована безпосередньо з наявних даних, або отримана внаслідок подальшої декомпозиції на дві складові: *частота загрозливих подій* (ЧЗП) та *вразливості системи* (В). В обох випадках ЧПВВ, зазвичай, виражається як розподілення (наприклад, між 5 та 25 разів на рік, з найбільшою ймовірністю 10 разів на рік).

ЧЗП – це як часто, у визначений період часу, загрозливий агент діятиме у спосіб, який може спричинити втрати.

З першого погляду ЧПВВ та ЧЗП мають майже тотожні дефініції. Проте між ними існує принципова різниця: чи будуть втрати внаслідок загрозливої події, чи ні. Наприклад, хакерська атака на сервер є загрозливою подією. Проте подія, що викликає втрату, виникає лише у разі настання деструктивних наслідків (викрадення інформації, перешкоджання роботі обчислювальної системи, зараження програмного забезпечення шкідливим кодом).

Отже, ймовірність реалізації загрозливої події є функцією вразливості.

ЧЗП, зі свого боку, також може бути оцінена або безпосередньо, або через подальшу декомпозицію на дві складові: *частота контактів* (ЧК) та *ймовірність акції* (ІА).

Частота контактів (ЧК) – це ймовірна частота, у визначений проміжок часу, з якою загрозливий агент входитиме в контакт з активом. До того ж контакт може бути фізичним, або віртуальним (за допомогою комп'ютерної мережі). Відповідно до моделі контакт може бути трьох типів:

випадковий – загрозливий агент випадково контактує з активом, наприклад, стихійне лихо;

регулярний – контакт відбувається на регулярній основі, наприклад, прибирання серверних кімнат кліринговим складом;

наполегливий – загрозливий агент цілеспрямовано намагається дістатися активу, наприклад, хакер вживає заходи, спрямовані на отримання несанкціонованого доступу до комп'ютерних баз даних.

Зі свого баку ІА визначає ймовірність, з якою *загрозливий агент* (ЗА) впливатиме на актив, коли контакт між ними відбудеться. Важливо зазначити, що ІА використовуються лише у разі, коли ЗА є суб'єктом, здатним приймати рішення. До того ж вибір зазначеного суб'єкта залежить від трьох факторів:

сприйнята цінність такого акту з погляду ЗА;

сприйнятий рівень зусиль та (або) ціна такого акту з погляду ЗА;

сприйнятий рівень ризику для ЗА, наприклад, імовірність бути спійманим (викритим) та отримання неприйнятних для ЗА наслідків.

Слід зазначити, що у практиці застосування ФАІР отримання результатів ЧЗП за допомогою визначення ЧК та ІА не є типовим. Проте це достатньо часто буває корисним під час прийняття оптимального рішення за наявністю розбіжностей між оцінками окремих аналітиків.

Також розуміння факторів, які впливають на ІА, важливі під час планування та застосування політики контролю у визначеній системі безпеки. Так, зменшення видимої цінності активу, підвищення рівню зусиль, потрібних ЗА для впливу на актив, та (або) збільшення ризиків для ЗА здатні зменшити ІА, що, зі свого боку, зменшує ЧЗП.

Вразливість (В) – це ймовірність того, що результатом дій ЗА стануть втрати.

З усіх термінів ФАІР таке визначення В має найбільшу відмінність від загальноприйнятого поняття. Так, часто відкрите вікно або ненадійний пароль називають вразливістю, маючи на увазі, що ці умови являють собою слабкі місця, які можуть бути використані ЗА.

Водночас, такі міркування можуть призвести до хибних висновків. На практиці багато хто схиляється до думки, що зачинене вікно або складний пароль не є вразливими. Насправді різниця в обох випадках полягає лише у рівні зусиль, потрібних ЗА.

Тому, з погляду ФАІР, вразливість – це ймовірність, з якою дії ЗА призведуть до втрат.

Наприклад:

цей будинок має 100 % вразливість для торнадо;

цей замок має 10 % вразливість для "професійного" крадія;

цей пароль має 1 % вразливість для "brute force" атаки.

Вразливість може бути розрахована безпосередньо, або бути похідною від таких складових, як *потенціал загрози* (ПЗ) та *рівень складності загрози* (РС).

Потенціал загрози. У попередніх версіях ФАІР ПЗ визначався як рівень сили, яку ЗА може застосувати. Це, безумовно, вірно у разі оцінювання ризикових сценаріїв, коли як ЗА виступає зловмисник або природне лихо. Однак на практиці доволі часто необхідно оцінювати ситуації, пов'язані з людськими помилками. У такому разі мова йде не про потужність, але скоріше про навички та/або ресурси (до речі ті ж самі фактори можуть працювати у разі оцінювання впливу на систему безпеки зловмисного актора). З огляду на викладене дефініція для ПЗ має бути більш узагальненою.

Оцінювання ПЗ може стати найскладнішим елементом аналізу. Це пов'язане з тим, що більшу частину часу аналітик змушений мати справу з найбільш невизначеними факторами, такими як людські знання та досвід. Для вирішення викладеного питання у ФАІР вводиться поняття відносної шкали (від 1 до 100), що має назву "ПЗ континуум". Тобто найменше значення ПЗ дорівнює 1 та, відповідно, найбільше значення буде 100. Так, наприклад, у разі оцінювання зловмисного сценарію, коли як ЗА визначені кіберзлочинці, які, безумовно, мають відповідні ресурси та високій рівень навичок, ПЗ визначається в діапазоні від 60 до 100, з найбільш імовірним значенням 90. Окрім зазначеного відповідна концепція оцінки ПЗ може бути застосована під розгляду сценарію, коли як ЗА виступає програміст, який ненавмисно припускається програмних помилок під час написання коду. У такому разі ПЗ високопрофесійного програміста із значними обчислювальними ресурсами також перебуватиме на вершині континууму.

З викладеного випливає логічне загальне припущення: високий рівень ПЗ для сценарію за участю зловмисника необхідно зменшувати (зменшуючи таким чином В), та навпаки у випадку сценарію, пов'язаного з помилками програміста рівень ПЗ потрібно збільшувати (зменшуючи В).

Рівень складності. РС – це значення потенціалу, необхідного ЗА для подолання захисту активу. За аналогією з ПЗ, для вимірювання РС також використовується відносна шкала (континуум).

Відповідно, у випадку зловмисного сценарію політика контролю має збільшувати РС, проте під час розгляду сценаріїв, пов'язаних з людською помилкою РС необхідно зменшувати.

Прикладами заходів, спрямованих на збільшення РС, можуть слугувати такі: запровадження автентифікації; розподіл привілеїв користувачів; своєчасне оновлення програмних продуктів та правильне конфігурування системи; запровадження шифрування.

Для зменшення впливу людських помилок можуть бути запропоновані такі заходи: тренування; добре розроблена документація; максимальне спрощення процесу.

Магнітуда втрат (МВ). МВ у ФАІР розглядається як складова ймовірної *магнітуди первинних втрат* (МПВ) та *вторинного ризику* (ВР), які виникають унаслідок настання події.

До того ж головною характеристикою МПВ є безпосередні (прямі) втрати, спричинені конкретною подією. Зі свого боку ВР може виникати внаслідок завдання шкоди побічним суб'єктам (*вторинним зацікавленим особам* – ВЗО), що може призвести до додаткових збитків внаслідок накладених санкцій, компенсаційних виплат, а в деяких випадках, іміджевих втрат. У разі необхідності оцінка ВР здійснюється за методою розрахунку Ризику.

Вторинна частота подій, що викликає втрати (ВЧПВВ) визначається як відсоток від первинних подій, які мають вторинний ефект. Така дефініція випливає з логічного твердження, що не всі події можуть впливати на ВЗО та, відповідно, слугувати тригером для виникнення вторинного ефекту. Так само МВВ завжди є похідною від реакції ВЗО на певні події. Тобто МВВ складається з витрат та виплат безпосередньо пов'язаних з ВЗО.

Загалом ризик, під час використання онтології факторного аналізу інформаційних ризиків, має загальний вигляд, наведений на рис. 1.

Наступним кроком, з метою отримання чисельних значень ризику, пропонується використати метод Монте-Карло – широкий клас обчислювальних алгоритмів, які покладаються на генерацію випадкових вибірок для отримання чисельних результатів. Основна концепція полягає у використанні випадковості з метою розв'язання проблем, для яких важко або неможливо задіяти інші підходи. Вказаний метод дасть змогу оцінити можливі ризики на підставі наявних вхідних даних, які випадково генеруються в обраних діапазонах та обраховуються за наведеною

вище онтологією ФАІР, де кожний з її елементів представляється у вигляді вузла обчислювання (ВО).

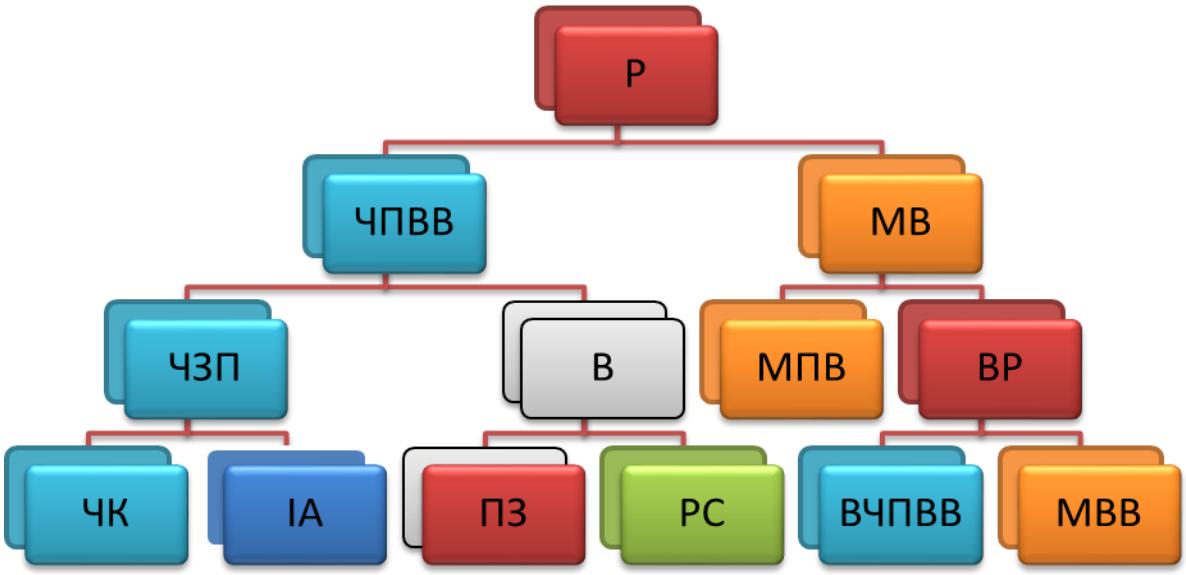


Рис. 1. Онтологія ФАІР

Вхідні дані до ВО представлені нормальним (гаусовим) розподілом, з такими параметрами, як математичне сподівання μ та дисперсія σ:

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\left(\frac{(x-\mu)^2}{2\sigma^2}\right)}.$$

Алгоритм обчислення вектора інформаційних ризиків наведено на рис. 2.

Вектор *TEF* – частота загрозливих подій (ЧЗП) – *k*-розмірний вектор елементів, вводиться безпосередньо, або розраховується за формулою

$$\begin{bmatrix} TEF_1 \\ \vdots \\ TEF_k \end{bmatrix}=\begin{bmatrix} CF_1 \\ \vdots \\ CF_k \end{bmatrix}\times\begin{bmatrix} PA_1 \\ \vdots \\ PA_k \end{bmatrix},$$

де *CF* – частота контакту (ЧК);

PA – імовірність атаки (ІА).

V – вразливість (В) – *k*-розмірний вектор елементів, кожне значення якого представляє ймовірність того, що потенційна загроза насправді призводить до втрати; вводиться безпосередньо, або розраховується за умовою

$$V_i=\begin{Bmatrix} 1, \text{ якщо } TC_1 \ge DL_i \\ 0, \text{ якщо } TC_1 < DL_i \end{Bmatrix},$$

де *TC* – потужність загрози (ПЗ);

DL – рівень складності (РС).

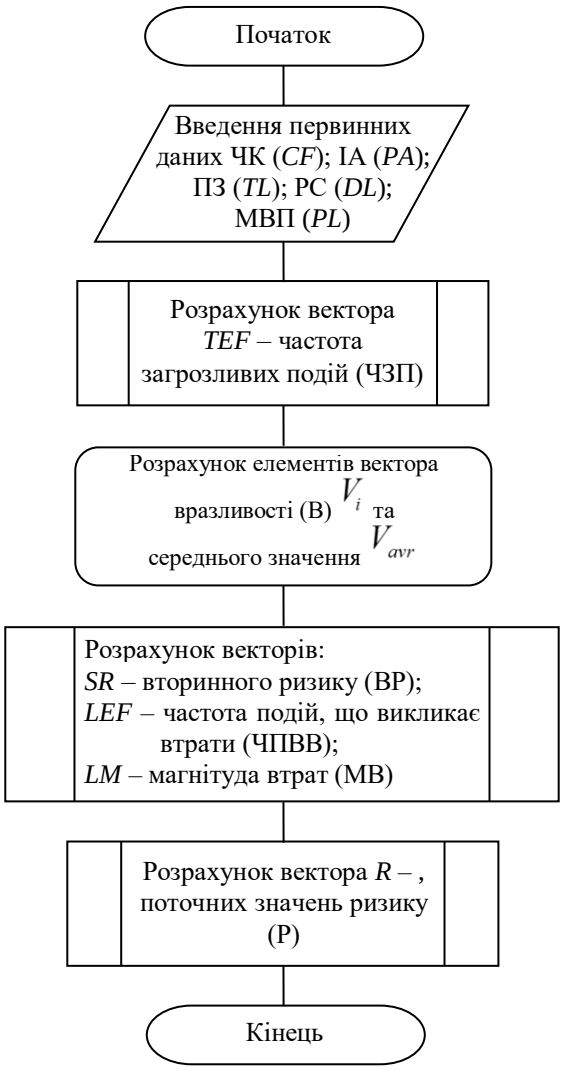
Потім вираховується середнє значення отриманого проміжного масиву одиниць і нулів, яке представляє відсоток разів, коли загроза перемогла контроль в наших імітаціях:

$$V_{avr}=\frac{V_1+V_2+\cdots+V_k}{K}.$$

SR – вторинний ризик (ВР) розраховується за формулою

$$\begin{bmatrix} SR_1 \\ \vdots \\ SR_k \end{bmatrix}=\sum_{j=1}^{n}\begin{bmatrix} SLEF_{1,1}\cdots SLEF_{1,n} \\ \vdots \quad \ddots \quad \vdots \\ SLEF_{k,1}\cdots SLEF_{k,n} \end{bmatrix}\circ\begin{bmatrix} SLEM_{1,1}\cdots SLEM_{1,n} \\ \vdots \quad \ddots \quad \vdots \\ SLEM_{k,1}\cdots SLEM_{k,n} \end{bmatrix},$$

де *SLEF* – вторинна частота подій, що викликає втрати (ВЧПВВ)



Умовні позначення

CF – частота контакту (ЧК);
PA – імовірність атаки (ІА);
TC – потужність загрози (ПЗ);
DL – рівень складності (РС);
PL – магнітуда первинних втрат (МПВ);
R – ризик

CF; *PA*; *TC*; *DL*; *PL* – *k*-розмірні вектори (де *k* – кількість випадкових генерацій) з елементами, які безпосередньо генеруються генератором псевдовипадкових значень (ГПВЗ)

Рис. 8. Алгоритм обчислення вектора інформаційних ризиків

SLM – магнітуда вторинних втрат (МВВ) – матриці сум поточних значень, де кожен рядок представляє одну імітацію, і кожен стовпець представляє значення ймовірності того, що конкретний виду збитку відбудеться (або значення суми збитку за сумою конкретного виду збитку, що залежать від вторинних факторів), які також безпосередньо генеруються ГПВЗ;

LEF – частота подій, що викликають втрати (ЧПВВ) – *k*-розмірний вектор елементів вводиться безпосередньо або розраховується за формулою

$$\begin{bmatrix} LEF_1 \\ \vdots \\ LEF_k \end{bmatrix} = \begin{bmatrix} TEF_1 \\ \vdots \\ TEF_k \end{bmatrix} \times \begin{bmatrix} V_1 \\ \vdots \\ V_k \end{bmatrix};$$

LM – магнітуда втрат (МВ) – *k*-розмірний вектор елементів, який вводиться безпосередньо, або розраховується за формулою

$$\begin{bmatrix} LM_1 \\ \vdots \\ LM_k \end{bmatrix} = \begin{bmatrix} PL_1 \\ \vdots \\ PL_k \end{bmatrix} \times \begin{bmatrix} SR_1 \\ \vdots \\ SR_k \end{bmatrix};$$

R – ризик (Р) – вектор поточних значень розмірності *k*, які представляють кінцеву втрату за даний часовий період (зазвичай один рік) розраховується за формулою

$$\begin{bmatrix} R_1 \\ \vdots \\ R_k \end{bmatrix} = \begin{bmatrix} LEF_1 \\ \vdots \\ LEF_k \end{bmatrix} \times \begin{bmatrix} LM_1 \\ \vdots \\ LM_k \end{bmatrix}.$$

Однією з переваг ФАІР вважається гнучкість, пов’язана з можливістю вибору даних, які надаються користувачем або обраховуються імітаційною моделлю. На нижчу ієрархію слід переходити лише у разі відсутності даних для вищої. Якщо необхідна інформація є в наявності, то вона вводиться до відповідного ВО без потреби заглиблюватись далі.

Висновок. Отже, запропонована імітаційна модель, яка була отримана на

основі запровадження методу факторного аналізу інформаційних ризиків, та наведений алгоритм розрахунку, у разі його реалізації як комп'ютерної програми, дасть змогу отримати ймовірні значення ризиків під час реалізації передбачених сценаріїв розвитку подій та приймати більш виважені та обґрунтовані рішення щодо попередження настання негативних наслідків у разі реалізації визначених кібернетичних загроз. Викладене, зі свого боку, допоможе в реалізації проактивного реагування на загрози в системі забезпечення кібернетичної безпеки в Збройних Силах України.

Напрями подальших досліджень. Надалі доцільно проаналізувати джерела отримання найбільш актуальних первинних даних, необхідних для функціонування імітаційної моделі та на основі проведених експериментів з'ясувати найбільш оптимальні шляхи підвищення ефективності функціонування системи забезпечення кібернетичної безпеки в Збройних Силах України та розробити відповідний програмний комплекс для розрахунків значень ризику за наведеними формулами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В Україні вперше розпочались курси з кіберзахисту для офіцерів-зв'язківців. Дата оновлення 28.01.2020. Сайт Defense Express. URL: https://defence-ua.com/index.php/home-page/9396-v-ukrayini-vpershe-rozpochalys-kursy-z-kiberzakhystu-dlya-ofitseriv-zv-yazkivtsiv (дата звернення: 28.01.2020).
2. Кацалап В. О., Устименко О. В Створення, розвиток та захист кібернетичного простору воєнної сфери України. *Гілея: науковий вісник.* Київ, 2013. Вип. 75 (№ 8). С. 519–521.
3. Устименко А. В., Кацалап В. О., Сарычев Ю. А. Киберпространство военной сферы. *Информационная безопасность в свете Стратегии Казахстан-2050* : сб. трудов I междунар. науч.-практ. конф. (м. Астана, 12 сент. 2013 г.). Астана, 2013. С. 539–545.
4. Сніцаренко П. М, Саричев Ю. О., Рогов П. Д. Методика оцінки інформаційного впливу на елементи інформаційної інфраструктури держави. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення* : зб. мат. VII наук.-техн. конф. НТТУ ДУТ. (м. Київ, 23 – 24 жовтня 2014 р.). Київ, 2014. С. 88–96.
5. Телелим В. М, Даник Ю. Г., Зінченко А. О. Модель оцінювання вразливостей систем з критичною кібернетичною інфраструктурою. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2018. № 2 (63). С. 63–67.
6. ВСТ 01.004.004 – 2014 (01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення. [Чинний від 2014-02-27]. (Військовий стандарт).
7. ВСТ 01.004.002 – 2019 (02). Воєнна безпека. Стратегічне планування. Терміни та визначення. [Чинний від 2020-01-01]. (Військовий стандарт).
8. Jack Freund and Jack Jones "Measuring and Managing Information Risk. A FAIR Approach". Waltham, MA 02451, USA, 2015. 392c.

Стаття надійшла до редакційної колегії 16.03.2020

Methodology for quantitative information risk assessment using the ontology of factor analysis

Annotation

Unlike the already familiar scheme of threat development (for example, in the military sphere), the development of cyber threats follows a different logic. At the moment of detecting the influence of a threat, it can already entail significant negative consequences. At the same time, the efficiency of the cyber security system, as a rule, lags significantly behind the growth rates of material and non-material losses from the implementation of the threat.

To neutralize cyber threats in the world practice, the theory of risk management, or risk management, is successfully used, which, unfortunately, is still rarely used in Ukrainian realities. According to current best cyber security practices, optimal security is achieved through an ongoing process of identification, risk assessment, and ongoing maintenance of security processes, combined with vulnerability remediation.

The article is devoted to improving the methodology for quantitative risk assessment, which uses the methods of factor analysis of information risks (FAIR) by decomposition, the mathematical apparatus of simulation, and allows you to make more balanced and well-grounded decisions to prevent the onset of negative consequences in the event of the implementation of certain cybernetic threats. The given calculation algorithm, if implemented as a computer program, will help in the implementation of a proactive response to threats in the cyber security system in the Armed Forces of Ukraine.

In the future, it is advisable to analyze the sources of obtaining the most relevant primary data necessary for the functioning of the simulation model and, on the basis of the experiments carried out, to find out the most optimal ways to increase the efficiency of the functioning of the cyber security system in the Armed Forces of Ukraine and to develop an appropriate software package for calculating the risk values according to the formulas given.

Keywords: factor analysis; informational risks; risk calculation; the frequency of the event that causes the loss; loss magnitude.