УДК 621.392

О.Г. Пузиренко[1], С.О. Івко[2], О.О. Лаврут[2]

[1] *Генеральний штаб Збройних Сил України, Київ*
[2] *Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів*

# АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАБЕЗПЕЧЕННІ ЖИВУЧОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

*Проведено аналіз процесу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування система захисту інформації. Надана оцінка процесу управління ризиками, проаналізовані сучасні методики управління ризиками інформаційної безпеки. Запропоновано удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування системи захисту інформації в інформаційно-телекомунікаційні системи.*

***Ключові слова**: захист інформації, інформаційно-телекомунікаційні системи, ризики інформаційної безпеки.*

## Вступ

**Постановка проблеми в загальному вигляді. Анализ останніх досліджень і публікацій.** У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність інформаційно-телекомунікаційної системи 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 діяльності установи, організації є неперервність його виконання, що також відноситься і до інформаційно-телекомунікаційних систем спеціального призначення. 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 живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації інформаційно-телекомунікаційні системи (ІТС) є основним методом збору, обробки, зберігання та передавання інформації. Водночас, слід зазначити важливість такого складового компонента інформаційно-телекомунікаційних систем, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних складових [2].

Методика забезпечення неперервності функціонування СЗІ передбачає етап управління ризиками інформаційної безпеки (ІБ) як один із етапів забез-

печення неперервного функціонування СЗІ зокрема, та ІТС загалом. Управління ризиками ІБ може здійснюватися для всіх ІТС або ж поширюватись лише на певну її сферу. У випадку, якщо оцінювання ризиків проведено в загальних масштабах ще з моменту формулювання завдання забезпечення неперервності функціонування СЗІ, вибіркові результати такої оцінки можуть бути використані як результат етапу аналізу ризиків запропонованої методики. Якщо ж управління ризиками ІБ попередньо не проводилось, то згідно з методикою виконують аналіз ризиків ІБ, який здійснюється в контексті забезпечення неперервності функціонування ІТС, зокрема СЗІ для ідентифікації загроз та визначення потенційного збитку від реалізації сценарію впливу ЧД.

Основні категорії чинників дестабілізації нормальної роботи СЗІ як складової ІТС в контексті забезпечення їхнього неперервного функціонування такі [3]:

– 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 або носієм інформації);

– порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування ІТС (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 атаками на ІТС та використанням її вразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості, спроба входу, втручання, відмова в обслуговуванні (DDoS).

Тому для забезпечення неперервності функціонування СЗІ необхідно забезпечити стійкий і безперервний процес управління ризиками ІБ, що неможливо якісно зробити без проведення аналізу самого процесу.

**Мета статті** полягає у всебічному аналізі процесу управління ризиками ІБ, узагальненні існуючих методик управління ризиками та розробці адаптованої методики, що забезпечує живучість та неперервність функціонування СЗІ в ІТС.

## Основна частина

**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 ІТС, 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 ІТС 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.

Графічне зображення життєвого циклу процесу управління ризиками ІБ в контексті забезпечення неперервності функціонування представлено на рис. 1.

**2. Аналіз методик управління ризиками інформаційної безпеки**

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

Однією з класичних 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 організацій, установ виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

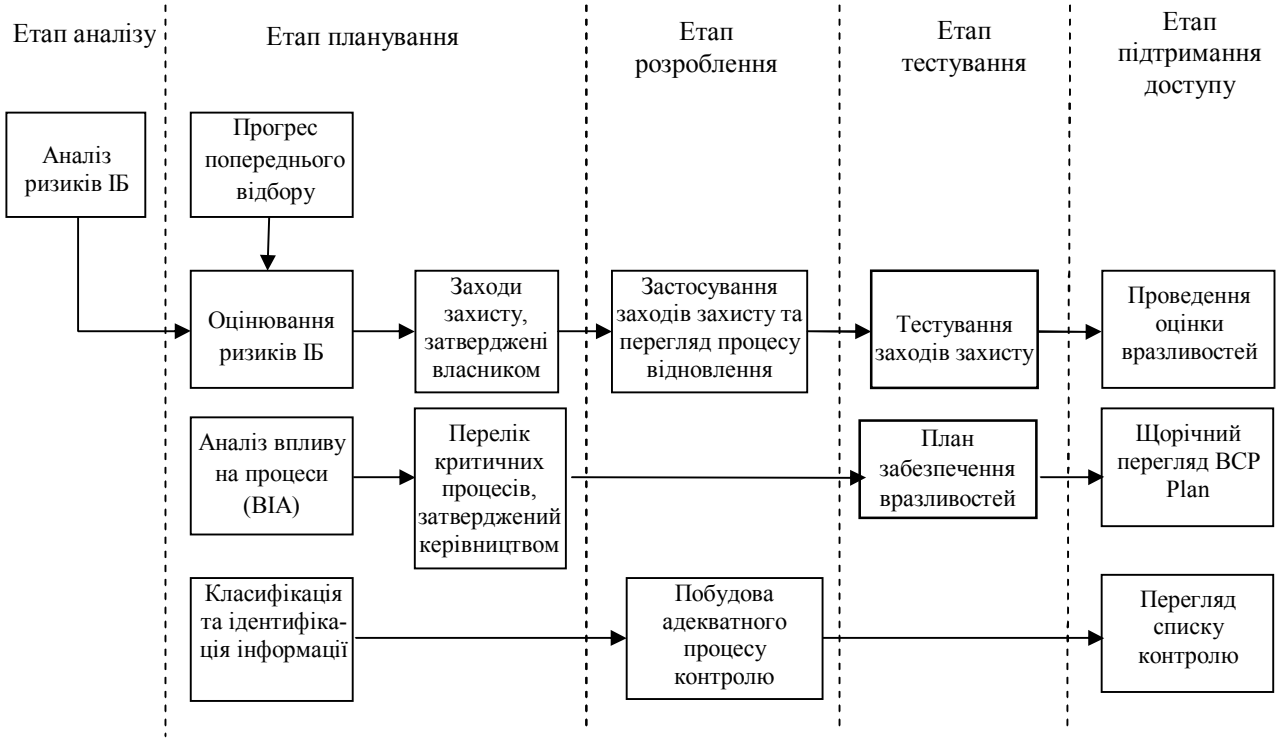


Рис. 1. Життєвий цикл процесу управління ризиками ІБ

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях NIST 800-30, охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Запропонований процес оцінювання ризику ІБ, представляється 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 відторюваність [7].

Використання такої методики передбачає наступні 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.

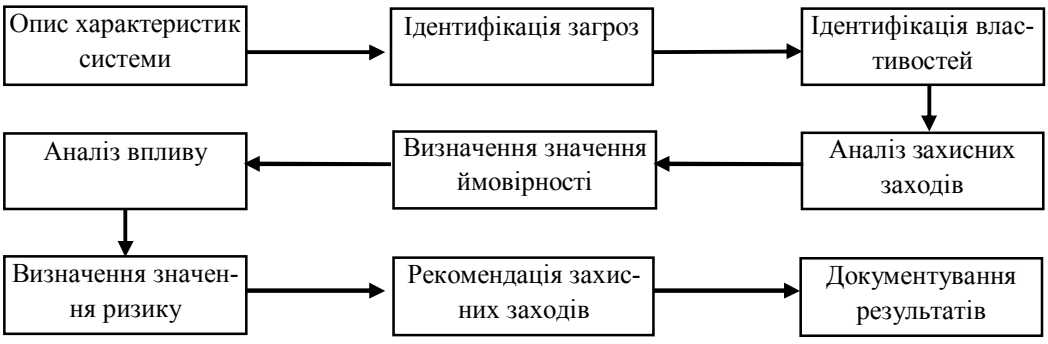


Рис. 2. Алгоритм методики управління ризиками NIST 800-30

Наступною методикою є методика CRAMM (CCTA Risk Analysis and Managment Method), Агентства з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency), що розроблена 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].

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 організації 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 розглянутої методики представлено на рис. 3.


Рис. 3. 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, можливо визна-

чити основні переваги та недоліки перелічених вище методик (табл. 1). У випадку забезпечення неперервності функціонування СЗІ в ІТС, 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 ІТС. Так, на основі проведеного аналізу можливо зробили висновок, що оптимальним варіантом для вибору методики управління ризиками ІБ в контексті забезпечення неперервності функціонування ІТС та СЗІ зокрема є адаптація та удосконалення відомих методик логічним поєднанням їх переваг та мінімізацією недоліків.

Таблиця 1

Переваги та недоліки методик з управління ризиками ІБ

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

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

Внаслідок проведеного аналізу методик для управління ризиками ІБ виникає можливість представлення методики управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в ІТС як адаптованої методики, що поєднує переваги трьох охарактеризованих вище методик і, тим самим, мінімізує їх основні недоліки. Це дає змогу підвищити ефективність процесу управління ризиками ІБ, оптимізувавши часові витрати на процес управління, надавши можливість використання адаптованої методики для ІТС різного розміру та напряму діяльності та запровадити в методику як якісну, так і кількісну оцінку ризиків ІБ.

Алгоритм адаптованої методики управління ризиками ІБ, в контексті забезпечення неперервності функціонування ІТС та СЗІ, запропоновано в роботі [12]. Після ряду удосконалень адаптована методика буде мати алгоритм розрахований на шість етапів (рис. 4).

**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 ІТС.

**Етап 2.** Ідентифікація загроз. Команда з управління ризиками ІБ визначає загрози як небажані по-

дії, які можуть вплинути на роботу СЗІ в ІТС. Деякі загрози виникають, коли впроваджені контролі або впроваджені неправильно, або втратили актуальність і вже стали причиною вразливості ІТС 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.

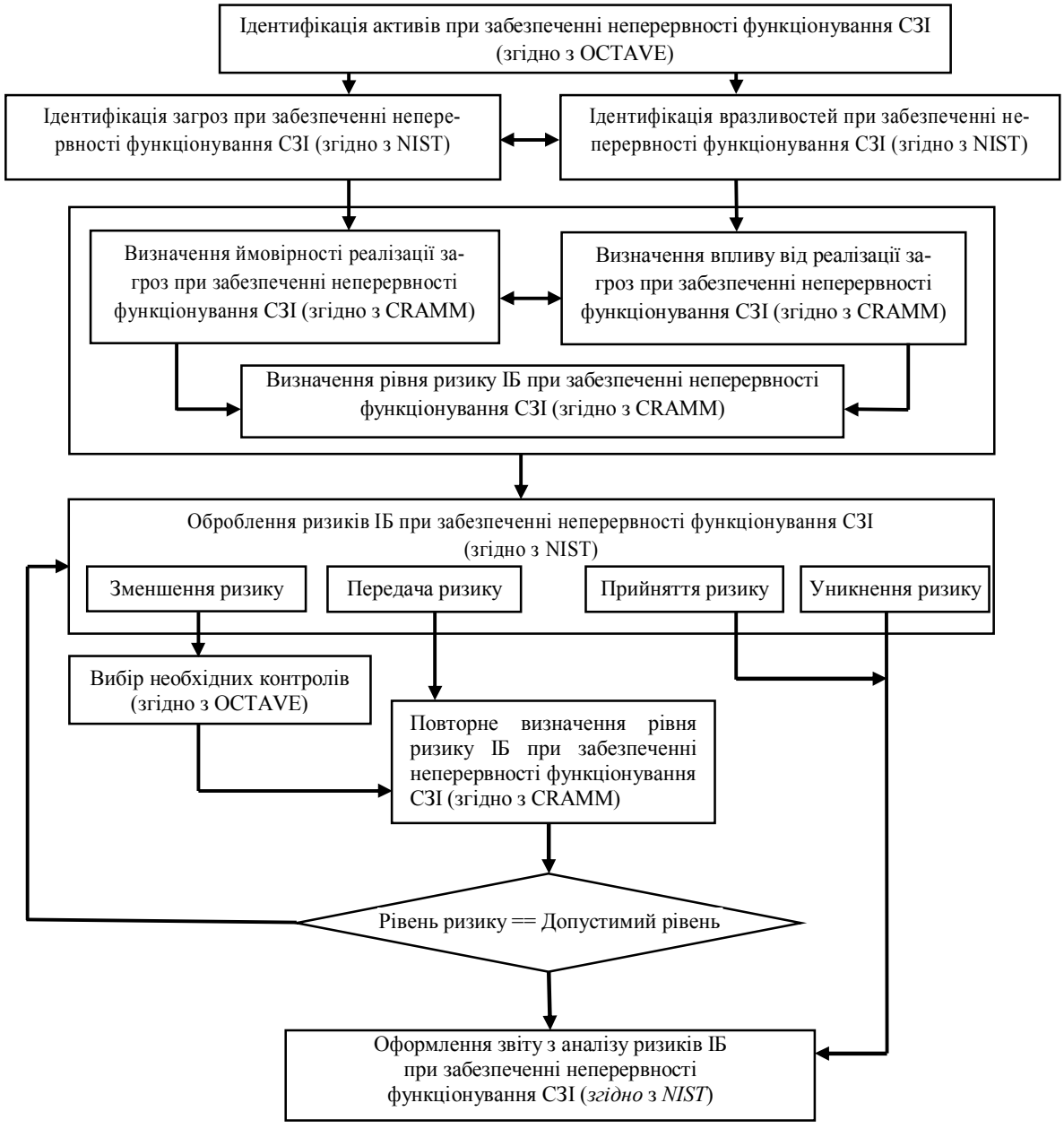


Рис. 4. Удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в ІТС

**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.

## Висновки

У статті проаналізовано процес управління ризиками ІБ в забезпеченні неперервності функціонування ІТС та СЗІ. 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 розглянуто адаптацію методик до процесу управління ризиками ІБ із забезпеченням неперервності функціонування СЗІ.

Результатом аналізу є запропонована адаптована методика управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в ІТС.

Розроблена методика враховує позитивні якості розглянутих вище методик і мінімізує їх недоліки.

Подальші дослідження необхідно спрямувати на вдосконалення запропонованої методики шляхом розробки методів системного моніторингу ризиків інформаційної безпеки, що дозволяють не лише контролювати, а й підтримувати такий стан інформаційної безпеки, за якого її показники перебуватимуть у допустимих мережах.

## Список літератури

*1. Гарасим Ю.Р. Аналіз систем захисту, які мають властивість живучості / Ю.Р. Гарасим // Військово-технічний збірник – Львів: Видання Національного університету "Львівська політехніка", 2010. – Вип. 1. – 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 Національного університету "Львівська політехніка" науково-технічний збірник – Львів: Оріон, 2012. – Вип. 741. – С. 105-112. – (Серія "Автоматика, вимірювання та керування").*

*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. Чередниченко В.С. Обґрунтування пріоритетних заходів, щодо підвищення рівня інформаційної безпеки / В.С. Чередниченко // Захист інформації, – 2008. – № 4. – С. 13-15.*

*6. Кириличев Б.В. Моделирование систем / Б.В. Кириличев. – М.: МГУ, 2009. – С. 274-276.*

*7. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики: учебное пособие / П.А. Балашов, В. . Безгузиков, Р.И. Кислов – М.: Научная литература, 2009. – С. 165.*

*8. Куканова Н.А. Актуальность задачи – обеспечение информационной безопасности для бизнеса: монография / Н.А. Куканова – К.: Бизнесинформ, 2010. – С. 136.*

*9. Методология OCTAVE для оценки информационных рисков. – М.: Информационный ресурс, 2005. – С. 25.*

*10. Методологии управления ИТ-рисками: – М.: Информационный ресурс, 2010. – 103 с.*

*11. Ткаченко В.А. Современные подходы к оценке рисков информационных технологий: монография / В.А. Ткаченко/ – М.: Экономическая безопасность, 2013. – 156 с.*

*12. Гарасим Ю.Р. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем / Ю.Р. Гарасим, В.А. Ромака, М.М. Рибій // Вісник Національного університету "Львівська політехніка" "Автоматика, вимірювання та керування". – 2013. – № 756. – С. 105-123.*

*Надійшла до редколегії 2.09.2014*

**Рецензент:** д-р техн. наук, ст. наук. співр. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

### АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ ЖИВУЧЕСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

О.Г. Пузыренко, С.А. Ивко, А.А. Лаврут

*Проведен анализ процесса управления рисками информационной безопасности в контексте обеспечения непрерывности функционирования система защиты информации. Дана оценка процесса управления рисками, проанализированы современные методики управления рисками информационной безопасности. Предложен усовершенствованный алгоритм адаптированной методики управления рисками при обеспечении живучести и непрерывности функционирования системы защиты информации в информационно-телекоммуникационных системах.*

***Ключевые слова:*** *защита информации, информационно-телекоммуникационные системы, риски информационной безопасности.*

### ANALYSIS OF RISK MANAGEMENT INFORMATION SECURITY PROVISION OF SURVIVABILITY OF INFORMATION AND TELECOMMUNICATIONS SYSTEMS

O.G. Puzyrenko, S.O. Ivko, O.O. Lavrut

*The analysis of the risk management of information security in the context of ensuring continuity of operation of the system of information security. The estimation of the risk management process, analyzes the modern techniques of risk management information security. A improved algorithm adapted techniques of risk management while ensuring survivability and continuity of the system of information security in information and telecommunication systems.*

***Keywords:*** *information security, information and telecommunication systems, information security risks.*