DOI:**10.33099/2311-7249/2023-47-2-41-47**

УДК: 004.056

Сидоркін Павло Григорович [1]
Горліченко Сергій Олександрович [1]
Некоз Василь Сергійович [1]
Шилан Микола Володимирович [2]

[1] ***Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна***
[2] ***Національний університет оборони України, Київ, Україна***

МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ CRAMM ТА COBIT 5 FOR RISK

Метою статті є проведення детального аналізу відомих методів управління ризиками CRAMM та COBIT 5 for Risk для їх використання стосовно мінімізації впливу ризиків на інформаційну безпеку підприємства (організації, установи). Під час написання статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за тематикою управління ризиками. Зазначений методологічний підхід дає змогу порівняти основні методи управління ризиками. У роботі зазначено, що найбільш поширеними у світі методами та методиками управління ризиками інформаційної безпеки є CRAMM, COBIT for Risk, FRAP, Octave і Microsoft. Проведено ретельний аналіз методів CRAMM і COBIT 5 for Risk. Зазначено що метод CRAMM має етапи ініціювання, ідентифікації й оцінювання IT-активів, оцінювання загроз і вразливостей, визначення ризику. Наведено структуру методології COBIT 5 for Risk, розглянуто компоненти установи стосовно опису функцій і процесів управління ризиками за цією методологією та запропоновано рекомендації щодо впровадження заходів зниження ризиків. Наведено основні переваги та недоліки розглянутих методів управління ризиками. Значимість ризиків інформаційної безпеки зростає через збільшення кількості реалізованих нападів, і з урахуванням їх руйнівного потенціалу. Поряд із визначеними перевагами вони мають і свої обмеження. Зокрема, розглянуті методи ефективно використовуються комерційними компаніями і державними установами, а також можуть бути застосовані під час оцінювання й управління ризиками інформаційної безпеки об'єктів критичної інфраструктури.

Ключові слова: *управління ризиками, потенційна шкода, ранжування ризиків, оцінювання ризиків безпеці інформації, реагування на ризик.*

Вступ

Постановка проблеми. У сучасних умовах агресії російської федерації проти України спостерігається тенденція до зростання кількості нападів на об'єкти критичної інфраструктури і стратегічні промислові об'єкти нашої держави. Це призводить до виведення з ладу систем життєзабезпечення промисловості, що вже спричинило глобальну техногенну катастрофу (знищення греблі *Каховської гідроелектростанції)*. Водночас, ризики інформаційної безпеки (далі – ІБ) входять до категорії найбільш ймовірних ризиків, поряд із природніми катаклізмами, екстремальними погодними умовами та іншими.), Також вони містяться у переліку з шести найбільш критичних ризиків за можливою шкодою. Цей список включає ризики пов'язані із застосуванням зброї масового ураження, природними катаклізмами, погодними аномаліями та нестачею питної води. Рівень захисту об'єктів інформаційної діяльності залежить від ризиків ІБ, що зростають через збільшення кількості реалізованих нападів і з урахуванням їх руйнівного потенціалу. Управління ризиками ІБ та їх підтримка на прийнятному рівні є важливою функцією підприємства (організації, установи) (далі – установа), що реалізується за допомогою комплексних систем захисту інформації. Створення таких систем потребує вибору засобів захисту, що забезпечують зниження впливу потенційних ризиків та виявлених під час аналізу ризиків ІБ без суттєвих витрат на впровадження цих засобів та їх підтримку в робочому стані. Результатом проведеного аналізу ризиків ІБ може бути визначення потрібної та достатньої сукупності засобів захисту інформації, рекомендований перелік організаційних заходів, спрямованих на зниження ризиків ІБ та розроблена (удосконалена) архітектура системи ІБ установи. Це дає змогу створити ефективну систему захисту, яка враховує специфіку діяльності конкретної установи та спрямована на зниження саме її ризиків ІБ. За таких умов процес

управління ризиками складається з двох етапів.

Першим етапом управління ризиками є прийняття рішення відносно ризиків ІБ, що мають бути ідентифіковані та оцінені з погляду шкоди для ІБ установи та ймовірності реалізації ризиків.

Другим етапом управління ризиками є ранжування ризиків щодо визначення пріоритетності під час реагування на ризики для подальшого розроблення плану реагування.

Склад і наповнення наведених етапів залежить від методів управління ризиками та їх оцінювання. Тому питання вибору оптимальних і ефективних методів для управління ризиками ІБ установи та їх оцінювання є важливим науковим завданням. Для вирішення цього завдання потрібно провести аналіз відомих методів управління ризиками.

Аналіз останніх досліджень і публікацій. В Україні розроблено і затверджено низку нормативних документів, що регулюють основні засади інформаційної безпеки, зокрема кібербезпеки стосовно необхідності оцінювання ефективності систем захисту установ та об'єктів критичної інфраструктури, проте єдиного розуміння щодо використання методів оцінювання ризиків ІБ для них не наведено [1; 2]. Водночас, у світі розроблено низку міжнародних стандартів для систем управління інформаційною безпекою, що визначають вимоги до системи управління ІБ управління ризиками, метрики і вимірювання, а також керівництво з їх впровадження. Аналіз цих стандартів проведено у декількох наукових публікаціях. Так, у статті [3] зазначені принципи системного підходу, що мають використовуватися під час оцінювання ризиків безпеки інформації. Докладно описуються лише методи аналізу Magerit та Mehari. В роботі [4] розглянуто загальні положення щодо оцінювання і управління ризиками кібер- і інформаційної безпеки, наведені критерії вибору методів оцінки і управління ризиками та проведено короткий аналіз відомих методів відповідно до критеріїв вибору.

У роботі [5] наведено переваги та недоліки програмного забезпечення для визначення і оцінювання ризиків інформаційної безпеки (CRAMM, CORAS, Risk Watch, OCTAVE, Oracle Crystal Ball) і сформовано ряд рекомендацій щодо доцільності застосування розглянутих програмних засобів. Також у статті [6] проведено аналіз процедур оцінювання інформаційних ризиків з допомогою таких видів програмного забезпечення, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE, що розроблені та функціонують згідно міжнародних стандартів. Слід зазначити, що у роботах [3–6] методологія COBIT for Risk не розглядалась.

Метою статті є проведення детального аналізу методів управління ризиками CRAMM та COBIT 5 for Risk для їх використання стосовно мінімізації впливу ризиків на інформаційну безпеку підприємства (організації, установи).

Виклад основного матеріалу дослідження

Метод аналізу та управління ризиками *CRAMM* (CCTA Risk Analysis and Management Method), розроблений 1985 року у Великобританії і базується на стандартах управління інформаційної безпеки серії BS7799 (переопрацьований в ISO 27000) та описує підхід до якісного оцінювання ризиків [7]. Водночас перехід до шкали значень якісних показників відбувається за допомогою спеціальних таблиць, що визначають відповідність між якісними і кількісними показниками. Оцінювання ризику проводиться на основі аналізу функціонування інформаційних технологій (далі – ІТ), що використовуються в установі з урахуванням цінності ІТ-активу, вразливостей, загроз і ймовірностей їх реалізації відповідно до алгоритму (рис. 1) [3].

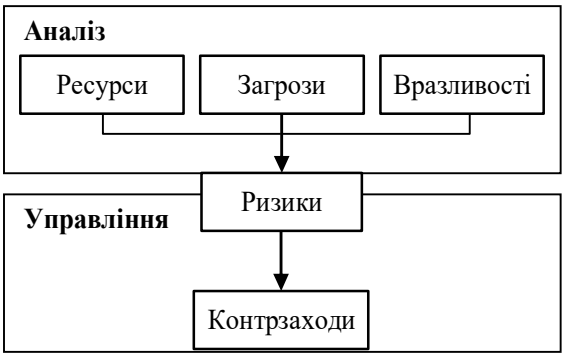

Рисунок 1 – Алгоритм реалізації методу CRAMM

Процес управління ризиками за методом CRAMM складається з таких етапів:

Ініціювання (Initiation). Проводиться серія інтерв'ю із зацікавленими у 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. За підсумками надається формалізований опис області для подальшого дослідження, її меж і визначається склад залучених до аналізу ризиків осіб.

Ідентифікація й оцінювання ІТ-активів (Identification and Valuation of Assets). Визначається перелік ІТ-активів, що використовує організація у визначеній області дослідження. ІТ-активи можуть мати такий вид: дані; програмне забезпечення; фізичні носії.

Для кожного активу визначається його критичність для діяльності організації і спільно з представниками підрозділів, що використовують ІТ-актив для виконання завдань, оцінюються наслідки для діяльності організації від порушення його конфіденційності, цілісності та доступності.

Оцінювання загроз і вразливостей (Threat and Vulnerability Assessment). На доповнення до оцінювання критичності ІТ-активів, важливою є оцінювання ймовірності загроз і вразливостей

ІТ-активів. Метод CRAMM містить таблиці, що описують відповідність між вразливостями ІТ-активів і загрозами, які можуть впливати на них завдяки цим вразливостям. Також маються таблиці, що описують шкоду для ІТ-активів у випадку реалізації цих загроз. Цей етап виконується тільки для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів забезпечення ІБ. Визначення актуальних вразливостей і загроз проводиться шляхом інтерв'ювання осіб, що є відповідальними за адміністрування й експлуатацію ІТ-активів. Для решти ІТ-активів метод CRAMM містить набір потрібних базових заходів забезпечення інформаційної безпеки.

Визначення ризику (Risk Calculation) проводиться за виразом:

$$R = P_{\text{реаліз}} \times S_{\text{шк}}, \quad (1)$$

де $P_{\text{реаліз}} = P_{\text{загрози}} \times P_{\text{уразливості}}$ – ймовірність реалізації ризику;

$S_{\text{шк}}$ – шкода ІТ-активам за реалізації загроз.

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

Визначення ризику (Risk Management). На основі визначеного ризику за виразом (1) розробляється перелік заходів із забезпечення інформаційної безпеки. Для цього використовується спеціальний каталог, що містить до 4 тис. заходів. Рекомендований перелік заходів порівнюється із заходами, які вже застосовані. В підсумку ідентифікуються області, що вимагають додаткової уваги в частині застосування заходів захисту, і області з надлишковими заходами захисту. Ця інформація використовується для формування плану дій зі зміни переліку заходів захисту, що застосовуються в організації з метою приведення рівня ризиків до потрібного стану.

З погляду практичного застосування слід виділити такі переваги методу CRAMM:

апробований метод, за яким накопичено значний досвід і професійні компетенції;

наявність зрозумілого формалізованого опису зводить до мінімуму можливість виникнення помилок за реалізації процесів аналізу та управління ризиками;

наявність засобів автоматизації аналізу ризиків дає змогу мінімізувати трудові витрати і час виконання заходів з аналізу та управління ризиками;

каталоги загроз, вразливостей, наслідків, заходів забезпечення інформаційної безпеки спрощують вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками.

Основними недоліками методу CRAMM є:

складність і трудомісткість збору початкових даних, що потребує 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 потребує значних витрат на організацію спільної роботи, комунікацій всередині проєктної команди та узгодження підсумків;

неможливість оцінити ризики у грошовому еквіваленті ускладнює використання підсумків оцінювання ризиків інформаційній безпеці за техніко-економічного обґрунтування інвестицій, потрібних для впровадження засобів і методів захисту інформації.

Метод CRAMM застосовується як в урядових, так і в комерційних установах, і є фактично стандартом управління ризиками інформаційної безпеки у Великобританії. Метод може бути використаний в установах, що орієнтовані на міжнародну взаємодію та відповідають міжнародним стандартам управління, які здійснюють первісне впровадження процесів управління ризиками ІБ. Водночас така установа має виділяти значні ресурси і час на впровадження методу CRAMM та використання у своїй діяльності.

Відомим методом управління ризиками є *COBIT 5 for Risk* (Control Objectives for Information and Related Technologies – завдання управління за інформаційними та суміжними технологіями) (далі – COBIT), що є методологію управління інформаційними технологіями. Зазначена методологія розроблена асоціацією ISACA (Information Systems Audit and Control Association) базується на найкращих практиках управління ризиками (COSO ERM, ISO 31000, ISO\IEC 27000) [8]. Методологія COBIT розглядає ризики ІБ стосовно основної діяльності установи, описує підходи до реалізації функції управління ризиками ІБ в установі до процесів якісного аналізу ризиків інформаційної безпеки і управління ними. Структура методології наведена на рис. 2.

Компоненти установи стосовно опису функцій та процесів управління ризиками за методологією COBIT наведені на рис 3. Компонентами функції управління ризиками є: процеси, організаційна структура, культура та поведінка, принципи політики, процедури, інформація, пропозиції та ІТ-сервіси, персонал і компетенції. До процесу управління ризиками слід віднести: процес, що містить ризик, ризикові сценарії – віднесення сценаріїв і паролів, інші документи з бібліотеки COBIT. Під час реалізації функції управління ризиками в установі методологія COBIT виділяє компоненти, що впливають як на ризики інформаційної безпеки, так і на процес управління ними, а саме: принципи політики, процедури організації; процеси; організаційна структура; корпоративна культура, етика і правила поведінки; інформація; ІТ-сервіси, ІТ-інфраструктура і додатки; персонал, його досвід і компетенції.

Основним елементом аналізу та управління ризиками ІБ згідно з COBIT є ризикові сценарії. Кожний сценарій є «описом події, яка у випадку виникнення, може призвести до невизначеного (позитивного чи негативного) впливу на досягнення цілей організації».

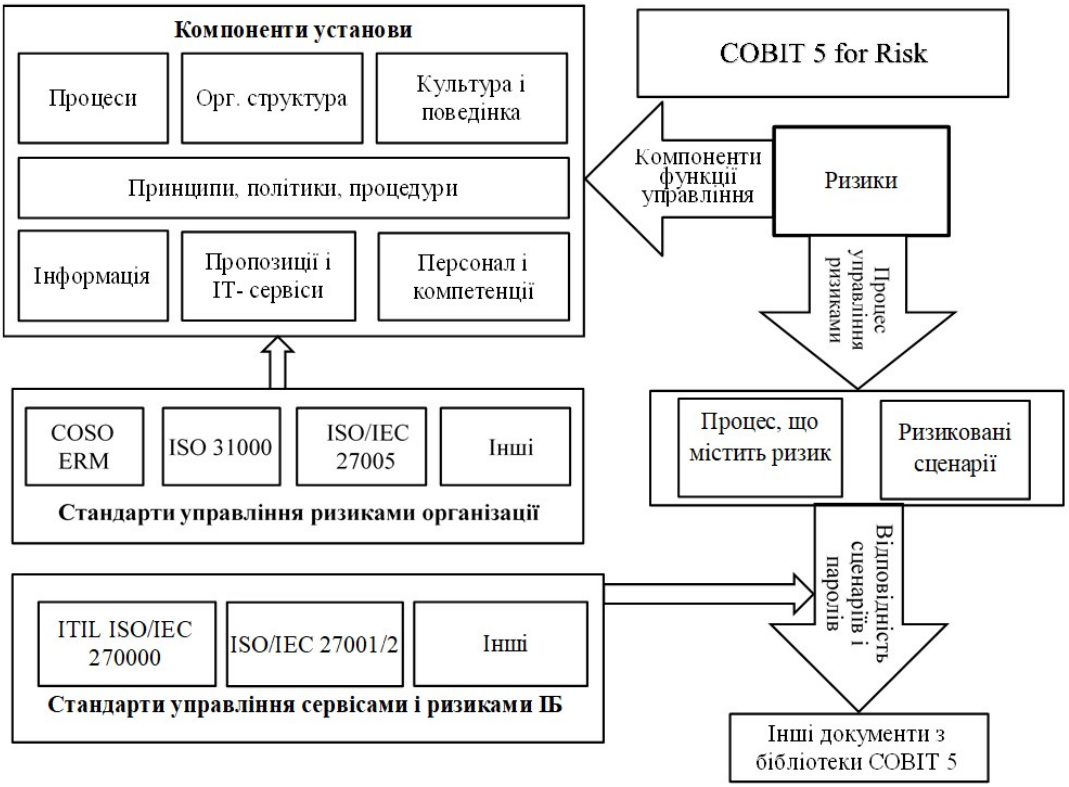

Рисунок 2 – Структура методології COBIT 5 for Risk

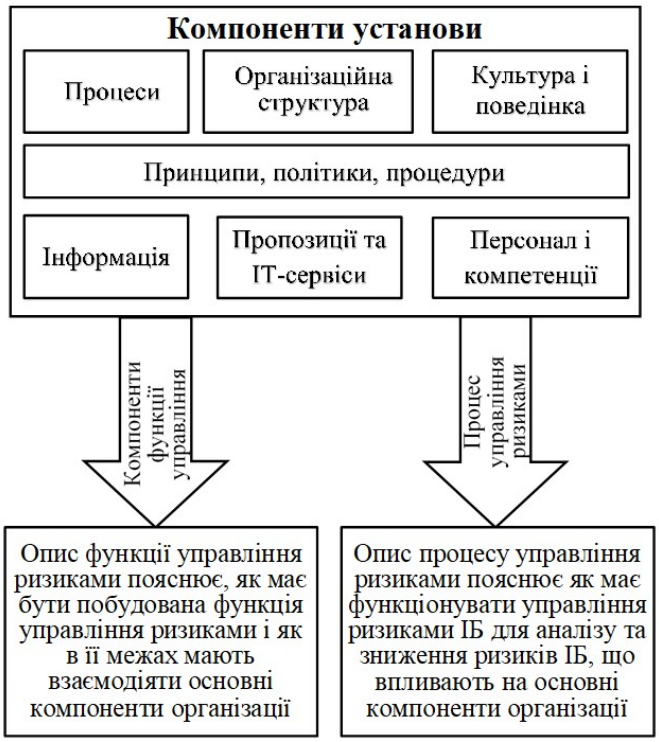

Рисунок 3 – Компоненти установи стосовно опису функцій та процесів управління ризиками за методологією COBIT

Методологія містить більш, ніж 100 ризикових сценаріїв, що охоплюють 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 та управління постачальниками IT; відповідність нормативним вимогам; геополітика; викрадання елементів інфраструктури; шкідливе програмне

забезпечення; логічні напади; техногенний вплив; навколишнє середовище; природні явища; інновації.

Для кожного сценарію визначений ступінь його належності до конкретного типу ризиків:

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

проєктні ризики, що пов'язані з впливом IT на створення чи розвиток існуючих процесів організації;

ризики управління IT і надання IT-сервісів, що пов'язанні із забезпеченням доступності, стабільності та надання користувачам IT-сервісів з потрібним рівнем якості, проблеми, що можуть призвести до втрат у основної діяльності організації.

Кожен ризиковий сценарій містить таку інформацію:

тип джерела загрози – внутрішній або зовнішній;

тип загрози – зловмисна дія, природне явище, помилка;

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

типи активів (компонентів) організації, на які впливає подія – люди, процеси, IT-інфраструктура;

час події.

У випадку реалізації ризикового сценарію діяльності організації заподіюється шкода. Таким чином, під час аналізу ризиків інформаційної безпеки у відповідності з методологією COBIT виявляються актуальні для організації ризикові сценарії і заходи щодо зниження ризиків, спрямованих на зменшення ймовірності реалізації цих сценаріїв. Для кожного з виявлених ризиків проводиться аналіз його відповідності ризик-апетиту установи з подальшим прийняттям одного з таких рішень: уникання ризику; прийняття ризику; передача ризику; зниження ризику.

Подальше управління ризиками ІБ 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 (рис. 4).

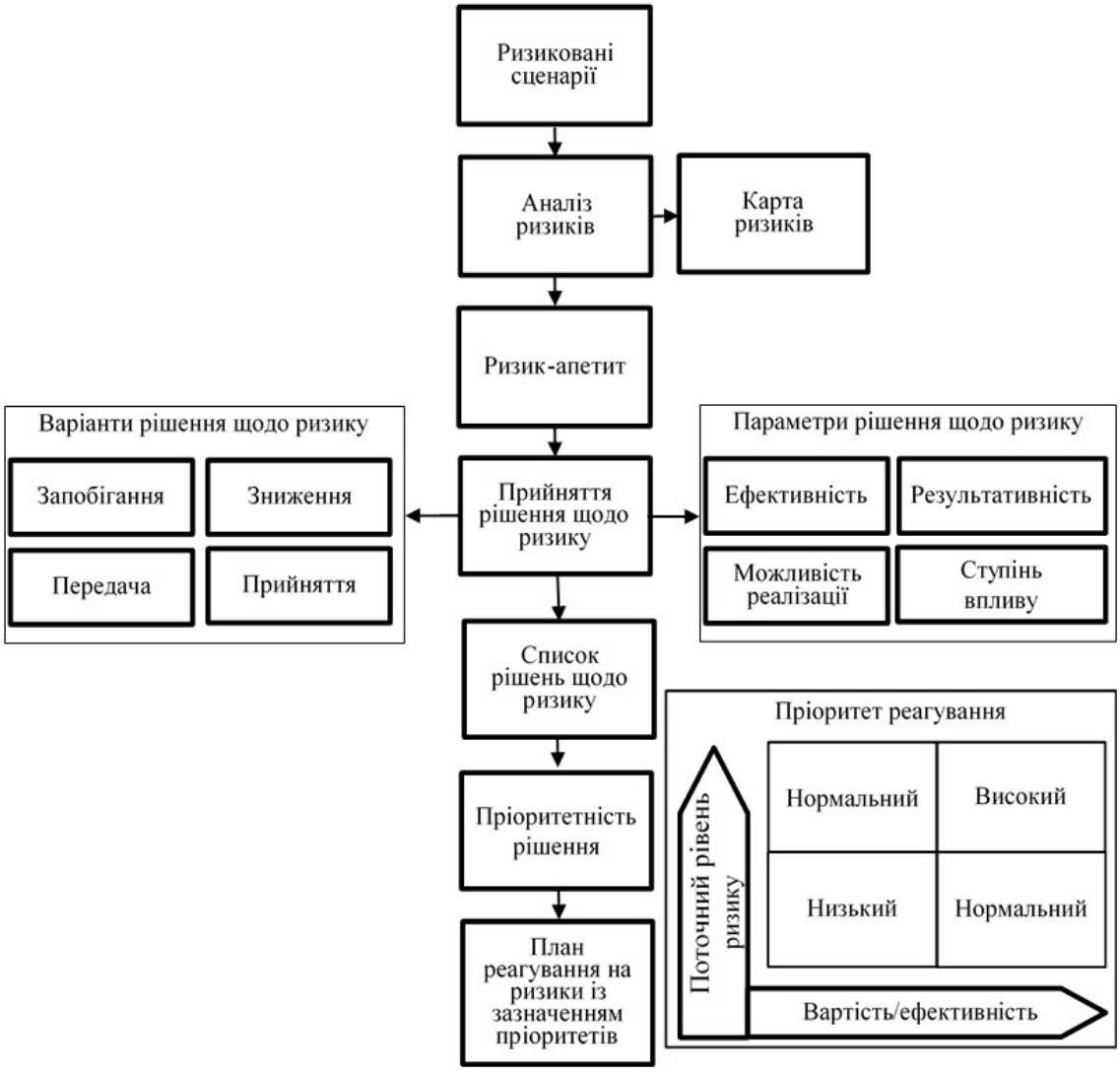

Рисунок 4 – Рекомендації щодо впровадження заходів зниження ризиків

З погляду практичного застосування методології COBIT можна виділити такі переваги:

зв'язок із загальною бібліотекою COBIT і можливість використовувати підходи та «IT-контролі» (заходів зі зниження ризиків) із суміжних областей, які дають змогу розглядати ризики ІБ і заходи щодо їх зниження відносно впливу ризиків на процеси установи;

багаторазово апробований метод, за яким накопичений значний досвід і професійні компетенції, а підсумки якого визнаються міжнародними інститутами;

наявність зрозумілого формалізованого опису методології дає змогу звести до мінімуму помилки під час реалізації процесів аналізу та управління ризиками;

каталоги ризикових сценаріїв та «IT-контролів» дають змогу спростити вимоги щодо спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками;

можливість використання методології під час проведення аудитів дає змогу знизити трудовитрати і потрібний час для інтерпретації підсумків зовнішніх і внутрішніх аудитів.

За таких умов методиці COBIT властиві такі недоліки та обмеження:

складність і трудомісткість збору початкових даних потребує залучення значних ресурсів всередині установи або ззовні;

залучення великої кількості зацікавлених осіб потребує значних витрат на організування їх спільної роботи, виділення часу на комунікації всередині проєктної команди та узгодження підсумків з усіма зацікавленими особами;

відсутність можливості оцінювання ризиків у грошовому еквіваленті ускладнює використання підсумків оцінювання ризиків ІБ під час обґрунтування інвестицій, потрібних для впровадження засобів і методів захисту інформації [28].

Методологія COBIT використовується в установах різних форм власності та є найбільш придатною для великих технологічних підприємств із високим ступенем залежності основної діяльності від інформаційних технологій і мають потрібні ресурси і компетенції для використання цієї методології. В цьому випадку можлива ефективна інтеграція процесів управління ризиками інформаційної безпеки та процесів загального управління IT і досягнення синергетичного ефекту, який дасть змогу оптимізувати витрати на реалізацію процесів аналізу й управління ризиками інформаційної безпеки.

Таким чином, проведений аналіз методу CRAMM та методології COBIT 5 for Risk стосовно процесу управління ризиками інформаційної безпеки установи дав змогу визначити переваги та недоліки зазначених методів. Використання ризиково-орієнтованих підходів, реалізованих у розглянутих методах дає змогу побудувати більш ефективну систему безпеки для установ, захищати в першу чергу найбільш критичні для забезпечення функціонування об'єкти, враховуючи актуальні загрози безпеки і технології, що застосовуються. Також слід відзначити важливість обміну інформацією про ризики, інциденти та загрози для спільної протидії новим викликам і загрозам.

Висновки й перспективи подальших досліджень

Розглянуті методи CRAMM та COBIT 5 for Risk зарекомендували себе як дієві та ефективні стосовно мінімізації впливу ризиків на інформаційну безпеку установ різних форм власності. Зазначені методи можна рекомендувати для застосування в управлінні критичною інфраструктурою з метою забезпечення їх безпеки [9], проте це вимагає належного нормативно-правового регулювання, оскільки від функціонування критичних об'єктів, значною мірою, залежить національна безпека держави. Крім того, потрібно розробляти (удосконалювати) конкретні вимоги, виконання яких дасть змогу забезпечити належний рівень захищеності. Водночас заходи забезпечення безпеки мають обиратися під конкретний об'єкт захисту з урахуванням його характеристик та особливостей функціонування.

Подальші дослідження слід спрямувати на розгляд та порівняльний аналіз інших методів і методик, де реалізовані ризиково-орієнтовані підходи (стандарти NIST SP 800-30 і ISO/IES 27005;2008).

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 30.08.2023). **2. Про** рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 14 вересня 2020 року: Указ Президента України від 14 вересня 2020 року № 392/2020. URL:https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 30.08.2023). **3. Потій О. В., Горбенко Ю. І., Замула О. А., Ісірова К. В.** Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки Радіотехніка. 2021. Вип. 206. С. 5–23. **4. 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. ХУПС. 2010. Вип. 2(24). С. 85–91. **5. Савельєва Т. В., Панаско О. М., Пригодюк О. М.** Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. Вісник Черкаського державного технологічного університету. Сер: Технічні науки. 2018. № 1. С. 81–89. **6. Бучик С. С., Шалаєв В. О.** Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. Наукоємні

технології № 3(35). 2017. С. 215–226. **7. CRAMM** user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001. **8. COBIT 5:** A Business Framework for the Governance and Management of Enterprise ISACA, 2012. **9. Мельничук О.** Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. Державне управління та місцеве самоврядування. 2019. № 3(42). С. 13–27.

METHODS OF MANAGEMENT OF INFORMATION SECURITY RISKS CRAMM AND COBIT 5 for Risk

Sydorkin Pavlo [1]
Horlichenko Serhii [1]
Nekoz Vasyl [1]
Shylan Mykola [2]

[1] ***Institute of Special Communications and Information Protection National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine***
[2] ***National Defence University of Ukraine, Kyiv, Ukraine***

The purpose of the article is to conduct a detailed analysis of known risk management methods CRAMM and COBIT 5 for Risk for their use in minimizing the impact of risks on the information security of the enterprise (organizations, institutions). During the writing of the article, theoretical methods were applied, namely the analysis of research and publications on the topic of risk management. The specified methodological approach makes it possible to compare the main methods of risk management. The work states that the most common methods and techniques of information security risk management in the world are CRAMM, COBIT for Risk, FRAP, Octave and Microsoft. A thorough analysis of CRAMM and COBIT 5 for Risk methods was carried out. It is noted that the CRAMM method has stages of initiation, identification and assessment of IT assets, assessment of threats and vulnerabilities, and risk determination. The structure of the COBIT 5 for Risk methodology is presented, the components of the institution are considered in relation to the description of risk management functions and processes according to this methodology, and recommendations are offered for the implementation of risk reduction measures. The main advantages and disadvantages of the considered risk management methods are given. The importance of information security risks is growing due to the increase in the number of implemented attacks, and taking into account their destructive potential. Along with certain advantages, they also have their limitations. In particular, the considered methods are effectively used by commercial companies and state institutions, and can also be applied during the assessment and management of information security risks of critical infrastructure objects.

Keywords: *risk management, potential harm, risk ranking, information security risk assessment, risk response.*

References

1. On the Fundamental Principles of Ensuring Cybersecurity in Ukraine [online], (2017). Zakon Ukrainy № 2163-VIII. 5 October/ Available at: https://zakon.rada.gov.ua/laws/show/392/2020#Text [Accessed 30 August 2023]. **2. On the Decision** of the National Security and Defense Council of Ukraine 'On the Strategy of National Security of Ukraine [online], (2020). Presidential Decree of Ukraine № 392/2020 of September 14, Available at: https://zakon.rada.gov.ua/laws/show/392/2020#Text [Accessed 30 August 2023]. **3. Potii, O. V., Horbenko, Yu. I., Zamula, O. A., Isirova, K. V.,** (2021). Analysis of Methods for Assessing and Managing Risks in Cyber and Information Security. *Radiotekhnika*, Issue 206, 5-23. **4. Potii, O. V., Lenshin, A. V.** (2010). Research on Methods of Assessing Information Security Risks and Proposals for their Improvement Based on a Systemic Approach. *Collection of Scientific Works*, Kharkiv. KhUPS, Issue 2(24), 85-91. **5. Savelieva, T. V., Panasko, O. M., Pryhodiuk, O. M.** (2018). Analysis of Methods and Tools for Implementing a Risk-Oriented Approach in the Context of Enterprise Information Security. *Bulletin of Cherkasy State Technological University. Series: Technical Sciences*, 1, 81-89. **6. Buchyk, S. S., Shalaiev, V. O.** (2017). Analysis of Instrumental Methods for Determining Information Security Risks in Information and Telecommunication Systems. *Technology-Intensive Technologies*, 3 (35), 215-226. **7. United** Kingdom Central Computer and Telecommunication Agency (CCTA) (2001). CRAMM User Guide, Risk Analysis and Management Method, UK. **8. ISACA** (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise. **9. Melnychuk, O.** (2019). Management of the State's Critical Infrastructure: Basic Methods and Criteria for Object Identification. *Public Administration and Local Government*, 3(42), 13-27.