УДК 004.056, 004.75

Ю.Р. Гарасим[1], В.А. Ромака[2], М.М. Рибій[2]
[1]ТзОВ "ІТ Капітал",
відділ інформаційної безпеки
[2]Національний університет "Львівська політехніка",
кафедра захисту інформації

АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ ЗАБЕЗПЕЧЕННЯ ВЛАСТИВОСТІ ЖИВУЧОСТІ СИСТЕМ

Запропоновано підхід до вирішення завдання управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. Розглядається приклад неперервності функціонування систем захисту інформації у корпоративних мережах зв'язку. Запропоновано алгоритм кількісної оцінки ризиків на базі NIST 800-30, CRAMM, OCTAVE.

Ключові слова: властивість живучості, неперервність функціонування, система захисту інформації, процес управління ризиками.

The paper considers information security risk management problem solving approach during enterprise communication network information security system continuity functioning providing. The information security risk management methodology based on NIST 800-30, CRAMM, OCTAVE is improved and the quantitative risk assessment algorithm is proposed.

Key words: survivability property, continuity functioning, information security system, risk management process.

Вступ

У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність системи (надалі розглядатимемо бізнес-процес компанії) ефективно функціонувати за умови впливу чинників дестабілізації (ЧД): збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу [1]. Згідно з цим визначенням невід'ємною складовою властивості живучості бізнес-процесу компанії є неперервність його виконання. Міжнародний стандарт ISO 27001, який визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ), тлумачить неперервність функціонування як один із рекомендованих контролів у життєвому циклі СМІБ. Отже, неперервність функціонування є не лише запорукою ефективного розроблення та впровадження СМІБ, але й дієвим способом та невід'ємною складовою процесу забезпечення властивості живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації корпоративні мережі зв'язку (КМЗ) є основним методом збору, оброблення, зберігання та передавання інформації. Водночас, автори статті наголошують на важливості такого складового компонента КМЗ, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних активів компанії. Тому наголошуємо не просто на властивості живучості організації загалом, а на забезпеченні неперервності функціонування СЗІ в КМЗ як невід'ємній та критично важливій частині ефективного та безпечного функціонування компанії, виконання її основних бізнес-процесів.

Запропонована авторами статті методика забезпечення неперервності функціонування СЗІ [2] передбачає етап управління ризиками інформаційної безпеки (ІБ) як один із етапів забезпечення неперервного функціонування СЗІ зокрема, та, відповідно, КМЗ загалом. Управління ризиками ІБ може здійснюватись для всієї організації або ж поширюватись лише на певну її сферу (межі застосування – scope). У випадку, якщо оцінювання ризиків проведено в загальних масштабах ще

до моменту формулювання завдання забезпечення неперервності функціонування СЗІ, вибіркові результати такої оцінки можуть бути використані як результат етапу аналізу ризиків запропонованої методики [2]. Якщо ж управління ризиками ІБ попередньо не проводилось (цей випадок поширеніший в Україні, оскільки в компаніях ризик-орієнтований підхід в управлінні лише на етапі становлення, що зумовлено, зокрема, невисокою "зрілістю" компаній в управлінні як ІТ, так й ІБ), то згідно з методикою [2] виконують аналіз ризиків ІБ, який здійснюється в контексті забезпечення неперервності функціонування КМЗ, зокрема СЗІ, і слугує для ідентифікації загроз та визначення потенційного збитку від реалізації сценарію впливу ЧД.

Розрізнятимемо такі основні категорії чинників дестабілізації нормальної роботи СЗІ як складової КМЗ в контексті забезпечення їхнього неперервного функціонування [3]:

– Стихійні лиха. Порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад, потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині.

– Соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства (наприклад, акти вандалізму, терористичні акти, війни тощо).

– Фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на СЗІ або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил, корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації).

– Порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування КМЗ (наприклад, відмова мережі електроживлення, системи кондиціонування повітря, системи водопостачання).

– Порушення ІБ внаслідок порушень, які зумовлені, наприклад, електромагнітним випромінюванням, коливаннями напруги, електронними завадами.

– Технічний збій. Порушення ІБ, спричинене відмовами СЗІ або пов'язаними з нею нетехнічними можливостями. До такого типу ризиків зараховуємо апаратний, програмний збій, перевантаження, порушення ремонтоздатності.

– Технічні атаки. Порушення ІБ, що зумовлене атакуванням КМЗ та використанням її вразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS / DDoS).

У статті розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як невід'ємної складової ефективної та безпечної роботи компанії.

1. Процес управління ризиками ІБ

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ, зокрема підсистеми СЗІ:

1. Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності вразливостей, величини завданого збитку.

3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування СЗІ.

4. Оцінка вразливостей та контролів. Аналіз основних властивостей КМЗ та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Представимо графічне зображення життєвого циклу процесу управління ризиками ІБ в контексті забезпечення неперервності функціонування (рис. 1).

Рис. 1. Життєвий цикл процесу управління ризиками ІБ

2. Аналіз методик управління ризиками інформаційної безпеки

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30 [4], методика CRAMM [5] та методика OCTAVE [6].

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [7].

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність [7].

Використання такої методики передбачає такі етапи:

- опис характеристик системи;
- ідентифікація загроз;
- ідентифікація вразливостей;

– аналіз наявних засобів/заходів захисту;
– визначення значення ймовірності;
– аналіз впливу;
– визначення значення ризику;
– вибір засобів/заходів захисту;
– документування отриманих результатів.

Алгоритм цієї методики зображено на рис. 2.

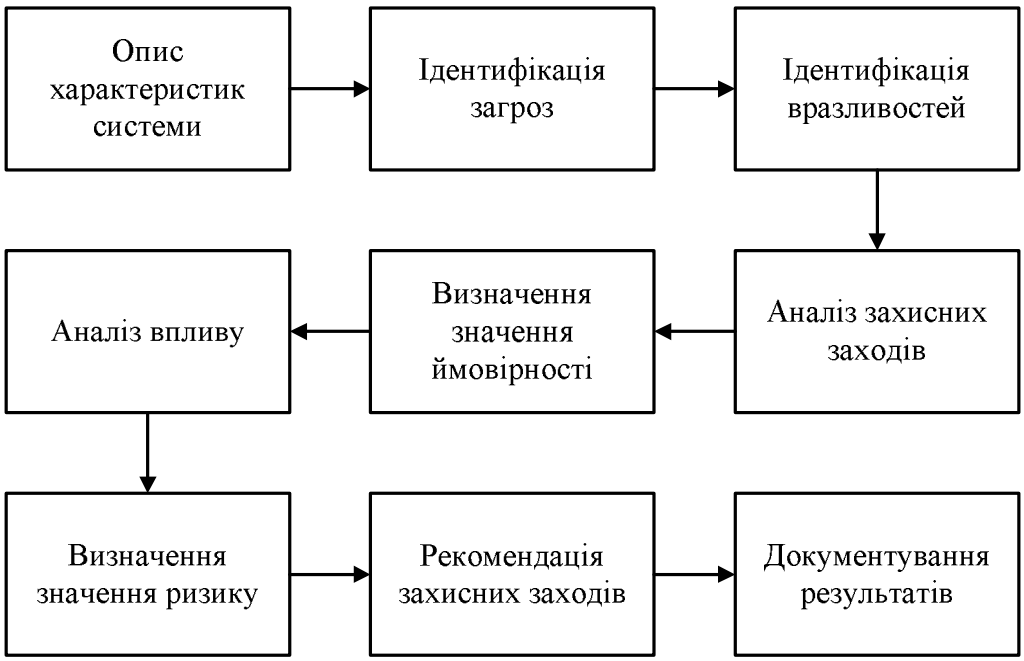

Рис. 2. Алгоритм методики управління ризиками NIST 800-30

Наступною методикою, яку аналізують автори статті, є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM [8].

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга") [8].

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: "Чи достатньо для захисту системи застосування засобів

базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?" На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів [8].

Алгоритм методики CRAMM подано на рис. 3.

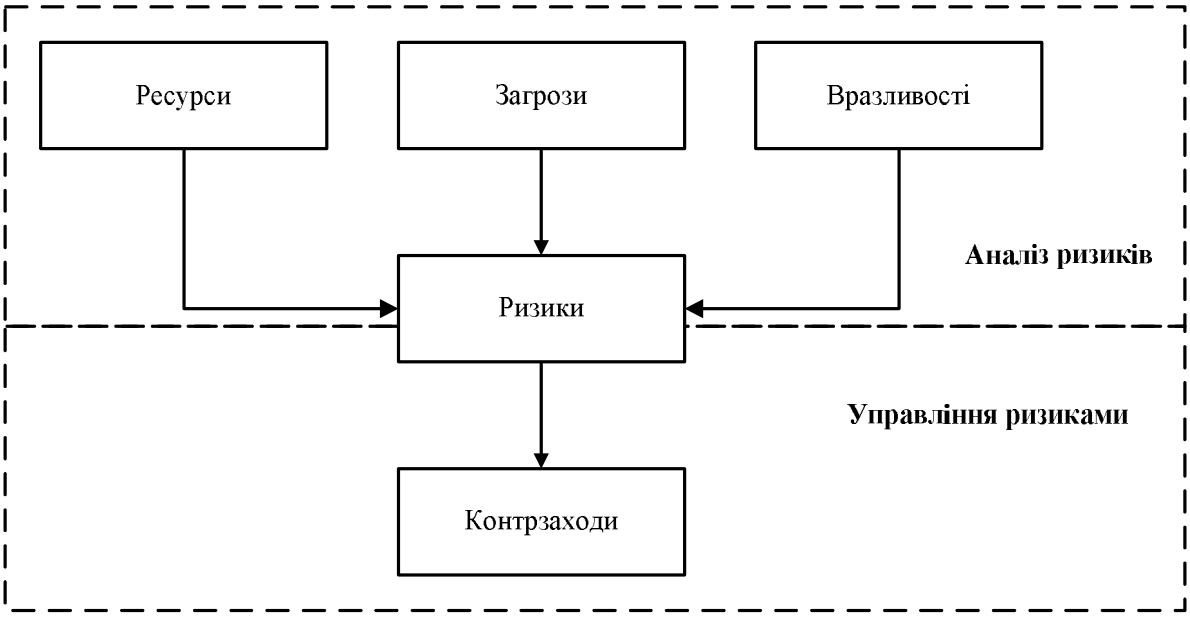

Рис. 3. Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності [9].

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [9].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 4.

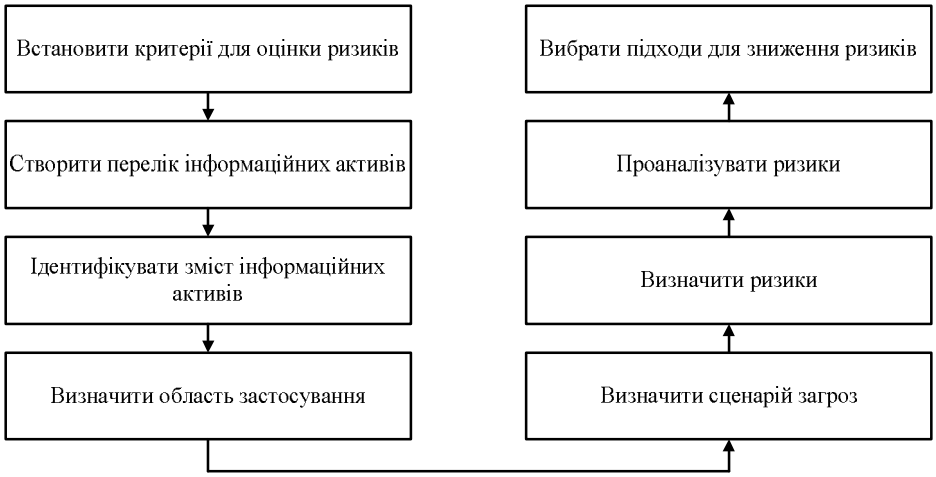

Рис. 4. Алгоритм методики управління ризиками OCTAVE

Отже, коротко охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки [8, 10, 11] та здійснивши аналіз основних властивостей цих методик, автори визначили основні переваги та недоліки перелічених вище методик. Їх подано у вигляді табл. 1.

Таблиця 1

Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST	– порівняно проста в реалізації; – придатна для підприємств різного розміру; – детально описує всі можливі ризики для інформаційних активів; – припускає використання як способів зниження ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику); – існує автоматизоване програмне забезпечення, що реалізовує принципи методики; йому властива відносна легкість та зручність використання.	– довготривалий процес аналізу; – розроблена для використання у федеральних організаціях США; – оцінювання ризиків проводиться за трирівневою шкалою, що істотно обмежує можливості методики загалом.
CRAMM	– є універсальною і підходить для організацій як державного, так та комерційного сектору; – використовує кількісні і якісні способи оцінки ризиків; – розроблені комерційні програмні продукти, що реалізовують положення CRAMM;	– використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; – довготривалий процес аналізу; – програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці; – не дає змоги створювати власні шаблони звітів або модифікувати наявні; – припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як “уникнення” або “прийняття”, не розглядаються.
OCTAVE	– швидко впроваджується; – можливе застосування для організацій різного розміру та галузей зайнятості; – є комерційні програмні продукти, що реалізовують положення методики; – високий рівень гнучкості.	– не дає кількісної оцінки ризиків; – припускає використання як способів зниження ризиків лише його зниження і прийняття.

У випадку забезпечення неперервності функціонування СЗІ в КМЗ, що є довготривалим та ресурсомістким процесом, аналіз ризиків ІБ, які можуть стати загрозою для неперервності функціонування СЗІ, є лише одним з багатьох етапів, що повинні бути успішно виконані. Саме тому дуже важлива можливість швидкого та порівняно простого управління ризиками ІБ, що входять у сферу впливу неперервності функціонування СЗІ в КМЗ. Так, на основі проведеного аналізу, автори статті зробили висновок, що оптимальним варіантом для вибору методики управління ризиками ІБ в контексті забезпечення неперервності функціонування КМЗ та СЗІ зокрема є адаптація та удосконалення відомих методик логічним поєднанням їх переваг та мінімізацією недоліків.

3. Методика управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ

Внаслідок проведеного в попередньому розділі аналізу методик для управління ризиками ІБ автори статті прийняли рішення представити методику управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як адаптовану методику, що поєднує переваги трьох охарактеризованих вище методик і, тим самим, мінімізує їх основні недоліки, наведені в табл. 1. Це дало змогу підвищити ефективність процесу управління ризиками ІБ, оптимізувавши часові витрати на процес управління, надавши можливість використання адаптованої методики для організацій різного розміру та напряму діяльності та запровадивши в методику як якісну, так і кількісну оцінку ризиків ІБ.

Алгоритм адаптованої методики управління ризиками ІБ в контексті забезпечення неперервності функціонування КМЗ та СЗІ зокрема запропонували автори статті в роботі [12] після ряду удосконалень. Коротко опишемо згаданий вище алгоритм.

Отже, методика передбачає шість етапів.

Етап 1. Ідентифікація активів. На цьому етапі команда з управління ризиками ІБ та власник інформаційного активу повинні визначати процеси, додатки, системи або активи, які розглядаються. Ключовим моментом є розуміння факту, що в цьому випадку розгляду підлягають лише ті системи/ активи, які є критичними для забезпечення неперервності функціонування СЗІ в КМЗ.

Етап 2. Ідентифікація загроз. Команда з управління ризиками ІБ визначає загрози як небажані події, які можуть вплинути на роботу СЗІ в КМЗ. Деякі загрози виникають, коли впроваджені контролі або впроваджені неправильно, або втратили актуальність і вже стали причиною вразливості КМЗ та можуть бути використані для обходу контролів. Цей процес відомий як використання вразливості.

Етап 3. Визначення ймовірності виникнення. Після того, як список загроз визначено і команда з управління ризиками погодила його, необхідно з’ясувати, наскільки ймовірне виникнення конкретних загроз.

Етап 4. Визначення впливу від реалізації загрози. Після того, як встановлено ймовірність виникнення загрози, необхідно визначити вплив, який спричинить її реалізація. Перш ніж визначити величину впливу, необхідно переконатися, що сфера застосування аналізу ризиків була правильно визначена. Це необхідно для того, щоб команда з управління ризиками зрозуміла мету або місію активу, що розглядається, і як вона впливає на загальну місію організації або її цілі.

Етап 5. Оброблення ризиків ІБ та вибір рекомендованих контролів. Після того, як рівень ризику визначено, команда з управління ризиками визначає способи, які могли б усунути ризик або принаймні знизити його до прийнятного рівня, та вибирає відповідні контролі або заходи захисту. Одна з цілей оцінки ризику – задокументувати належну обачність компанії під час прийняття рішень. Отже, дуже важливо визначити всі контролі та заходи захисту, які можуть, на думку команди, знизити ризик до прийнятного рівня.

Етап 6. Документація. Після завершення аналізу ризиків результати повинні бути задокументовані в стандартному форматі й у звіті, призначеному для власника активів. Цей звіт допоможе керівництву, власнику приймати рішення в аспекті політик, процедур, бюджету та управління змінами. У звіті з аналізу ризиків повинна міститись систематична та аналітична оцінка

ризиків, так, щоб вище керівництво оцінило ризики ІБ і виділило необхідні ресурси для зниження ризику до прийнятного рівня.

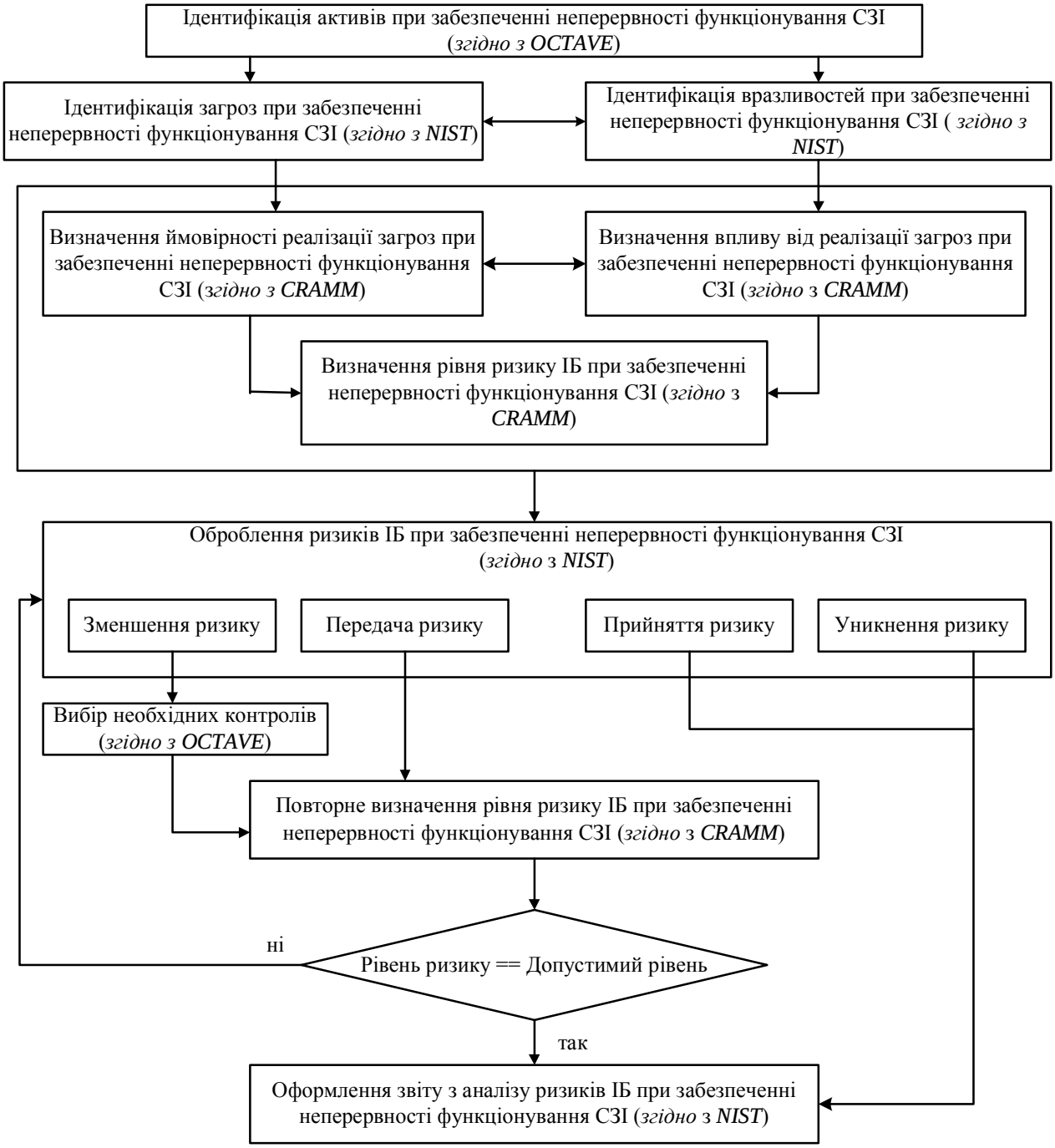

Рис. 5. Удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в КМЗ

4. Кількісна оцінка ризиків ІБ при забезпеченні неперервності функціонування СЗІ в КМЗ

Опишемо процес кількісної оцінки ризиків у контексті забезпечення живучості, як один із варіантів виконання етапу оцінки ризиків, представленого в методиці, яку описано в п. 3. Запропонований алгоритм кількісної оцінки ґрунтується на ймовірнісній постановці прийняття рішень.

Відповідно, ризик – категорія ймовірнісна, тому в процесі кількісного оцінювання ризиків використовуватимемо ймовірнісні розрахунки. Отже, завдяки теорії ймовірності така методика

кількісної оцінки ризиків ІБ представляє можливий збиток від реалізації загрози ІБ як математичне сподівання, а рівень ризику у вигляді середнього квадратичного відхилення.

Згідно з нерівністю Чебишева, ймовірність P того, що величина X відхилиться від свого математичного сподівання більше, ніж на задане допустиме $e > 0$, не перевищує її дисперсії, поділеної на e^2. Тобто [13]

$$P(|X - E| > e) \le \frac{D}{e^2}, \tag{1}$$

де E – математичне сподівання

$$E = \sum P_i \cdot X_i, \tag{2}$$

де D – дисперсія

$$D = s^2 = (X_i - E)^2 \cdot P_i. \tag{3}$$

Ризиком називатимемо число s – середнє квадратичне відхилення керуючого фактора X, яке позначимо $s = r$ [14].

Якщо під X розуміти можливий збиток від реалізації загрози Q, тоді E_Q є середнім очікуваним збитком, а середнє квадратичне відхилення s_Q – оцінкою ризикованості, ризиком і позначається r_Q.

Коефіцієнт варіації $V_Q = \frac{s_Q}{E_Q} \cdot 100\%$ – безрозмірна величина. Він дає змогу порівняти коливання ознак, які виражені в різних одиницях вимірювання. Коефіцієнт варіації вимірюється від $0\,\%$ до $100\,\%$. Чим більший коефіцієнт, тим більше коливання. Встановлена така кількісна оцінка різних значень коефіцієнта варіації: до 10 % – слабке коливання, 10–25 % – помірне коливання, більше за 25 % – сильне коливання [13].

Наприклад, під час аналізу основні параметри оцінки ризиків ІБ (ймовірність реалізації загрози, можливий збиток) для загроз Q (розглянуто два типи: DDoS атака, вихід з ладу обладнання кондиціонування) оцінено за трьома критеріями – ризик матеріальних втрат (X_1), порушення законодавства і/або договірних зобов'язань (X_2), репутаційні ризики (X_3). Значення шкали оцінювання ймовірності реалізації загроз коливається від 1 (1 раз на 3 роки) до 5 (1 раз на 1 годину), а значення шкали оцінювання збитку розглядає максимальний збиток як 1 (від 100 000 грн.), а мінімальний – 5 (до 5 000 грн.).

Отже, експертна оцінка параметрів надала такі результати: DDoS атака – $P_1 = 2$, $X_1 = 2$, $X_2 = 5$, $X_3 = 3$; вихід з ладу обладнання кондиціонування – $P_2 = 2$, $X_1 = 1$, $X_2 = 5$, $X_3 = 3$.

Тоді середній очікуваний збиток від реалізації DDoS атаки становить $E_{1Q} = \sum P_1 \cdot X_i = 20$, а ризик $r_{1Q} = s_1 = \sum \sqrt{(X_i - E_{1Q})^2 \cdot P_1} = \sqrt{1676} = 41$. Відповідно, середній очікуваний збиток від виходу з ладу обладнання кондиціонування становить $E_{2Q} = \sum P_2 \cdot X_i = 18$ та ризик $r_{2Q} = s_2 = \sum \sqrt{(X_i - E_{2Q})^2 \cdot P_2} = \sqrt{1750} = 42$.

Перевагою цього методу оцінки ризику ІБ є простота математичних розрахунків, а недоліком – необхідність великої кількості вихідних даних (чим більший масив, тим достовірніша оцінка ризику) [13].

Висновки

У статті розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування КМЗ та СЗІ зокрема. Здійснено аналіз трьох поширених методик в сфері управління ризиками ІБ (NIST 800-30, CRAMM, OCTAVE), що дало змогу визначити їх основні особливості, встановити переваги та недоліки. В процесі аналізу прийнято рішення про адаптацію розглянутих методик до процесу управління ризиками ІБ із забезпеченням неперервності

функціонування СЗІ. Процес адаптації автори оформили у вигляді методики, яка враховує позитивні якості розглянутих вище трьох методик і, отже, мінімізує їх недоліки. Це рішення дало змогу вирішити завдання обмеженості відомих методик управління ризиками ІБ для застосування в контексті забезпечення неперервності функціонування СЗІ в КМЗ. Представлено удосконалений алгоритм цієї методики. Як варіант, запропоновано алгоритм кількісної оцінки ризиків ІБ, що може застосовуватись на етапі оцінки ризиків адаптованої методики.

1. Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – 2010. № 1 (4). – С. 87–95. 2. Гарасим Ю. Р. Забезпечення живучості та неперервності функціонування систем захисту інформації / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2012. – № 741. – С. 105-112. 3. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p. 4. Swanson M. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. – 2010. – 149 p. 5. CCTA Risk Analysis and Management Method. 6. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 1999. – С. 84. 7. Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики / П. А. Балашов, В. П. Безгузиков, Р.И. Кислов // [Електронний ресурс]. – режим доступу: http://www.nwaktiv.ru/textstat2/index.html 8. Куканова Н. Актуальность задачи – обеспечения информационной безопасности для бизнеса / Н. Куканова // [Електронний ресурс] режим доступу: http://www.dsec.ru/about/articles/ar_compare/ 9. Методология OCTAVE для оценки информационных рисков [Електронний ресурс]. – Режим доступу: http://www.risk24.ru/octave.htm 10. Методологии управления ИТ-рисками [Електронний ресурс]. – Режим доступу: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami 11. Ткаченко В. Современные подходы к оценке рисков информационных технологий / В. Ткаченко, В. Сысоев // [Електронний ресурс]. – Режим доступу: http://www.cbz.com.ua/resources/files/12224515494d0f29e1ca cc9.pdf 12. Гарасим Ю.Р. Аналіз ризиків при забезпеченні живучості та неперервності функціонування систем захисту інформації / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Матеріали шістнадцятої Всеукраїнської наукової інтернет-конференції. – Тернопіль: Тайп, 2012 – С. 3–5. 13. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций / А. С. Шапкин. – М. : Издательско-торговая корпорация "Дашко и К", 2003. – 544 с.