# МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

**УДК 681.3.06** **DOI:10.30837/rt.2021.3.206.01**

*О.В. ПОТІЙ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,*
*О.А. ЗАМУЛА, д-р техн. наук, К.В. ІСІРОВА*

## АНАЛІЗ МЕТОДІВ ОЦІНКИ І УПРАВЛІННЯ РИЗИКАМИ КІБЕР- І ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

### Вступ

Ефективність роботи установи, підприємства, компанії, організації безпосередньо залежить від якості і оперативності управління виробництвом (бізнес-процесами). У сферу управління включаються різні ресурси – інформація, персонал, технологічні процеси, техніка. Загальновизнаним стратегічним чинником зростання конкурентоспроможності компанії є ефективне застосування інформаційних технологій (ІТ). При цьому застосування ІТ немислимо без підвищеної уваги до питань кібер- і інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати організації значних матеріальних збитків. Для організацій, комп'ютерні мережі яких налічують не один десяток комп'ютерів з різними апаратними платформами, програмним забезпеченням, операційними системами, додатками тощо, на перше місце виступає завдання управління безліччю різноманітних захисних механізмів в таких гетерогенних корпоративних мережах. Складність мережевої інфраструктури, різноманіття даних і додатків призводять до того, що при реалізації системи інформаційної безпеки за межами уваги адміністраторів безпеки можуть виявитися багато загроз. Тому необхідне здійснення надійного і ефективного управління комп'ютерними мережами і засобами мережевої безпеки.

На перший план при вирішенні задач забезпечення інформаційної і кібербезпеки, а також приватності виходить створення системи управління інформаційною безпекою (СУІБ), яка охоплює всю інфраструктуру компанії.

СУІБ дозволяє (надає можливості) [1]:

- централізовано і оперативно надавати керуючі впливи на всю інформаційну інфраструктуру;
- проводити регулярний аудит і всеохоплюючий моніторинг, що дає об'єктивну інформацію про стан кібер- і інформаційної безпеки для прийняття оперативних рішень;
- накопичувати статичні дані про роботу інформаційної інфраструктури для прогнозування її розвитку;
- оцінювати ризики інформаційної безпеки.

Управління ризиками безпеки та приватності вимагає участі всієї організації – від старших керівників, які визначають стратегічне бачення, цілі та задачі для організації найвищого рівня, до керівників середнього рівня, які здійснюють планування, виконання та управління проєктами, та осіб, які розробляють, впроваджують, використовують і підтримують системи і процеси.

### 1. Загальні положення щодо оцінки і управління ризиками кібер- і інформаційної безпеки

Активна діяльність міжнародних організацій зі стандартизації підтверджує важливість питань забезпечення кібер- і інформаційної безпеки в системах інформаційних технологій та постійного удосконалення моделей, методів та механізмів безпеки інформаційних технологій. Основний підхід до забезпечення інформаційної безпеки в ІС – стратегія захисту на основі ризику (Risk-Based Protection Strategy). Успішні програми управління ризиками перед-

бачають побудову системи забезпечення інформаційної безпеки, яка інтегрована в організаційну і технічну інфраструктуру. Це вимагає здійснення координованого комплексу заходів, спрямованих на реалізацію вимог безпеки. Ці заходи захисту мають реалізуватися як елементи загального управління, що здійснюється організацією.

Роль управління ризиками стосовно кібер- і інформаційної безпеки під час функціонування та використання інформаційної системи є критичною для досягнення організацією своїх стратегічних цілей та задач.

Виходячи з цих позицій NIST США розробив та впроваджує як методологічну основу забезпечення інформаційної та кібербезпеки концепцію Risk Management Framework (RMF). Концепція RMF впроваджує структурований гнучкий підхід до управління ризиками, що пов'язаний із впровадженням інформаційних систем у бізнес-процеси організації. Концепція RMF викладена у NIST SP 800-37 (Rev 2) та є еволюційним розвитком концепції життєвого циклу системи безпеки (System Security Lifecycle), що використовується NIST з початку 2000-х років. Ця концепція об'єднує серію документів NIST SP 800-XX.

У 2018 р. у зв'язку з актуалізацією питання захисту персональних даних, прийняттям основних положень забезпечення кібербезпеки, впровадженням моделі довірчих систем NIST розпочав перегляд багатьох документів серії NIST SP 800-XX та видав нову версію NIST SP 800-37 – Risk Management Framework in Information Systems and Organizations [1]. У цьому документі впроваджуються принципи управління ризиками та життєвого циклу систем для забезпечення безпеки та приватності.

У нинішній редакції RMF акцентує увагу на управлінні ризиками, створенні умов для забезпечення безпеки та приватності в інформаційних системах на всіх етапах життєвого циклу проєктування системи (SDLC), підтримки інформування про безпеку та приватність на постійний основі за допомогою безперервних процесів моніторингу безпеки, наданні інформації вищому керівництву та керівникам відповідних підрозділів для прийняття рішень стосовно ризиків щодо процесів, ресурсів, персоналу організації, які виникають під час експлуатації та використання систем.

Основні цілі впровадження RMF:

- забезпечення повторюваного процесу забезпечення інформаційної безпеки у відповідності до чинних ризиків;
- впровадження цілісного загальносистемного підходу до управління ризиками безпеки та приватності;
- впровадження єдиної методики класифікації (категоризації) інформаційних систем та загальних заходів безпеки;
- забезпечення управління ризиками в режимі реального часу через впровадження надійних безперервних процесів моніторингу безпеки;
- впровадження засобів автоматизації для забезпечення керівництва необхідною інформацією для прийняття ефективних, економічно доцільних рішень на основі ризиків для ІС, що підтримують місію та бізнес функції організації;
- забезпечення інтеграції вимог безпеки та приватності, заходів захисту в архітектуру підприємства, SDLC, процеси закупівель та постачання, процеси системного інжинірингу;
- об'єднання процесів управління ризиками на рівні організації та бізнес-процесів з процесами управління ризиками на рівні інформаційних систем;
- встановлення відповідальності та спостереження за впровадженням та реалізацією заходів безпеки в ІС.

Під час планування системи управління інформаційною безпекою організація повинна, у відповідності до [2], визначити сукупність методів захисту інформації і організацію проведення аудиту системи управління інформаційної безпеки, визначити ризики та можливості, які потрібно мати на увазі, щоб:

а) гарантувати, що система управління інформаційною безпекою може досягти запланованого результату(-ів);

б) запобігти або зменшити небажані ефекти;

в) досягти постійного вдосконалення.

Організація повинна планувати:

г) дії, які стосуються цих ризиків та можливостей;

д) як саме:

- інтегрувати й упровадити ці дії до процесів її системи управління інформаційною безпекою;

- та оцінювати ефективність цих дій.

Організація повинна визначити та застосовувати процес оцінювання ризиків інформаційної безпеки, який:

а) встановлює та підтримує критерії ризиків інформаційної безпеки, які містять:

– критерії прийняття ризиків; і

– критерії для виконання оцінки ризиків інформаційної безпеки;

б) гарантує, що повторні оцінки ризиків інформаційної безпеки призводять до послідовних, дійових та порівняльних результатів;

в) ідентифікує ризики інформаційної безпеки:

- застосовує процес оцінювання ризиків інформаційної безпеки для ідентифікації ризиків, пов'язаних із втратою конфіденційності, цілісності й доступності в межах сфери застосування системи управління інформаційною безпекою;

- ідентифікує власників ризиків;

г) виконує аналіз ризиків інформаційної безпеки:

- оцінює потенційні наслідки, які будуть результатом реалізації ідентифікованих ризиків;

- оцінює практичну імовірність появи ідентифікованих ризиків;

– визначає рівні ризиків;

д) оцінює ризики інформаційної безпеки:

- порівнює результати аналізу ризиків з визначеними критеріями ризиків; та

- визначає пріоритети проаналізованих ризиків для оброблення ризиків.

Склад і наповнення зазначених процесів залежить від використовуваної методики оцінки та управління ризиками:

Організація повинна визначити та застосовувати процес оброблення ризиків інформаційної безпеки задля:

а) вибору доречних опцій оброблення ризиків інформаційної безпеки з урахуванням результатів оцінки ризиків;

б) визначення всіх заходів безпеки, які необхідно впровадити для вибраної(-их) опції(-ій) оброблення ризиків;

в) порівняння визначення заходів безпеки з наведеними в додатку А [2], і підтвердження, що не було опущено потрібних заходів безпеки;

г) підготовки Положення щодо застосовності, яке містить:

- необхідні заходи безпеки;

- обґрунтування для їх застосування;

- впровадження необхідні заходи безпеки чи ні;

- обґрунтування для виключень заходів безпеки, наданих у додатку А [2] «Цілі заходів безпеки та заходи безпеки» стандарту;

д) розробку плану оброблення ризиків інформаційної безпеки;

е) отримання від власників ризиків підтвердження плану обробки ризиків інформаційної безпеки та згоди на залишкові ризики інформаційної безпеки.

Організація повинна ідентифікувати і оцінити можливості по обробці ризиків. Можливі дії включають в себе наступне [2]:

- застосування відповідних заходів захисту;
- усвідомлене і об'єктивне прийняття ризиків, за умови, що вони строго відповідають

політиці організації та критеріям прийняття ризиків;

- уникнення ризиків;
- перенесення об'єднаних бізнес-ризиків на інші сторони, наприклад страховиків, постачальників.

Методологія визначення оцінки ризиків може бути якісною або кількісною, або деякою комбінацією. Якісна оцінка дуже часто використовується для отримання загального рівня ризику і виокремлення головних ризиків. При якісному підході не використовуються кількісні або грошові вираження для об'єкта оцінки. Замість цього об'єкту оцінки присвоюється показник, що проранжовано за трибальною (низький, середній, високий), п'ятибальною або десятибальною шкалою (0...10). Для збору даних при якісній оцінці ризиків застосовуються опитування цільових груп, інтерв'ювання, анкетування, особисті зустрічі.

При кількісному підході всім елементам оцінки ризиків привласнюють конкретні і реальні кількісні значення. Об'єктом оцінки може бути цінність активу в грошовому вираженні, ймовірність реалізації загрози, збитки від реалізації загрози, вартість захисних заходів та ін.

Кількісний підхід до оцінки ризиків може включати такі етапи:

1. Визначити цінність інформаційних активів в грошовому вираженні.

2. Оцінити в кількісному вираженні потенційний збиток від реалізації кожної загрози щодо кожного інформаційного активу.

3. Визначити ймовірність реалізації кожної із загроз ІБ.

Для цього можна використовувати статистичні дані, опитування співробітників і зацікавлених осіб. У процесі визначення ймовірності розрахувати частоту виникнення інцидентів, пов'язаних з реалізацією даної загрози ІБ за контрольний період (наприклад, за один рік).

4. Визначити загальний потенційний збиток від кожної загрози щодо кожного активу за контрольний період. Значення розраховується шляхом множення разового шкоди від реалізації загрози на частоту реалізації загрози.

5. Провести аналіз отриманих даних по збитку для кожної загрози.

Ідентифікація критеріїв ризику визначає прийняття рішень щодо характеру можливих наслідків та способу їх вимірювання. При визначенні критеріїв необхідно визначити, за якими критеріями прийматимуться рішення щодо необхідності оброблення ризику та критерії, за якими будуть прийматися рішення щодо допустимості чи прийняття ризику. Наявні на сьогодні методи оцінки ризиків в переважній кількості засновані на статистичних підходах. У більшості країн подібна статистика не ведеться, як на державному рівні, так і на рівні підприємств. Саме це обмежує можливості засобів оцінки, наприклад відсутність інформації для використання вхідних даних для оцінки ризику. Загальне оцінювання ризику дає змогу впроваджувати необхідні міри на рівні підрозділів, проєктів, конкретних ризиків або на рівні організації в цілому. Після завершення загального оцінювання ризику провадять обробляння ризику, що передбачає прийняття заходів, які дають можливість зменшити ймовірність виникнення ризиків та їх вплив на систему.

Ризики інформаційної безпеки характеризуються двома параметрами: потенційним збитком для організації та ймовірністю реалізації. Використання для аналізу ризиків сукупності цих двох характеристик дозволяє порівнювати ризики з різними рівнями шкоди і ймовірності, приводячи їх до вигляду зрозумілому для осіб, котрі приймають рішення щодо мінімізації ризиків в організації.

## 2. Критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки

При створенні системи управління ІР постає питання вибору заходів захисту, що забезпечують зниження виявлених в процесі аналізу ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих коштів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність заходів, спрямованих на зниження ризиків

інформаційної безпеки, і розробити архітектуру СУІБ організації, максимально ефективну для її специфіки діяльності і спрямовану на зниження саме її ризиків інформаційної безпеки.

Проведені дослідження дозволяють сформулювати критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки:

– наявність науково-методичного обґрунтування методу для оцінки і управління ризиками;

– відповідність вимогам сучасних стандартів і нормативних документів у сфері створення систем управління інформаційною безпекою;

– простота проведення заходів з оцінки ризиків (ОР) із можливістю залучення на окремих етапах ОР вузькоспеціалізованих фахівців;

– можливість застосування принципів системності та використання засобів структурного аналізу і автоматизованих методів прийняття рішень;

– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;

– можливість отримання результатів щодо ОР у якісному та кількісному представленні;

– можливість збору інформації, що буде вихідним матеріалом формування (редагування) концепції та розробки політики інформаційної і кібербезпеки Організації, робіт з ОР,

– наявність програмного забезпечення для обробки результатів у повному обсязі із зрозумілим та дружнім інтерфейсом;

– структурованість та модульність складових методу;

– наявність модулю економічного підрахунку вартості проведення ОР та впровадження системи управління інформаційною безпекою;

– наявність модулю економічного обґрунтування доцільності впровадження заходів захисту;

– придатність до застосування як в існуючих інформаційних системах (ІС), так і для ІС, що розробляються;

– наявність шаблонів для звітних документів;

– наочність результатів проведення ОР для Замовника;

– наявність каталогів: загроз, типів інформації, порушників, заходів захисту із встановленими на множинах відносинах причино-наслідкового зв’язку та інші.

## 3. Порівняльний аналіз методів управління ризиками інформаційної і кібербезпеки

Розглянемо загальну характеристику та проведемо порівняльний аналіз широко застосовуваних методик і методів управління і оцінки ризиками інформаційної і кібербезпеки у відповідності до наведених у розд. 2 та інших критеріїв.

1. Фреймворк "NIST Risk Management Framework" – на базі американських урядових стандартів NIST (National Institute of Standards and Technology), включає в себе набір взаємозв'язаних стандартів:

– Стандарт NIST SP 800-30 "Guide for Conducting Risk Assessments" ("Керівництво з проведення оцінки ризиків") сфокусований на ІТ, інформаційній безпеці (ІБ) і операційних ризиках, описує підхід до процесів підготовки і проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки;

– Стандарт NIST SP 800-39 "Managing Information Security Risk" пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Даний стандарт описує методологію процесу управління ризиками: визначення, оцінка ризиків інформаційної безпеки, реагування та моніторинг ризиків;

– Стандарт NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations" пропонує для забезпечення безпеки і конфіденційності використовувати підхід управління життєвим циклом систем;

– Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" описує підхід до процесу моніторингу інформаційних систем і IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ і необхідність їх перегляду.

2. Стандарти управління ризиками інформаційної безпеки Міжнародної організації зі стандартизації ISO (International Organization for Standardization):

– Стандарт ISO / IEC 27005: 2018 "Information technology – Security techniques – Information security risk management" («Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризиків інформаційної безпеки») входить в серію стандартів ISO 27000 та є логічно взаємопов'язаним з іншими стандартами по ІБ з цієї серії. Даний стандарт відрізняється фокусом на ІБ при розгляді процесів управління ризиками;

– Стандарт ISO / IEC 27102: 2019 "Information security management – Guidelines for cyber-insurance" пропонує підходи до оцінки необхідності придбання кіберстраховки як заходу обробки ризиків безпеки інформаційних систем, а також до оцінки і взаємодії зі страховиком;

– Серія стандартів ISO / IEC 31000: 2018 описує підхід до ризик-менеджменту без прив'язки до IT / ІБ. У цій серії варто відзначити стандарт ISO / IEC 31010: 2019 "Risk management – Risk assessment techniques".

3. Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки основних ризиків інформаційної безпеки, з фокусом тільки на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем і всіх бізнес-процесах компанії.

5. Стандарт AS / NZS 4360 є австралійським і новозеландським стандартом з фокусом не тільки на IT-системах, але і на бізнес-здоров'я компанії, тобто пропонує більш глобальний підхід до управління ризиками інформаційної безпеки (наприклад, в банку). Відзначимо, що даний стандарт зараз замінений на стандарт AS / NZS ISO 31000-2009.

6. Методологія FMEA (Failure Modes and Effect Analysis) пропонує проведення оцінки системи з точки зору її слабких місць для пошуку ненадійних елементів.

7. Методологія CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) пропонує використання автоматизованих засобів для управління ризиками інформаційної безпеки.

8. Методологія FAIR (Factor Analysis of Information Risk) – Фреймворк для проведення кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками на основі економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

9. Концепція COSO ERM (Enterprise Risk Management) описує шляхи інтеграції ризик-менеджменту зі стратегією і фінансової ефективністю діяльності компанії і акцентує увагу на важливість їх взаємозв'язки.

Проведемо порівняльний аналіз окремих перерахованих методів у відповідності до критеріїв, наведених у розділі 2.

## 4. Методика NIST 800-30

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків National Institute of Standards and Technology (NIST), яка визначена 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 [3]. 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 спеціаль-

них 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.

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 1.

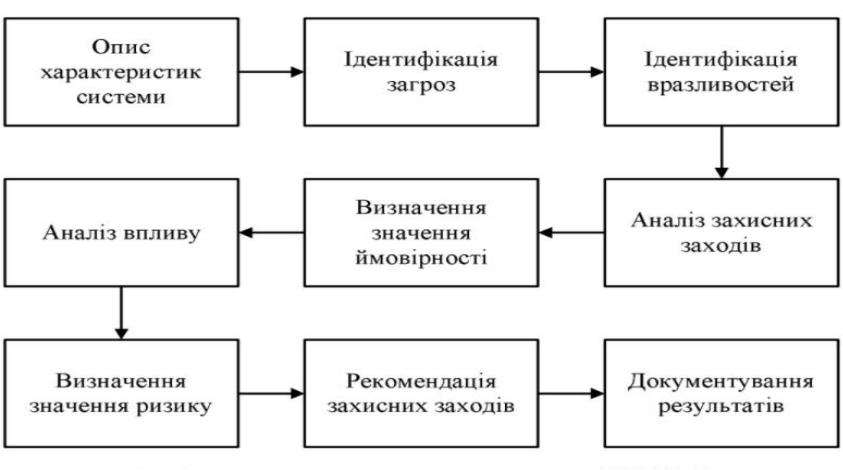


Рис. 1. Алгоритм методики управління ризиками NIST 800-30

Переваги методу NIST 800-30:

– відносна простота проведення заходів з оцінки ризиків (ОР);
– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;
– детально описує всі можливі ризики для інформаційних активів;
– припускає використання як способів обробки ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику);
– наявність програмного забезпечення для обробки результатів, що реалізовує принципи методики;

Метод NIST 800-30 має деякі обмеження для застосування, а саме:

– довготривалий процес аналізу і оцінки ризиків;
– оцінювання ризиків проводиться лише за трирівневою шкалою, що істотно обмежує можливості методики загалом.

### 5. Методика CRAMM

Методика CRAMM (CCTA Risk Analysis and Management Method), розроблена Службою безпеки Великобританії, базується на стандартах управління інформаційної безпеки серії BS7799 (в даний час перероблені в ISO 27000) і описує підхід до якісної оцінки ризиків [4].

При цьому перехід до шкали значень якісних показників відбувається за допомогою спеціальних таблиць, що визначають відповідність між якісними та кількісними показниками. Оцінка ризику проводиться на основі аналізу цінності ІТ-активу для бізнесу, вразливостей, загроз і ймовірності їх реалізації.

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.

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 ОР 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.

Алгоритм методики CRAMM надано на рис. 2

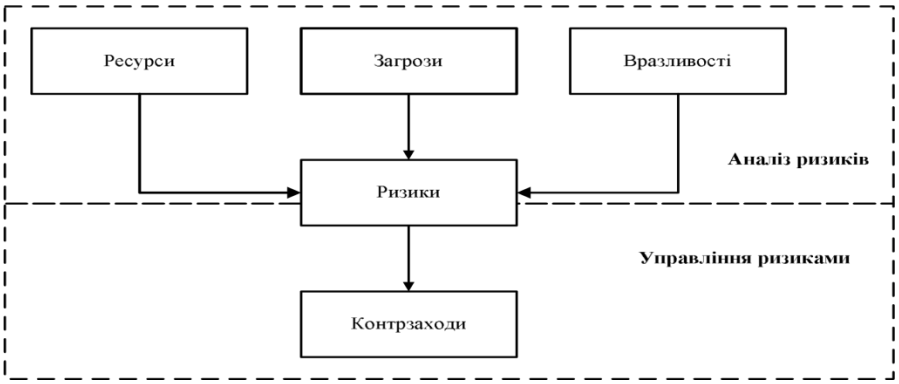


Рис. 2. Алгоритм методики управління ризиками CRAMM

Процес управління ризиками за методикою CRAMM складається з наступних етапів:

1. Ініціювання (Initiation). На цьому етапі проводиться серія інтерв'ю з зацікавленими в процесі аналізу ризиків інформаційної безпеки особами, в тому числі з відповідальними за експлуатацію, адміністрування, забезпечення безпеки і використання ІТ-активів, для яких проводиться аналіз ризиків. В результаті дається формалізований опис області для подальшого дослідження, її кордонів і визначається склад залучених в аналіз ризиків осіб.

2. Ідентифікація та оцінка ІТ-активів (Identification and Valuation of Assets). Визначається перелік ІТ-активів, які використовуються організацією в певній галузі дослідження. Відповідно до методології CRAMM ІТ-активи можуть бути одного з наступних типів:

– дані;
– програмне забезпечення;
– фізичні активи.

Для кожного активу визначається його критичність для діяльності організації і спільно з представниками підрозділів, що використовують ІТ-актив для вирішення прикладних

завдань, оцінюються наслідки для діяльності організації від порушення його конфіденційності, цілісності та доступності.

3. Оцінка загроз і вразливостей (Threat and Vulnerability Assessment). На додаток до оцінки критичності ІТ-активів важливою частиною методології CRAMM є оцінка ймовірності загроз і вразливостей ІТ-активів. Методологія CRAMM містить таблиці, що описують відповідність між уразливими ІТ-активів і погрозами, які можуть впливати на ІТ-активи через ці уразливості. Також є таблиці, що описують збиток для ІТ-активів в разі реалізації цих загроз. Даний етап виконується тільки для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів забезпечення інформаційної безпеки. Визначення актуальних вразливостей і загроз проводиться шляхом інтерв'ювання осіб, відповідальних за адміністрування та експлуатацію ІТ-активів. Для інших ІТ-активів методологія CRAMM містить набір необхідних базових заходів забезпечення інформаційної безпеки.

4. Обчислення ризику (Risk Calculation). Обчислення ризику здійснюється за формулою

$$\text{Ризик} = \text{Р (реалізації)} * \text{Збиток}.$$

При цьому ймовірність реалізації ризику обчислюється за формулою

$$\text{Р (реалізації)} = \text{Р (загрози)} * \text{Р (уразливості)}.$$

На етапі обчислення ризиків для кожного ІТ-активу визначаються вимоги до набору заходів щодо забезпечення його інформаційної безпеки за шкалою від «1» до «7», де значенням «1» відповідає мінімальний необхідний набір заходів щодо забезпечення інформаційної безпеки, а значенням «7» – максимальний.

5. Управління ризиком (Risk Management). На основі результатів обчислення ризику методологія CRAMM визначає необхідний набір заходів щодо забезпечення інформаційної безпеки. Для цього використовується спеціальний каталог, що включає близько чотирьох тисяч заходів. Рекомендований методологією CRAMM набір заходів порівнюється з заходами, які вже прийняті організацією. В результаті ідентифікуються області, які потребують додаткової уваги в частині застосування заходів захисту, і області з надлишковими заходами захисту. Дана інформація використовується для формування плану дій зі зміни складу застосовуваних в організації заходів захисту – для приведення рівня ризиків до необхідного рівня.

Методологія CRAMM у значній мірі відповідає критеріям, що наведено у розд. 2, це, насамперед:

– 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;

– наявність зрозумілого формалізованого опису методології зводить до мінімуму можливість виникнення помилок при реалізації процесів аналізу, оцінки та управління ризиками;

– наявність засобів автоматизації аналізу ризиків дозволяє мінімізувати трудовитрати і час виконання заходів з аналізу та управління ризиками;

– наявність каталогів загроз, порушників, вразливостей, наслідків, заходів забезпечення інформаційної безпеки, що спрощує вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу, оцінки та управління ризиками.

Зазначена методологія має і суттєві обмеження для застосування, які обумовлені такими чинниками:

– висока складність і трудомісткість збору вихідних даних, що вимагає залучення значних ресурсів усередині організації або ззовні;

– великі витрати ресурсів і часу на реалізацію процесів аналізу та управління ризиками інформаційної безпеки;

– залучення великої кількості зацікавлених осіб вимагає значних витрат на організацію спільної роботи, комунікацій усередині проєктної команди і узгодження результатів;

– неможливість оцінити ризики в грошах ускладнює використання результатів оцінки ризиків ІБ при техніко-економічному обґрунтуванні інвестицій, необхідних для впровадження засобів і методів захисту інформації.

CRAMM широко застосовується як в урядових, так і в комерційних організаціях по всьому світу, будучи фактично стандартом управління ризиками інформаційної безпеки в Великобританії. Методика може бути успішно застосована у великих організаціях, орієнтованих на міжнародну взаємодію і відповідність міжнародним стандартам управління, які здійснюють початкове впровадження процесів управління ризиками інформаційної безпеки для покриття ними всієї організації відразу. При цьому організації повинні мати можливість виділення значних ресурсів і часу для застосування CRAMM.

### 6. Метод OCTAVE

Метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблений 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.

Зміст методики OCTAVE [5] 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 проєктної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять 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 інформаційної безпеки (ІБ).

Алгоритм цієї методики зображено на рис. 3.

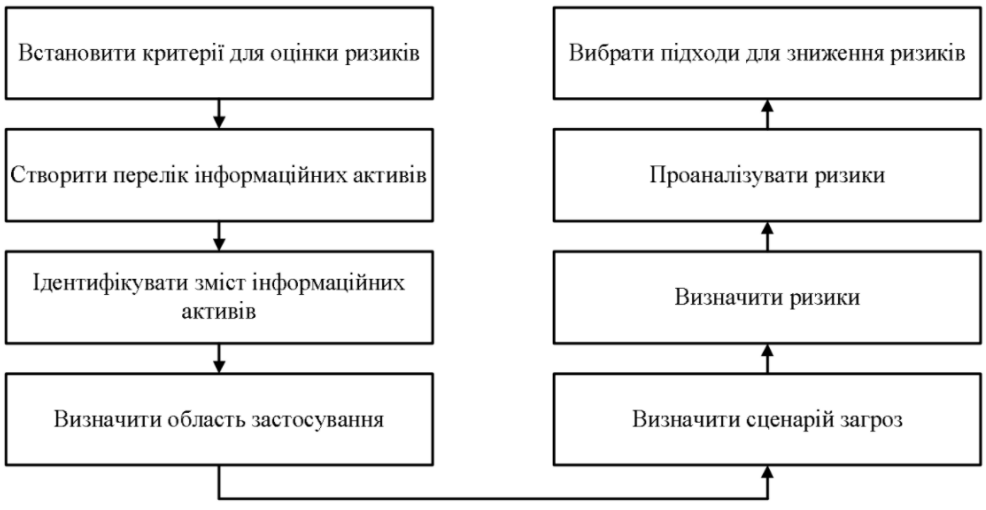


Рис. 3. Алгоритм методики управління ризиками OCTAVE

До показників методики OCTAVE, що відповідають критеріям обрання методів оцінки ризиків, можна віднести:

– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;
– можливість отримання результатів щодо ОР у якісному та кількісному представленні;
– є комерційні програмні продукти, що реалізовують положення методики;
– високий рівень гнучкості при застосуванні.

Тим не менш даній методиці притаманні низка недоліків, а саме:
– не дає можливості реалізовувати кількісну оцінки ризиків;
– припускає можливість як способів обробки ризиків лише його зниження і прийняття.

### 7. Методологія COBIT

Методологія COBIT for Risk [6] розроблена асоціацією ISACA (Information Systems Audit and Control Association) в 2013 р. і базується на кращих практиках управління ризиками (COSO ERM, ISO 31000, ISO\IEC 27xxx і ін.). Методологія розглядає ризики інформаційної безпеки стосовно ризиків основної діяльності організації, описує підходи до реалізації функції управління ризиками інформаційної безпеки в організації та до процесів якісного аналізу ризиків інформаційної безпеки і управління ними.

При реалізації функції і процесу управління ризиками в організації методологія виділяє наступні компоненти, що впливають як на ризики інформаційної безпеки, так і на процес управління ними:
– принципи, політики, процедури організації;
– процеси;
– організаційна структура;
– корпоративна культура, етика і правила поведінки;
– інформація;
– IT-сервіси, IT-інфраструктура і додатки;
– люди, їх досвід і компетенції.

Основним елементом аналізу та управління ризиками інформаційної безпеки відповідно до методології є ризикові сценарії. Кожен сценарій являє собою «опис події, яка в разі виникнення, може привести до невизначеного (позитивного або негативного) впливу на досягнення цілей організації».

Методологія містить більше 100 ризикових сценаріїв, що охоплюють такі категорії впливу:
– створення та обслуговування портфелів IT-проєктів;
– управління життєвим циклом програми/проєкту;
– інвестиції в IT;
– експертиза і навички персоналу IT;
– операції з персоналом;
– інформація;
– архітектура;
– IT-інфраструктура;
– програмне забезпечення;
– неефективне використання IT;
– вибір і управління постачальниками IT;
– відповідність нормативним вимогам;
– геополітика;
– крадіжка елементів інфраструктури;
– шкідливе програмне забезпечення;
– логічні атаки;
– техногенне вплив;
– довкілля;
– природні явища;
– інновації.

Для кожного ризикового сценарію в методології визначено ступінь його приналежності до кожного типу ризиків:

– стратегічні ризики – ризики, пов'язані з втраченими можливостями використання ІТ для розвитку та підвищення ефективності основної діяльності організації;

– проєктні ризики – ризики, пов'язані з впливом ІТ на створення або розвиток існуючих процесів організації;

– ризики управління ІТ та надання ІТ-сервісів – ризики, пов'язані із забезпеченням доступності, стабільності і надання користувачам ІТ-сервісів з необхідним рівнем якості, проблеми з якими можуть привести до збитку для основної діяльності організації.

Кожен ризиковий сценарій містить наступну інформацію:

– тип джерела загрози – внутрішній/зовнішній;

– тип загрози – зловмисні дії, природне явище, помилка і ін. ;

– опис події – доступ до інформації, знищення, внесення змін, розкриття інформації, крадіжка та ін. ;

– типи активів (компонентів) організації, на які впливає подія – люди, процеси, ІТ-інфраструктура та ін. ;

– час події.

У разі реалізації ризикового сценарію діяльності організації завдається шкода. Таким чином, при аналізі ризиків інформаційної безпеки відповідно до методології COBIT for Risk проводиться виявлення актуальних для організації ризикових сценаріїв і заходів зниження ризиків, спрямованих на зменшення ймовірності реалізації цих сценаріїв.

Для кожного з виявлених ризиків проводиться прийняття одного з рішень щодо обробки ризику:

– уникнення ризику;

– прийняття ризику;

– передача ризику;

– зниження ризику.

Подальше управління ризиками здійснюється шляхом аналізу залишкового рівня ризиків і прийняття рішення про необхідність реалізації додаткових заходів зниження ризиків. Методологія містить рекомендації щодо впровадження заходів зниження ризиків стосовно кожного з типів компонентів організації.

З точки зору практичного застосування, можна виділити такі переваги методології COBIT for Risk:

– відповідність вимогам сучасних стандартів у сфері створення систем управління інформаційною безпекою (СУІБ);

– зв'язок із загальною бібліотекою COBIT і можливість використовувати підходи та «ІТ-контролі» (заходів щодо зниження ризиків) з суміжних областей, що дозволяють розглядати ризики інформаційної безпеки та заходи щодо їх зниження стосовно впливу ризиків на бізнес-процеси організації;

– багаторазово апробований метод, за яким накопичені значний досвід і професійні компетенції і результати якого визнаються міжнародними інститутами;

– наявність зрозумілого формалізованого опису методології дозволяє звести до мінімуму помилки при реалізації процесів аналізу та управління ризиками;

– є універсальною і підходить для організацій як державного, так комерційного сектору;

– високий рівень гнучкості.

– каталоги ризикових сценаріїв і «ІТ-контролів» дозволяють спростити вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками;

– можливість використання методології при проведенні аудитів дозволяє знизити трудовитрати і необхідний час для інтерпретації результатів зовнішніх і внутрішніх аудитів.

При цьому методології COBIT for Risk притаманні такі недоліки і обмеження:

– висока складність і трудомісткість збору вихідних даних вимагає залучення значних ресурсів або всередині організації, або ззовні;

– допускає лише якісну (суб'єктивну) оцінку співвідношення втрат від загроз безпеки;

– значна трудомісткість реалізації методу.

Даний метод застосовується як в урядових, так і в комерційних структурах. Метод є найбільш ефективним для великих технологічних організацій або організацій з високим ступенем залежності основної діяльності від інформаційних технологій, для таких, що вже використовують (або планують використовувати) стандарти і методики COBIT для управління інформаційними технологіями та мають необхідні для цього ресурси та компетенції. В цьому випадку можлива ефективна інтеграція процесів управління ризиками інформаційної безпеки та процесів загального управління IT та досягнення синергетичного ефекту, який дозволить оптимізувати витрати на реалізацію процесів аналізу та управління ризиками інформаційної безпеки.

### 8. Методи оцінки ризиків безпеки інформації MAGERIT та MEHARI

Інструментарій MEHARI [7, 8] складається з чотирьох модулів (рис. 4), комплексне використання яких дозволяє адаптувати цей метод до використання у будь-якій організації. Розробники MEHARI пропонують такий порядок проведення ОР: оцінка загрози і її потенціалу, визначення ресурсів, які від неї постраждають, визначення заходів захисту (ЗЗ), що дозволяють забезпечити попередження, захист або відновлення бізнес-процесів організації після реалізації загрози. Для кожного етапу надані прикладні засоби MEHARI надають: практичні рекомендації, таблиці, розрахункові формули та шкали оцінок. Супутня документація містить: інструкції та поради щодо ефективного використання бази знань (подана у форматі Excel), а також теоретичні відомості щодо управління ризиками ІБ. Метод MEHARI використовує трьохфакторну модель ризиків ІБ, елементами якої є: імовірність реалізації загрози, рівень вразливості активу до цієї загрози та цінність втраченого активу.

Для побудови дерева загроз, що є актуальними для ресурсів організації, у методі MEHARI запропоновано використовувати метод сценаріїв. Іншою перевагою MEHARI є наявність шкал оцінювання та способу детермінованого визначення залишкових ризиків ІБ.

Крім цього, у MEHARI визначено підхід до класифікації активів різних типів та запропоновано таблицю відповідності кращих практик з MEHARI до заходів, що визначені у стандарті ISO/IEC 27002 (наявність такої можливості є безумовно важливою, враховуючи широке застосування ISO/IEC 27002 у сучасній практиці з організації захисту інформації). У MEHARI запропоновані опитувальні листи, що дозволяють оцінити рівень досконалості ЗЗ, з урахуванням вагових коефіцієнтів відносної значущістю окремих кращих практик, що свідчать про ефективність/досконаліть ЗЗ. Коефіцієнти за замовчуванням можуть бути змінені в ході проведення ОР ІБ.

*Дотримання принципів системного підходу у ході оцінювання ризиків ІБ.*

Забезпечення керованості процесу оцінювання ризиків (ОР), а також повторюваності та порівнюваності результатів можливе за рахунок застосування таких принципів системного підходу:

1. Ієрархічність – цілі, що досягаються у результаті виконання процесів ОР мають знаходитись в ієрархічній залежності, тобто кожен рівень цілей має враховувати цілі та чинники, що є актуальними для нього.

2. Декомпозиція – кожен процес ОР має бути представлений у вигляді сукупності підпроцесів. Кожен із підпроцесів повинен мати власні цілі та критерії (метричні показники) своєї ефективності та результативності.

3. Достатність та логічна незалежність – логіка організації процесів ОР не повинна залежати від набору кращих практик захисту, ЗЗ, множини загроз безпеки та множини активів.

4. Модульність та функціональна автономність – має бути виділено окремі модулі (оцінювання активів, оцінювання ЗЗ тощо), що функціонують незалежно для отримання оцінки ризику ІБ.

5. Адаптивність – метод ОР має забезпечувати необхідний рівень ефективності незалежно від умов зовнішнього середовища, в якому проводиться оцінювання ризиків ІБ.

6. Формалізованість – ОР має забезпечувати отримання зрозумілих (для замовника) кількісних/якісних показників ризику ІБ та показників ефективності впровадження МЗ. Опис заходів, що проводяться у ході ОР, повинен виключати неоднозначність тлумачення, тим самим має забезпечуватися повторюваність і порівнюваність результатів оцінки ризиків ІБ.

7. Структурованість – дані, що збираються у процесі ОР, мають бути структуровані і подані у вигляді, придатному для подальшого використання іншими модулями ОР.

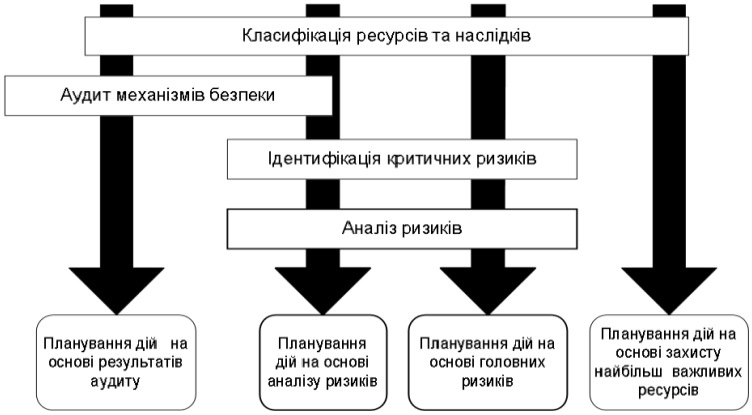


Рис. 4. Модулі MEHARI та підходи до проведення оцінювання ризиків БІ

*Застосування методів та засобів системного аналізу у ході оцінювання ризиків ІБ.*

Зважаючи на складність проведення ОР та обсяг даних, що мають бути зібрані, актуальною є задача вибору методу опису та представлення як самого процесу ОР, так і компонентів інформаційної системи (ІС), що розглядаються як активи організації.

Для розв’язання цієї задачі доцільно використовувати структурні методи – стандартні моделі та методи системного аналізу (СА), що забезпечують подолання складності великих систем шляхом декомпозиції їх на підсистеми [9].

Традиційно прикладні методи структурного аналізу (СА) поділяють на три групи:

- діаграми, що ілюструють функції, які система повинна виконувати, і зв'язки між цими функціями (DFD, SADT (IDEF0));
- діаграми, що моделюють дані і їх взаємозв'язки (ERD);
- діаграми, що моделюють поведінку системи (STD).

Мабуть найважливіший клас задач, що вирішується у ході ОР, є клас задач прийняття рішень. Рішення можуть стосуватися: визначення границь оцінювання, визначення рівня критичності інформаційних ресурсів, вибору пар загроза/інформаційний ресурс, визначення ефективності ЗЗ тощо. Для підвищення ефективності таких рішень, а також забезпечення порівнюваності та повторюваності результатів оцінки пропонується застосовувати методи підтримки та прийняття рішень. Наприклад, для генерування множини альтернативних рішень, що задовольняють заданим умовам, у СА широко використовуються такі методи: метод колективної генерації ідей, метод сценаріїв, метод Дельфі, морфологічні методи тощо. Однією з ознак, що можуть використовуватися для класифікації методів оцінювання і вибору альтернатив є кількість критеріїв, що вони дозволяють враховувати. Найкраща альтернатива може обиратися за значенням цільової функції, вид та правила побудови якої визначаються використовуваним математичним апаратом.

Для проведення ОР у методах Magerit [10, 11] та MEHARI використовуються такі методи та прийоми СА: композиція, декомпозиція, прикладні методи функціонального структурного аналізу IDEF-0 та DFD, експертні методи, метод Дельфі, метод сценаріїв, табличне завдання відповідностей, критеріальний метод вибору за результатами бінарного оцінюванням.

IDEF-0 – стандарт, що визначає технологію опису системи у виді множини взаємозалежних дій або функцій. Особливість IDEF-0 – функціональна спрямованість, це дозволяє чітко відокремити аспекти призначення системи від аспектів її фізичної реалізації. Опис системи організований у вигляді ієрархічно впорядкованих та взаємопов'язаних діаграм. Вершину структури займає загальний опис призначення та взаємозв'язок системи з оточуючим середовищем, коріння – найбільш деталізовані описи підлеглих функцій, що виконує система.

Слід відмітити, що ступінь деталізації опису процесів ОР у методі Magerit надає достатні дані для побудування родини діаграм процесів ОР у нотації IDEF-0. Даними для цього слугують визначені у методі Magerit: структура процесу; продукти кожного етапу; вхідні та вихідні дані; технологія отримання; керівна інформація; функції та обов'язки учасників; перелік виконавців тощо.

На рис. 5 наведено контекстну діаграму мета процесу ОР, на рис. 6 – результат моделювання під процесу ОР проміжного рівня деталізації [12].

DFD – стандарт для створення моделі потоків інформації, що циркулює в ІТС. Модель системи визначається як ієрархія діаграм потоків даних, що описують асинхронний процес перетворення інформації від введення у систему до отримання користувачем. DFD визначає, яким чином кожний процес перетворює вхідні дані у вихідні та дозволяє виявити співвідношення між процесами.

Розробниками Magerit було запропоновано використовувати DFD на етапі збору інформації, що використовується для визначення цінності активів.

Метод Дельфі – складається з кількох етапів, що циклічно повторюються до моменту прийняття компромісного рішення: проведення індивідуальних анкетних опитувань, обробка результатів, ознайомлення експертів із результатами, повторне анкетне опитування.

У Magerit пропонується використовувати метод Дельфі для ідентифікації елементів, що враховуються при оцінці ризиків БІ – активів, загроз, механізмів захисту тощо.

Метод сценаріїв передбачає підготовку та узгодження уявлень щодо проблеми або об'єкту, що аналізується, у письмовому вигляді. Зазвичай, текст містить логічну послідовність подій або можливі варіанти вирішення проблеми, впорядковані за хронологією. Сценарій передбачує змістовні міркування, що забезпечують деталізований розгляд проблеми, та результати кількісного техніко-економічного або статистичного аналізу з попередніми висновками, що можна отримати на їх основі. У методі MEHARI запропоновано розвинутий перелік ризик-сценаріїв, що дозволяють провести кількісне оцінювання рівнів ризиків БІ.

Критеріальний метод – кожна окрема альтернатива оцінюється одним або кількома показниками. Таким чином, порівняння альтернатив зводиться до обчислення узагальненого показника та порівняння альтернатив за його значенням на основі уведених критеріїв.

Метод попарного порівняння – альтернативи (А та В) порівнюються із використанням бінарних оцінок: (А та В) порівнюються із використанням бінарних оцінок: $A \leq B$, або $A > B$, або $A = B$.


Рис. 5. Контекстна діаграма процесу ОР у нотації IDEF-0

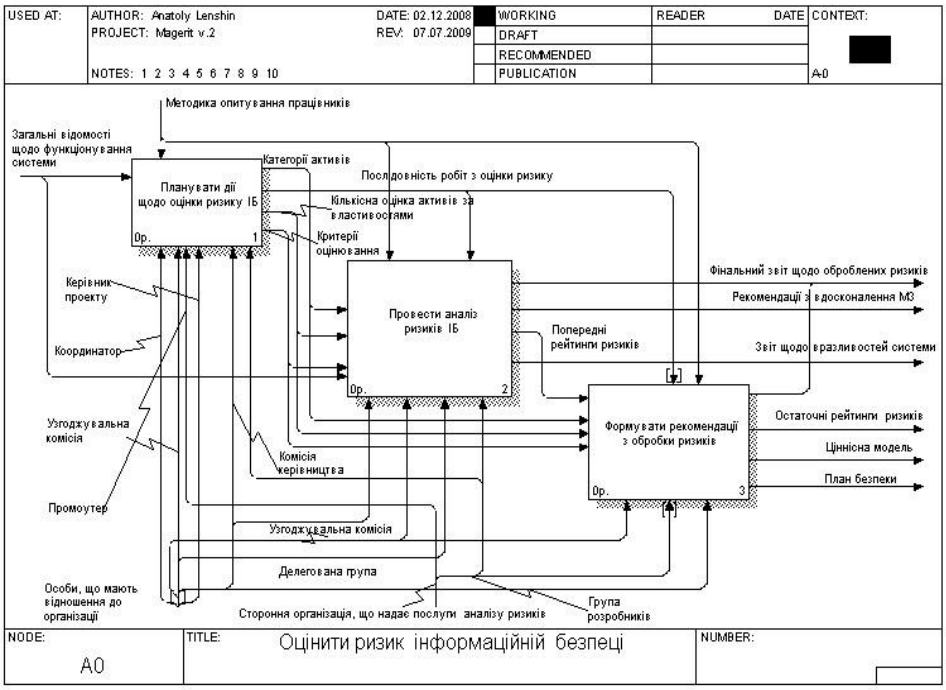


Рис. 6. Декомпозиція мета процесу ОР у нотації IDEF-0

За результатами дослідження зазначених методів (Magerit та MEHARI) можна стверджувати, що кожному із методів притаманні певні позитивні риси, які свідчать про системність підходу до проведення ОР. Проведемо порівняння цих методів за такими критеріями: ступінь відповідності стандартам (К1), організація процесів згідно з моделлю PDCA (К2), модель ризиків, що використовується (К3), вимоги до звітної документації (К4), підтримка методів аналізу вартості проведення ОР (К5), ступінь формалізації алгоритму (К6), суворість вимог до складу аналітичної групи (К7), наявність засобів проведення ОР (К8), види ЗЗ, що розглядаються (К9), використовувані методи збору даних (К10), наявні критерії оцінки (К11), підхід до обчислення ризику (К12), використовувані методи СА (К13), допоміжне ПЗ (К14). Результати порівняння методів ОР Magerit та MEHARI зведено до табл. 1.

Таблиця 1

| Номер | Magerit | MEHARI |
|---|---|---|
| К1 | Розроблений з урахуванням стандартів BSI. Сумісний з профілями захисту ISO/IEC 15408. Сумісний з ISO/IEC 13335 та ISO/IEC 27001 | Повністю відповідає ISO/IEC 27002. Формально відповідає ISO/IEC 13335 та ISO/IEC 27001 |
| К2 | Підтримується | Підтримується |
| К3 | Двофакторна: імовірність загрози та рівень наслідків | Трьохфакторна: імовірність загрози, рівень вразливості, рівень наслідків |
| К4 | По закінченні кожного етапу обов'язково складається документ за визначеною формою | Обов'язковим є розробка політики безпеки. Припускаються записи у довільній формі |
| К5 | Присутні бази для проведення розрахунків | Не підтримуються |
| К6 | Високий, кожний етап має фіксований вхід, вихід та дію | Середній, збираються дані лише для необхідних структур (таблиць) |
| К7 | Чітко визначені | Присутні у загальному вигляді |
| К8 | Діаграми процесів даних, діаграма цінності активів, типи активів, база МЗ, перелік загроз | Карта природного ризику, карта МЗ, база ризик-сценаріїв, опитувальні листи |
| К9 | Два види: зменшуючи частоту загрози, зменшуючи наслідки | 5 видів: попереджуючі, запобіжні, захисні, пом'якшуючі, відновлюючи |
| К10 | Співбесіди з робітниками, опитувальні листи | Опитувальні листи |
| К11 | Критерії для оцінки активів, цінності активів | Критерії для оцінки ризику, статус-ризик |
| К12 | Передбачено розрахунок відхиленого ризику як різниці між базовим та залишковим. Опис алгоритму відсутній | Обчислення з урахуванням множини факторів, передбачає обчислення коефіцієнту вагомості ризику. Наведено опис алгоритму |
| К13 | Експертні методи, метод Дельфі, опис процесів, достатній для побудови IDEF-0 діаграм, DFD | Бальна шкала оцінювання, використання вагових коефіцієнтів, метод сценаріїв |
| К14 | Фрагменти коду для подання даних як XML. | База знань MEHARI |

Метод Magerit містить формалізовану, ієрархічно структуровану концепцію проведення ОР, визначені обов'язки і ролі учасників ОР. До переваг методу MEHARI слід віднести формалізований модуль оцінки та розгалужену базу ризик-сценаріїв, спосіб класифікації активів, наявність баз даних у вільному доступі.

З урахуванням зазначеного можуть бути висунуті вимоги щодо розробки вдосконаленого методу ОР, що матиме переваги Magerit та MEHARI.

1. При формуванні групи учасників ОР слід використовувати рекомендації Magerit. У ході класифікації активів доцільно застосовувати бази знань MEHARI, взявши за основу критерії цінності та оцінки вартості, що запропоновані у методі Magerit.

2. Визначення загроз доцільно проводити за базами Magerit, при цьому обчислювати показники природного ризику слід згідно з підходом, визначеним у MEHARI.

3. З огляду на детальність опису МЗ у методі MEHARI та наявність таблиць відповідностей з кращими практиками, що визначені у ISO/IEC 27002 (табл. 2), для ідентифікації впроваджених ЗЗ рекомендується використовувати опитувальні листи MEHARI (табл. 3).

Таблиця 2

| Розділ ISO/IEC 27002 | Позначення МЗ з MEHARI |
|---|---|
| 5.1 Політика інформаційної безпеки | |
| 5.1.1 Задокументована політика ІБ | 01A02-01 |
| 5.1.2 Перегляд політики ІБ | 01A02-02 |
| 6. Організація інформаційної безпеки | |
| 6.1 Внутрішня організація | |
| 6.1.1 Затвердження концепції ІБ керівництвом | 01A02-09 |
| 6.1.2 Координація ІБ | 01A02-03:05 |
| 6.1.3 Розподіл обов'язків з ІБ | 01A02-06:07 |

Таблиця 3

| 01E | Управління безперервністю робочих процесів | Так/ Ні | $w_j^i$ | $UL_j^i$ | $LL_j^i$ |
|---|---|---|---|---|---|
| 01E01 | Питання управління безперервністю бізнесу | | | | |
| 01E0101 | Для визначення засад управління безперервністю бізнесу проведений аналіз критичності застосувань і сервісів. Поглиблений аналіз передбачає існування списку інцидентів і ризик-сценаріїв для визначення наслідків | Ні | 4 | 2 | |
| 01E0102 | Аналіз визначає мінімальні системні вимоги для сервісів та застосувань. Системні вимоги узгоджені з власниками/розпорядниками IP | Так | 4 | 2 | 3 |
| 01E0103 | Для розвитку та оновлення планів безперебійної роботи впроваджені та підтримуються процеси OP для кожного IP | Так | 2 | | |

В табл. 4 наведено ще один підхід [13] до вибору методів оцінки ризиків інформаційної безпеки, які можуть бути застосовані у інформаційних системах. Такий підхід враховує низку специфічних вимог, які можуть бути висунуті для обґрунтування вимог до вибору методу оцінки ризиків (вартість, необхідність ліцензування, розмір і складність організації, можливості щодо реалізації процедур обробки ризиків тощо).

Таблиця 4

| Характеристики / Методи | Ідентифікація ризику (Risk iden | Аналіз ризиків (Risk analysis) | Оцінка ризику (risk evaluation) | Ідентифікація ризику (Risk asses ment) | Обробка ризику (Risk treatment) | Прийняття ризику (Risk accepta | Повідомлення про ризик (Risk c munication) | Мови (Languages) | Ціна | Розмір організації (Size of organ tion) | Необхідні навички (skills neede | Ліцензування (Licensing) | Сертифікування (Certification) | Спеціальні засоби підтримки (D cated support tools) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Austrian IT Security Handbook | • • | • | • | • • • | • • • | • • • | • • • | DE | Free | All | ** | N | N | Prototype of charge) |
| CRAMM | • • • | • • • | • • • | | | | | EN, NL | Not fre | Gov, Lar | *** | N | N | CRAMM pert, CRA express |
| Dutch A&K analysi | • • • | • • • | • • • | | | | | NL | Free | All | * | N | N | |
| Ebios | • • • | • • • | • • • | • • • | • • • | • • • | • • • | EN, FR ES | Free | All | ** | Y | N | EBIOS ve 2 (open so |
| ISF methods | • • • | • • • | • • • | • • • | • • • | • • • | • • • | EN | For IS memb | All excep SME | * to * | N | N | Various IS tools(for m bers) |
| ISO/IEC IS 13335-2 (ISO/IEC IS 27005) | • • | • • | • • | • • | • • • | • • • | • • • | EN | Ca. €1 | All | ** | N | N | |
| ISO/IEC IS 17799 | • | | | | • | | | EN | Ca. €1 | All | ** | N | Y | Many |
| ISO/IEC IS 27001 | | | | | • | • | | EN, FR | Ca. €8 | Gov, Lar | ** | Y | Y | Many |
| IT-Grundschultz | • • • | • • • | • • • | • • • | • • • | • • • | • • • | EN, DE | Free | All | ** | Y | Y | Many |
| Marion (replaced by Mehari) | • • • | • • • | • • • | | | | | EN, FR | Not fre | Large | * | N | N | |
| Mehari | • • • | • • • | • • • | | | | | EN, FR | €100-5 | All | ** | N | N | RISICARI |
| Octave | • • | • • | • • | • • | • • | • • | • • | EN | Free | SME | ** | N | N | |
| SP800-30 (NIST) | • • • | • • • | • • • | • • • | • • • | • • • | | EN | Free | All | ** | N | N | |

**Висновки**

NIST США розробив як методологічну основу забезпечення інформаційної та кібербезпеки концепцію Risk Management Framework (RMF). Концепція RMF впроваджує структурований гнучкий підхід до управління ризиками, що пов'язаний із впровадженням інформаційних систем у бізнес-процеси організації.

Система управління інформаційною безпекою (СУІБ) забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. При створенні системи управління ІР постає питання вибору заходів захисту, що забезпечують зниження виявлених в процесі аналізу ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих коштів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність засобів захисту інформації, а також організаційних заходів спрямованих на зниження ризиків інформаційної безпеки, і розробити архітектуру СУІБ організації, максимально ефективну для її специфіки діяльності і спрямовану на зниження саме її ризиків інформаційної безпеки.

На основі наведеного аналізу можна стверджувати, що оптимальним варіантом для вибору методу управління ризиками ІБ в контексті забезпечення неперервності функціонування СУІБ є, зокрема, адаптація та удосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів. Крім того, при виборі того чи іншого методу оцінки ризиків ІБ необхідно враховувати низку чинників (критеріїв), які визначені у розд. 2 і 3 цієї роботи: наявність науково-методичного обґрунтування методу для проведення оцінки і управління ризиками; відповідність вимогам сучасних стандартам і нормативних документів у сфері створення систем управління інформаційною безпекою; простота проведення заходів з оцінки ризиків із можливістю залучення на окремих етапах оцінки ризиків (ОР) вузькоспеціалізованих фахівців; можливість застосування принципів системності та використання засобів структурного аналізу і автоматизованих методів прийняття рішень; можливість адаптації методу ОР до вимог організації залежно від її типу та розміру; можливість отримання результатів щодо ОР у якісному та кількісному представленні; вартість продукту, організаційно-штатна структура та форма власності організації, ступінь критичності інформації, що обробляється, та інші.

**Список літератури:**


1. NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, 2018.
2. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). ДСТУ ISO/IEC 27001:2015.
3. NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems.
4. CRAMM user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001.
5. Методология OCTAVE для оценки информационных рисков [Електроный ресурс]. Режим доступу: http://www.risk24.ru/octave.htm.
6. COBIT 5: A Business Framework for the Governance and Management of Enterprise ISACA, 2012.
7. MEHARI 2007: Concepts and Mechanisms, Club de la Sécurité de l'Information Français.
8. MEHARI 2007: Knowledge Bases, Club de la Sécurité de l'Information Français.
9. Спицнадель В.Н. Основы системного анализа: учеб. пос. / В.Н. Спицнадель. СПб.: Изд. дом «Бизнеспресса», 2000. 326 с.
10. Magerit v2 2006: Book I: The method, Ministerio de Administraciones Publicas, Spain.
11. Magerit v2 2006: Book III: Techniques, Ministerio de Administraciones Publicas, Spain.
12. Потій О.В., Лєншин А.В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу // Зб. наук. праць Харків. ун-ту Повітряних Сил. 2010. Вип. 2(24). С. 85-91.
13. Аналіз методів оцінки ризиків інформаційної безпеки [Електроний ресурс]. Режим доступу: https://www.securitylab.ru/blog/personal/secinsight/19205.php.


*Надійшла до редколегії 04.08.2021*

*Відомості про авторів:*

**Потій Олександр Володимирович** – д-р техн. наук, професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації; Україна; e-mail: potav@ua.fm; ORCID: https://orcid.org/0000-0002-2366-0541

**Горбенко Юрій Іванович** – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора; Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

**Замула Олександр Андрійович –** д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; email: zamylaaa@gmail.com; ORCID: http://orcid.org/0000-0002-8973-6190

**Ісірова Катерина Володимировна –** АТ «інститут інформаційних технологій», аналітик з систем захисту інформації; Україна; e-mail: katerinaisirova@gmail.com; ORCID: https://orcid.org/0000-0002-0250-7636