МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ПРОЦЕСИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВИМІРЮВАННЯ ЇХ ПОКАЗНИКІВ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Віталій ГОРОДНИЧИЙ

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Віталій ГОРОДНИЧИЙ

Керівник:
к.т.н. Дмитро РАБЧУН

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_____ Світлана ЛЕГОМІНОВА

“____”_____2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Городничому Віталію Валерійовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Процеси управління ризиками інформаційної безпеки та вимірювання їх показників”

керівник кваліфікаційної роботи Дмитро РАБЧУН, к.т.н.

(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, нормативні документи, стандарти, міжнародні стандарти.*

4. Перелік питань, які потрібно розробити:
   1. ???
   2. Перелік ілюстративного матеріалу: *презентація*

3. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	15.10.2023	
3.	Аналіз теоретичних аспектів управління ризиками інформаційної безпеки організації	25.10.2023	
4.	Огляд особливостей процесів управління ризиками інформаційної безпеки організації	11.11.2023	
5.	Формування рекомендацій щодо використання технологій в управлінні ризиками організації	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	16.01.2024	

Здобувач вищої освіти _____ Віталій ГОРОДНИЧИЙ

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Городничий В.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Ефективність корпоративного управління інформаційною безпекою в Україні"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ГОРОДНИЧИЙ Віталій** у кваліфікаційній роботі дослідив сучасний стан корпоративного управління інформаційною безпекою в Україні, визначив основні проблеми та розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності корпоративного управління інформаційною безпекою організацій (підприємств). **ГОРОДНИЧИЙ Віталій** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на трьох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **ГОРОДНИЧОМУ Віталію** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою"".

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти

на тему “ПРОЦЕСИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВИМІРЮВАННЯ ЇХ ПОКАЗНИКІВ”

Актуальність

Забезпечення ефективного управління ризиками інформаційної безпеки також є стратегічно важливим для забезпечення довіри стейкхолдерів. Клієнти, партнери та регулятори вимагають від організацій доведення, що їхні дані і системи належним чином захищені від можливих загроз.

Важливо зазначити, що росте важливість вимірювання показників управління ризиками. Комплексне вивчення та оцінка ефективності заходів безпеки ідентифікуються як критичні аспекти для постійного вдосконалення систем управління ризиками та адаптації до змін у загрозах.

Позитивні сторони

Цією роботою я звернувся до важливої та актуальної теми, пов'язаної з управлінням ризиками інформаційної безпеки, що відображає велику значущість цієї проблематики в сучасному цифровому світі.

Дипломна робота вражає ретельністю аналізу використовуваних методик та підходів до управління ризиками, зокрема врахуванням інноваційних підходів, таких як використання аналізу великих даних та штучного інтелекту.

Чітко структурований вступ та висновок роблять роботу добре впорядкованою та логічно зв'язаною.

Акцент на важливості вимірювання показників управління

ризиками є важливим аспектом роботи, що відображає сучасні тенденції в галузі інформаційної безпеки.

Недоліки

Хоча робота добре структурована, варто розглянути можливість більш детального розгляду окремих методик та їхнього порівняння, щоб надати читачеві глибший розуміння вибору конкретних підходів.

Деякі терміни та поняття можуть бути уточнені або додатково пояснені для полегшення сприйняття роботи менш кваліфікованими читачами.

Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування обраної методики управління ризиками на конкретних кейсах чи в реальних умовах підприємства.

Висновок:

Незважаючи на деякі незначні недоліки, дипломна робота є важливим та цікавим внеском у галузь управління ризиками інформаційної безпеки та заслуговує на високу оцінку за свою актуальність і глибину аналізу.

Рецензент: професор кафедри
Інформаційної та кібернетичної
безпеки,

д.т.н, професор _____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 67 стор., 10 рис., 2 табл., 60 джерел.

Метою роботи є дослідження процесів управління ризиками інформаційної безпеки та вимірювання їх показників.

Об'єкт дослідження – управління ризиками інформаційної безпеки.

Предмет дослідження – процеси управління ризиками інформаційної безпеки.

Методи дослідження. Дослідження процесів управління ризиками інформаційної безпеки та вимірювання їх показників є важливим завданням, щоб забезпечити ефективний захист інформації в сучасному цифровому середовищі. Існує кілька методів, які дозволяють проводити ці дослідження та отримувати вичерпні та об'єктивні результати.

Один із методів - аналіз стандартів та нормативів. Дослідження вимог та рекомендацій, встановлених відповідними стандартами (наприклад, ISO/IEC 27001), дозволяє оцінити ефективність і відповідність процесів управління ризиками інформаційної безпеки визначеним стандартам. Цей метод дозволяє визначити прогалини та вдосконалити існуючі практики.

Ще одним методом є проведення аудиту системи управління ризиками. Цей підхід передбачає детальний огляд та оцінку процесів управління ризиками в організації. Аудит може включати аналіз документації, спостереження за роботою персоналу та оцінку відповідності діючих процедур вимогам безпеки.

Всі ці методи, взяті разом, дозволяють отримати повну картину процесів управління ризиками інформаційної безпеки та вимірювання їх показників, що надає підстави для подальшого вдосконалення та забезпечення найвищого рівня захисту інформації.

Короткий зміст роботи. Дослідження присвячено аналізу процесів управління ризиками інформаційної безпеки в організаціях та вимірюванню їх показників. Робота включає вивчення традиційних та інноваційних методів управління ризиками, а також розглядає стандарти і нормативи, які регулюють ці процеси. Здійснено порівняльний аналіз методик, визначено їх переваги та недоліки. Досліджено використання аналізу великих даних та штучного

інтелекту для виявлення ризиків. Запропоновано рекомендації щодо вибору та впровадження технологій у сфері управління ризиками інформаційної безпеки. Робота висвітлює важливі аспекти управління ризиками, підкреслюючи актуальність теми у сучасному цифровому середовищі.

Галузь застосування. Результати дослідження процесів управління ризиками інформаційної безпеки є критично важливим для підприємств у всіх галузях, де забезпечення конфіденційності, цілісності та доступності інформації визначає успіх бізнесу.

КЛЮЧОВІ СЛОВА: ПРОЦЕСИ УПРАВЛІННЯ РИЗИКАМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІДЕНТИФІКАЦІЯ, МЕТОДИ ТА ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ, ТЕХНОЛОГІЇ МІНІМІЗАЦІЇ.

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 67 pages, 10 figures, 2 tables, 60 sources.

The purpose of the work is to investigate the processes of information security risk management and measurement of their indicators.

Object of research is information security risk management.

Subject of research is the processes of information security risk management.

Research methods. Researching information security risk management processes and measuring their performance is an important task to ensure effective information protection in the modern digital environment. There are several methods that allow you to conduct this research and obtain comprehensive and objective results.

One method is to analyze standards and regulations. A study of the requirements and recommendations established by the relevant standards (for example, ISO/IEC 27001) allows you to assess the effectiveness and compliance of information security risk management processes with certain standards. This method allows you to identify gaps and improve existing practices.

Another method is to conduct an audit of the risk management system. This approach involves a detailed review and assessment of the organization's risk management processes. The audit may include a review of documentation, observation of staff work, and an assessment of the compliance of existing procedures with security requirements.

All of these methods, taken together, allow you to get a complete picture of information security risk management processes and measure their performance, which provides the basis for further improvement and ensuring the highest level of information security.

Brief content of research. The research is devoted to the analysis of information security risk management processes in organizations and the measurement of their indicators. The work includes the study of traditional and innovative methods of risk management, as well as the standards and regulations governing these processes. A comparative analysis of the methods is carried out,

their advantages and disadvantages are identified. The use of big data analysis and artificial intelligence to identify risks is investigated. Recommendations for the selection and implementation of technologies in the field of information security risk management are proposed. The paper highlights important aspects of risk management, emphasizing the relevance of the topic in the modern digital environment.

Field of research. The results of the study of information security risk management processes are critical for enterprises in all industries where ensuring the confidentiality, integrity and availability of information determines business success.

KEYWORDS: RISK MANAGEMENT PROCESSES, INFORMATION SECURITY, IDENTIFICATION, METHODS AND TECHNOLOGIES OF RISK MANAGEMENT, MINIMIZATION TECHNOLOGIES.

ЗМІСТ

ВСТУП

Актуальність теми

Динамічний розвиток технологій, підвищення кількості цифрових платформ і збільшення обсягів обробки даних створюють унікальні виклики для забезпечення безпеки інформації. Однією з ключових причин актуальності цієї теми є постійне зростання кількості та складності кіберзагроз. Зловмисники намагаються експлуатувати вразливості в системах безпеки для отримання несанкціонованого доступу до конфіденційної інформації, викрадення даних, або навіть впливу на нормальне функціонування підприємства.

Мета роботи - дослідження процесів управління ризиками інформаційної безпеки та вимірювання їх показників

Об'єкт дослідження - управління ризиками інформаційної безпеки

Предмет дослідження – процеси управління ризиками інформаційної безпеки.

Методи дослідження.

. Один із методів - аналіз стандартів та нормативів. Дослідження вимог та рекомендацій, встановлених відповідними стандартами (наприклад, ISO/IEC 27001), дозволяє оцінити ефективність і відповідність процесів управління ризиками інформаційної безпеки визначеним стандартам. Цей метод дозволяє визначити прогалини та вдосконалити існуючі практики.

Ще одним методом є проведення аудиту системи управління ризиками. Цей підхід передбачає детальний огляд та оцінку процесів управління ризиками в організації. Аудит може включати аналіз документації, спостереження за роботою персоналу та оцінку відповідності діючих процедур вимогам безпеки.

Практичне значення одержаних результатів.

Апробація результатів кваліфікаційної роботи було оприлюднено на Всеукраїнській науково-практичній конференції 23 лютого 2023 року.

Розділ 1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1 Сутність управління ризиками інформаційної безпеки організації

У сучасному інформаційному суспільстві, де обмін та обробка інформації стали неодмінною складовою будь-якої діяльності, питання забезпечення безпеки інформації виникають на передній план. Управління ризиками інформаційної безпеки в організації є важливою стратегічною ініціативою, яка спрямована на ефективне управління можливими загрозами та забезпечення стійкості інформаційних активів.

У будь-якій компанії існує безліч ризиків, з якими керівництво стикається на щодень: фінансові, репутаційні, а також ризики в області інформаційної безпеки. Серед поширених загроз в інформаційній безпеці виділяються витік конфіденційної інформації, несанкціонований доступ до конфіденційних файлів, використання шкідливих програм, використання неліцензійного програмного забезпечення, втрати даних, кібервійни та кібертероризм. [1]

З урахуванням того, що повністю уникнути ризиків неможливо, найкращим підходом є їх управління. Перед тим, як розпочати процес регулювання, важливо ретельно розглянути побудову системи управління.

Сутність управління ризиками інформаційної безпеки полягає в системному підході до ідентифікації, оцінки, мінімізації та контролю ризиків, які можуть впливати на конфіденційність, цілісність та доступність інформації. Цей процес вимагає поєднання технічних, організаційних та людських ресурсів для створення високоефективного механізму, спроможного адаптуватися до постійно змінюючого середовища. [2]

Основні аспекти сутності управління ризиками інформаційної безпеки: [3]

- Ідентифікація ризиків:

організація повинна визначати та класифікувати ризики, які можуть впливати на безпеку її інформації. Ідентифікація охоплює аналіз загроз, вразливостей та потенційних наслідків для інформаційних активів.

- Оцінка ризиків:

проведення оцінки ймовірності виникнення ризиків та визначення їх потенційного впливу на організацію. Визначення прийнятного рівня ризику та його порівняння із забезпеченим рівнем захисту.

- Мінімізація ризиків:

розробка та впровадження стратегій та заходів для зменшення ймовірності виникнення ризиків або їх наслідків. Вибір оптимальних методів та технічних рішень для забезпечення ефективного управління ризиками.

- Моніторинг та контроль:

постійний аналіз та оцінка ризиків відповідно до змін у середовищі, технологічних умовах та стратегії організації. Встановлення системи моніторингу та контролю для негайного виявлення та вирішення можливих загроз.

- Інтеграція у бізнес-процесів:

включення управління ризиками інформаційної безпеки у загальний стратегічний та бізнес-план організації. Забезпечення взаємодії з іншими процесами управління та бізнес-функціями.

У центрі цього системного підходу лежить ідентифікація ризиків. Визначення потенційних загроз, вразливостей та можливостей виникнення ризиків створює фундаментальну основу для подальших дій. Аналіз взаємодії цих факторів визначає ймовірність виникнення ризиків та потенційний збиток від їхнього реалізації. [4]

Управління ризиками інформаційної безпеки не може бути успішним без встановлення чіткої стратегії та політики безпеки. Сутність цього процесу виявляється в розробці та впровадженні конкретних стратегій мінімізації ризиків, що відповідають конкретним потребам та характеристикам

організації. Це може включати технічні заходи безпеки, організаційні політики та процедури, а також освіту та навчання персоналу.

Важливим елементом сутності управління ризиками є постійний моніторинг та контроль. Динаміка сучасного бізнес-середовища вимагає системного виявлення, аналізу та вирішення ризиків в реальному часі. Інформаційні технології, такі як системи моніторингу та аналізу безпеки, грають ключову роль у забезпеченні ефективного функціонування цього процесу. [5]

Успішне управління ризиками інформаційної безпеки також передбачає активне залучення всіх учасників організації. Визначення ролей та відповідальностей забезпечує чітку лінію комунікації та координації у справлянні з ризиками.

Управління ризиками інформаційної безпеки є не тільки технічним завданням, але й стратегічною необхідністю, що відображає глибоке розуміння важливості інформаційних ресурсів для сучасних організацій. Сутність цього процесу виявляється в здатності організації не просто реагувати на потенційні загрози, але й передбачати їх, забезпечуючи проактивний та передбачуваний підхід до управління ризиками. [6]

Один із ключових аспектів сутності управління ризиками інформаційної безпеки - це прагнення до балансу між доступністю інформації, її конфіденційністю та цілісністю. Намагання захистити інформацію за всіма можливими засобами може призвести до обмежень доступності та ускладнення бізнес-процесів. Таким чином, управління ризиками стає викликом в забезпеченні оптимальної ефективності та продуктивності організації.

Сутність управління ризиками виявляється також в його піддатливості постійним змінам. Зростання технологічного розвитку, нові види загроз, зміна законодавства - усі ці фактори створюють динамічне середовище, яке вимагає гнучкості та готовності до адаптації. Організація повинна бути готовою не лише реагувати на нові ризики, але і вчасно їх визначати та прогнозувати. [7]

Не менш важливим елементом сутності управління ризиками є урахування фактора людського фактору. Організації повинні не лише вдосконалювати технічні заходи безпеки, але і враховувати освіту, тренування та психологічний аспект користувачів. Підвищення освіченості персоналу та формування безпечної культури стають неодмінною частиною сутності управління ризиками.

Оцінка ризиків інформаційної безпеки проводиться етапно, включаючи ідентифікацію загроз, вразливостей і активів. Різні методи управління, зазначені в стандарті, застосовуються для виконання якісного або кількісного аналізу загроз, визначення факторів ризику системи та пошуку оптимальних рішень через кластеризацію. Важливо відзначити, що чіткої методики розрахунку величин ризиків не існує. Тому відповідно до стандартів та кращого досвіду, організації повинні застосовувати всі доступні заходи для запобігання їм, такі як дотримання всіма співробітниками кібергігієни та внутрішніх положень безпеки, використання сучасних засобів захисту від новітніх атак і загроз, а також використання систем управління ризиками інформаційної безпеки. [8]

У сучасному світі поняття ризику інформаційної безпеки нерозривно пов'язане з автоматизацією робочих процесів, і тому управління ризиками даних також має бути автоматизоване за допомогою спеціального програмного забезпечення (аналіз уразливостей, захист інформації тощо).

Впровадження програмного забезпечення дозволяє ефективно організувати ідентифікацію ризиків, оцінку їх можливого виявлення та наслідків, визначення послідовності дій, залучення відповідальних осіб, моніторинг та відстеження ключових моментів, збір необхідної інформації, навчання персоналу з метою зменшення ризиків для організації. Надійна платформа захисту даних Lepide Data Security Platform, яка відповідає всім стандартам і основам безпеки, забезпечує необхідні перевірки та допомагає вчасно усувати неправильні налаштування, дотримуючись стандартів інформаційної безпеки. [9]

Класифікація ризиків означає об'єднання сукупності ризиків на підставі певних ознак і критеріїв. Такими критеріями, покладеними в основу класифікації інформаційних ризиків, є:

- основні аспекти інформаційної безпеки;
- час виникнення;
- джерело виникнення;
- природа інформаційного активу;
- характер загрози інформаційної безпеки;
- характер наслідків; механізм впливу.

Основними аспектами інформаційної безпеки є: доступність, цілісність і конфіденційність інформації.

Під доступністю розуміється можливість доступу суб'єкта до даних за запитом в будь-яке передбачене розкладом роботи час. Можливість отримання даних за запитом залежить від працездатності та завантаженості елементів інформаційної системи і її каналів передачі даних. [10]

Ризик порушення доступності інформації може залежати як від несправності обладнання і збоїв в програмному забезпеченні в компанії, так і від успішно реалізованих мережевих атак на інформаційну систему із зовні.

Даний тип ризику безпосередньо залежить від надійності апаратних і програмних компонентів інформаційної системи, а так само від рівня компетенцій персоналу, керуючого їх роботою. Порушення доступності можуть виникнути внаслідок невиконання вимог стандартів як на етапі проектування, так і на етапах виробництва та експлуатації системи. Під інтегрітетом розуміється актуальність та відсутність конфліктності інформації, а також рівень захисту від її руйнування, несанкціонованої зміни і видалення.

Ризик порушення цілісності забезпечується можливостями відмови обладнання і програмного забезпечення, ступенем продуманості алгоритмів і надійністю засобів доступу користувачів системи, які мають право на редагування інформації, ймовірністю наявності в системі недокументованих

можливостей, недосконалістю організаційної структури ІС, а так само недодержанням вимог стандартів на етапі проектування, виробництва і експлуатації системи.

Конфіденційність визначається як ступінь захисту інформації від несанкціонованого доступу.

Ризик порушення конфіденційності так само залежить від рівня алгоритмів аутентифікації користувачів, ймовірністю наявності недокументованих ситуацій при роботі з ІС, недосконалістю організаційної структури, недотриманням стандартів і людським фактором.

Інформаційні ризики можна класифікувати за часом їх виникнення на ретроспективні, поточні та перспективні. Проведення аналізу ретроспективних ризиків, їх характеру та застосування методів для їх мінімізації дозволяє більш точно прогнозувати поточні та перспективні ризики.

За середовищі виникнення ризики діляться на зовнішні і внутрішні.

Зовнішні ризики є незалежними від внутрішніх компонентів підприємства і не пов'язані з його прямою діяльністю. Ці ризики виходять за межі внутрішнього контролю підприємства і ніяк не можуть бути керуючими або впливати на їх рівень через внутрішні фактори підприємства.

Їх рівень обумовлений політичною обстановкою в країні і між державами, економічною ситуацією на ринку, соціальним рівнем громадян і т.д.

До внутрішніх інформаційних ризиків відносяться ризики, які залежать від безпосередньої діяльності підприємства і його персоналу. На їх рівень можуть впливати наступні фактори: виробничий потенціал організації, рівень технічного оснащення, ступінь кваліфікації персоналу, наявність засобів захисту інформації, наявність посадових інструкцій при роботі з ІС. [11]

За природою інформаційного активу інформаційні ризики можна розділити на ризики апаратні і програмні. Апаратні ризики виникають при виході з ладу комплексів ІС, таких як: сервери, персональні комп'ютери, мережеві комутатори і маршрутизатори, виробниче обладнання, верстати і т.д.

Програмні ризики безпосередньо пов'язані зі збоями в роботі програмного забезпечення підприємства, дії шкідливого програмного забезпечення, операційних систем користувачів ІС, а так само пов'язані з витоком інформації і дії мережевих атак. Формуючи класифікацію, пов'язану з характером загрози інформаційній безпеці, можна виділити наступні ризики:

Організаційні ризики - це ризики, пов'язані діяльністю персоналу, що експлуатує і обслуговує ІС, проблемами системи внутрішнього контролю, погано розробленими правилами робіт, тобто ризики, пов'язані з внутрішньою організацією роботи компанії.

Технічні ризики пов'язані з обладнанням, програмним забезпеченням, їх завданнями, способами проектування, розробки та експлуатації ІС. Ці ризики безпосередньо пов'язані з життєвим циклом ІС.

До природних інформаційним ризиків відносяться ризики, що не залежать від діяльності людини. Вони здатні завдати шкоди, який можемо привести до повної зупинки функціонування підприємства. Вони пов'язані з діяльністю природних явищ, таких як землетруси, повені, шторми, урагани, і т.д.

Найчастіше ризик характеризується сукупністю трьох якостей: наявністю джерела небезпеки; невизначеністю настання небезпечної події; можливістю заподіяння шкоди. Отже, управляти ризиком - це значить:

- виявляти, вивчати, усувати, нейтралізовувати або зменшувати джерела

небезпеки;

- здійснювати систематичний моніторинг і прогнозувати сценарії

розвитку небезпечних подій;

- запобігати, локалізувати і усувати негативні наслідки небезпечних

подій. [12]

Сутність управління ризиками інформаційної безпеки виявляється в її глибокому впливі на стратегію, культуру та результативність організації. Вона не лише визначає, як організація реагує на потенційні небезпеки, а й формує її життєздатність у цифровому віці, де інформація стала ключовим ресурсом.

Управління ризиками інформаційної безпеки виходить за межі технічних аспектів та перетинається з стратегічними та організаційними вимірами, створюючи цілісний підхід до забезпечення надійності та стійкості сучасних бізнес-процесів.

1.2 Методи управління ризиками в сфері інформаційної безпеки організації

Сучасна ділова обстановка ставить перед організаціями безпрецедентні виклики у сфері інформаційної безпеки. Зростаюча кількість технологічних загроз, розширення цифрового ландшафту та складність кібератак вимагають від організацій вдосконалення методів управління ризиками для забезпечення стійкості та захисту їхніх інформаційних ресурсів.

Перш ніж розглядати конкретні методи управління ризиками, важливо розуміти, що ризики інформаційної безпеки можна розглядати як невід'ємну частину сучасного бізнес-середовища. Традиційні методи управління ризиками часто включають етапи ідентифікації загроз, оцінки вразливостей та визначення можливих наслідків. Вирішальним елементом в цьому підході є створення матриці ризиків, яка дозволяє приділити пріоритетність конкретним ризикам та розробити стратегії їхнього управління. [13]

Традиційні методи також зазвичай передбачають впровадження заходів безпеки та контролю, таких як шифрування, аутентифікація та авторизація. Вони покликані створити бар'єри для потенційних загроз та зменшити ймовірність їхнього виникнення.

Один з етапів традиційного управління ризиками - ідентифікація загроз. Цей процес включає в себе аналіз всіх можливих джерел небезпеки, які можуть вплинути на конфіденційність, цілісність та доступність інформації. Загрози можуть походити як із зовнішніх джерел, так і виникати всередині самої організації.

Після ідентифікації загроз наступний етап - оцінка вразливостей і визначення можливих наслідків. Це включає в себе аналіз потенційних слабкостей в системах та процесах, які можуть бути використані загрозами. З оцінки вразливостей виводиться рівень ризику, який визначає ймовірність виникнення загрози та вплив її на інформаційні ресурси.

Однією з традиційних стратегій для зменшення ризиків є шифрування. Шифрування використовується для захисту конфіденційності інформації. Воно полягає у перетворенні тексту в незрозумілий для сторонніх код за допомогою криптографічних алгоритмів. Лише авторизовані користувачі, які мають правильний ключ, можуть розшифрувати дані.

Аутентифікація та авторизація - ключові елементи управління ризиками. Аутентифікація перевіряє, чи користувач є тим, за кого він вдається, використовуючи логіни, паролі, біометричні дані тощо. Авторизація визначає права доступу користувача після успішної аутентифікації, обмежуючи його права на різні рівні конфіденційності та цілісності.

Традиційні методи управління ризиками в інформаційній безпеці виявляються дієвими для запобігання та мінімізації потенційних загроз. Етапи ідентифікації, оцінки вразливостей та визначення наслідків визначають стратегії та заходи для зменшення ризиків. Шифрування, аутентифікація та авторизація додають додатковий рівень захисту для забезпечення безпеки інформації в динамічному цифровому середовищі. У результаті впровадження традиційних методів управління ризиками можливо досягти стійкості та надійності інформаційних систем.

Проте, з урахуванням стрімкого розвитку технологій, виникає необхідність у більш інноваційних підходах до управління ризиками інформаційної безпеки. Один з таких методів - це використання аналізу великих даних та штучного інтелекту для виявлення відхилень та несправностей у системах безпеки.

Застосування аналізу великих даних у сфері інформаційної безпеки визначається потужністю обробки великого обсягу інформації в реальному

часі. Аналітика даних великого обсягу дозволяє виявляти незвичайні та непередбачувані події, які можуть вказувати на потенційні загрози або атаки. Це означає, що великі обсяги данних, які раніше можливо було важко обробляти, тепер можуть бути використані для розпізнавання аномалій та виявлення потенційних ризиків.

Штучний інтелект вносить інтелектуальну автоматизацію в системи управління ризиками. Системи, що використовують штучний інтелект, можуть аналізувати та вивчати патерни поведінки, а також навчатися на основі історичних даних та змінюватися в реальному часі. Це дозволяє системі бути більш гнучкою та адаптивною до нових загроз та викликів.

Інтеграція аналізу великих даних та штучного інтелекту дозволяє створити систему, яка здатна виявляти відхилення та несправності в реальному часі. За допомогою алгоритмів машинного навчання, система може автоматично аналізувати величезні обсяги даних, виявляти аномалії та вчасно реагувати на події, які можуть призвести до порушень безпеки.

Враховуючи все вищесказане можемо виділити такі переваги інноваційного підходу:

- прогностичність: аналіз великих даних та штучний інтелект дозволяють не лише реагувати на існуючі загрози, але й передбачати майбутні ризики на основі динаміки подій та тенденцій.
- ефективність: системи на основі штучного інтелекту можуть автоматично адаптуватися до нових загроз та умов, що робить їх ефективними в змінних середовищах.
- швидкість реакції: розпізнавання аномалій в реальному часі дозволяє оперативно реагувати на потенційні загрози та надавати вчасні заходи безпеки.

Аналіз великих даних дозволяє обробляти величезні обсяги інформації в реальному часі, виявляючи навіть мінімальні аномалії, які можуть свідчити про потенційні загрози. Використання штучного інтелекту допомагає вдосконалити прогнозування та самонавчання систем безпеки, роблячи їх більш адаптивними та відповідальними на зміни в середовищі. [14]

Зокрема, автоматизовані системи управління ризиками інформаційної безпеки стають актуальними в сучасному світі. Вони дозволяють не лише виявляти та вирішувати ризики в реальному часі, але і забезпечують швидке реагування на нові виклики.

Інноваційний підхід, заснований на аналізі великих даних та штучному інтелекті, відкриває нові перспективи для управління ризиками інформаційної безпеки. Ці технології відзначаються високою ступенем автоматизації, ефективністю та можливістю передбачати та уникати потенційних загроз. Забезпечуючи комплексний підхід до управління ризиками, вони визначають новий рівень безпеки в сучасному цифровому середовищі.

1.3 Стандарти та нормативні документи регулювання управління ризиками організації

Управління ризиками у сфері інформаційної безпеки є важливою складовою стратегії будь-якої сучасної організації. З урахуванням постійно зростаючого обсягу цифрових даних та загроз кібербезпеки, впровадження ефективних методів управління ризиками стає необхідністю для забезпечення стабільності та надійності функціонування бізнес-процесів.

Вивчення цих документів є важливим етапом для будь-якої компанії, оскільки вони встановлюють стандарти і рамки, що допомагають розуміти, оцінювати та контролювати ризики інформаційної безпеки.

Необхідність ефективного управління ризиками визначається не лише стрімким розвитком технологій, але й постійно зростаючою кількістю загроз та викликів у цифровому просторі. Розгляд стандартів та нормативів стане важливим кроком для будь-якої організації, яка має на меті забезпечити надійний та безпечний обіг інформації в сучасному конкурентному середовищі.

У світі існує ряд різноманітних методик і підходів до оцінки ризиків інформаційної безпеки, таких як Austrian IT Security Handbook, AS/NZS4360,

BSI 100-3, CRISAM, EBIOS, HB167: 200X, ISF IRAM, CRAMM, ISO 27005, MAGERIT, MARION, MEHARI, NIST SP800-30, OCTAVE, OSSTMMRAV, SOMAP та інші. Проте, деякі з них застарілі та не отримують подальших розробок, а інші можуть бути важко доступні для вивчення через відсутність актуальних перекладів на англійську мову з мови оригіналу.

У роботі розгляну саме ті методики, які володіють розгорнутим підходом, вже здобули певну популярність в Україні, продовжують активно розвиватися (або не втратили своєї актуальності) і мають відносно легкий доступ.

Вибір конкретної методики залежить від рівня вимог, які ставить перед собою підприємство у сфері забезпечення інформаційної безпеки, характеру загроз, що беруться до уваги та ефективності заходів контролю за захистом інформації.

ISO/IEC 27005:2015 [15] є ключовим стандартом, призначеним для визначення та впровадження ефективної системи управління ризиками інформаційної безпеки в організаціях. Виданий Міжнародною організацією зі стандартизації (ISO) та Міжнародним електротехнічним комітетом (IEC), цей стандарт визначає принципи та загальні вимоги до процесу управління ризиками в контексті інформаційної безпеки.

Основною метою ISO/IEC 27005 є допомога організаціям у створенні, впровадженні та підтримці системи управління ризиками інформаційної безпеки, яка враховує специфічні характеристики та потреби кожного підприємства.

Процес менеджменту ризиків інформаційної безпеки складається з визначення обставин, оцінки ризику, обробки ризику, прийняття ризику, обміну інформацією щодо ризику, а також моніторингу та перегляду ризику (рис. 1.1).

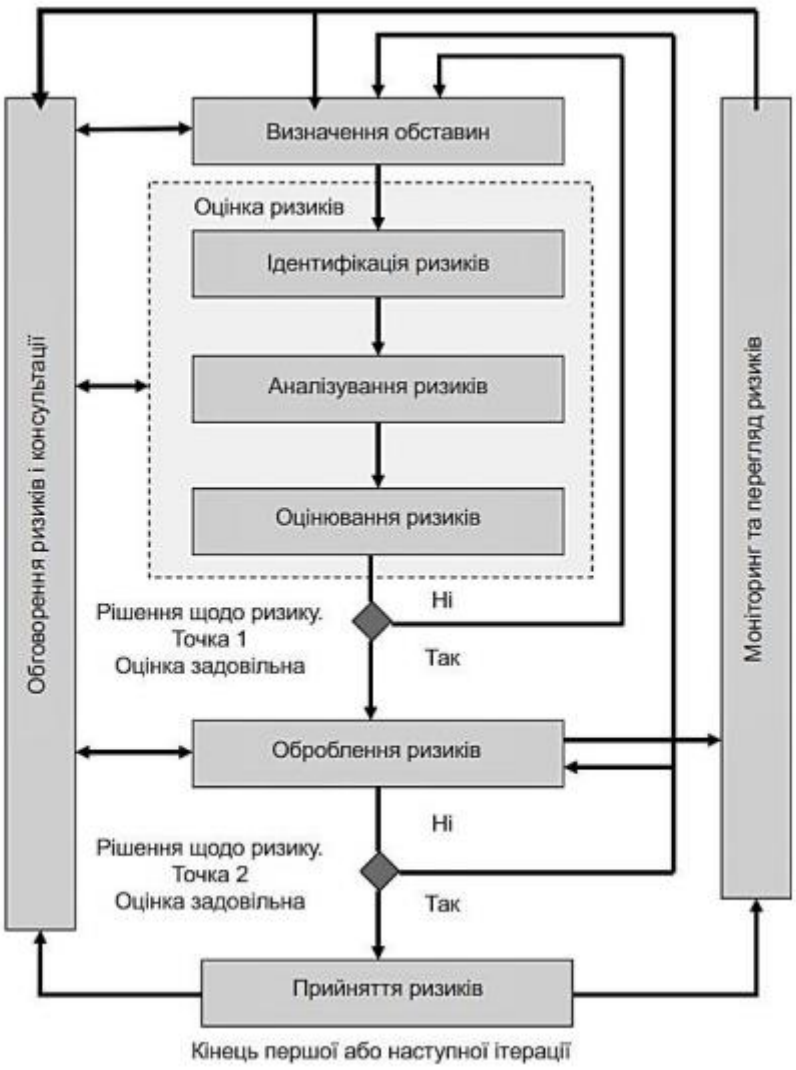

Рис. 1.1. Ілюстрація процесу управління ризиками ІБ за стандартом ISO 27005

На етапі визначення обставин проводиться аналіз зовнішніх та внутрішніх факторів для управління ризиками інформаційної безпеки (ІБ). Цей процес передбачає встановлення основних критеріїв, які є необхідними для управління ризиками ІБ, визначення сфери застосування та її меж, а також забезпечення функціонування управління ризиками ІБ, яке визнано в організації.

Базові критерії включають критерії порівняння ризиків, критерії впливу та критерії прийняття ризиків.

Оцінка ризиків включає ідентифікацію ризиків, аналіз ризиків та порівняння їх між собою. Метою ідентифікації ризиків є визначення можливих

загроз та уразливостей, які можуть викликати потенційні втрати. Цей етап передбачає ідентифікацію активів Системи управління інформаційною безпекою (СУІБ), загроз, існуючих засобів контролю, вразливостей та можливих наслідків.

Методологія аналізу ризиків може бути як якісною, так і кількісною, або їх комбінацією в залежності від умов.

Рівні ризиків порівнюються з критеріями оцінювання та прийняття ризиків. Для ефективності управління ризиками вимірювані ризики порівнюються з критеріями оцінювання.

Обробка ризиків включає чотири варіанти: модифікація ризиків, прийняття ризиків, усунення ризиків і розподіл ризиків.

Однією з найпопулярніших та широко використовуваних стратегій управління ризиками є методика National Institute of Standards and Technology (NIST), яка детально описана у Керівництві з управління ризиками в інформаційних технологіях **NIST 800-30** [16] (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика включає в себе попередню оцінку двох параметрів: потенційного збитку та ймовірності реалізації загрози. Для компаній важливо мати ефективну систему управління ризиками, особливо в умовах постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка описана в рекомендаціях 800-30, охоплює широкий спектр завдань, пов'язаних зі стратегією управління ризиками і виступає основою для розроблення власної системи управління ризиками. Проте сам процес оцінювання ризику ІБ, поданий у вигляді таблиці, що відображає залежність ризику від потенційного збитку і ймовірності можливого інциденту, має свої обмеження. Кожна змінна, включаючи ризик, оцінюється за трьома рівнями, утруднюючи отримання точних результатів, але забезпечуючи оперативність та відтворюваність.

Етапи використання цієї методики включають:

- опис характеристик системи;

- ідентифікація загроз;
- ідентифікація вразливостей;
- аналіз існуючих засобів захисту;
- визначення значення ймовірності;
- аналіз впливу;
- визначення рівня ризику;
- вибір заходів захисту;
- документування отриманих результатів.

Алгоритм цієї методики ілюстрований на рисунку 1.2.

Рис. 1.2 Алгоритм методики управління ризиками NIST 800-30

Переваги методу NIST 800-30 включають:

- відносну простоту проведення заходів з оцінки ризиків (ОР);
- можливість адаптації методу ОР до вимог конкретної організації залежно від її типу та розміру;
- детальний опис всіх можливих ризиків для інформаційних активів;
- можливість використання різних способів обробки ризиків, таких як зниження, прийняття, перенесення та уникнення ризику;

- наявність програмного забезпечення для обробки результатів, яке відповідає принципам методики.

З усім тим, метод NIST 800-30 має певні обмеження, такі як:

- тривалий процес аналізу і оцінки ризиків;
- використання трьохрівневої шкали для оцінювання ризиків, що значно обмежує можливості методики в цілому.

Метод **OCTAVE** [17] (Operationally Critical Threat, Asset and Vulnerability Evaluation), розроблений в Університеті Карнегі-Мелон (США), спрямований на оцінку критичності загроз, активів і вразливостей. Ця методика широко використовується у всьому світі для проведення оцінки ризиків інформаційної безпеки та впровадження процесів управління ризиками в компаніях загалом.

Суть методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність добре організованих внутрішніх семінарів (workshops). Процес оцінки ризиків складається з трьох етапів, перед якими йдуть підготовчі заходи, такі як узгодження графіка семінарів, призначення ролей, планування та координація дій учасників проєктної групи.

На першому етапі, під час семінарів, розробляються профілі загроз, які включають інвентаризацію та оцінку цінності активів, ідентифікацію відповідних вимог законодавства та нормативів, виявлення загроз та їх ймовірності, а також визначення системи організаційних заходів для підтримки режиму інформаційної безпеки.

Другий етап включає технічний аналіз вразливостей систем організації стосовно розглянутих загроз, де визначається наявність вразливостей та оцінюється їх ступінь.

На третьому етапі проводиться оцінка та оброблення ризиків інформаційної безпеки, що включає визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей. Також визначається стратегія інформаційної безпеки та обираються варіанти рішень для оброблення ризиків. Величина ризику обчислюється як середнє

значення річних втрат компанії в результаті реалізації загроз інформаційної безпеки (ІБ).

Алгоритм цієї методики ілюстровано на рис. 1.3.

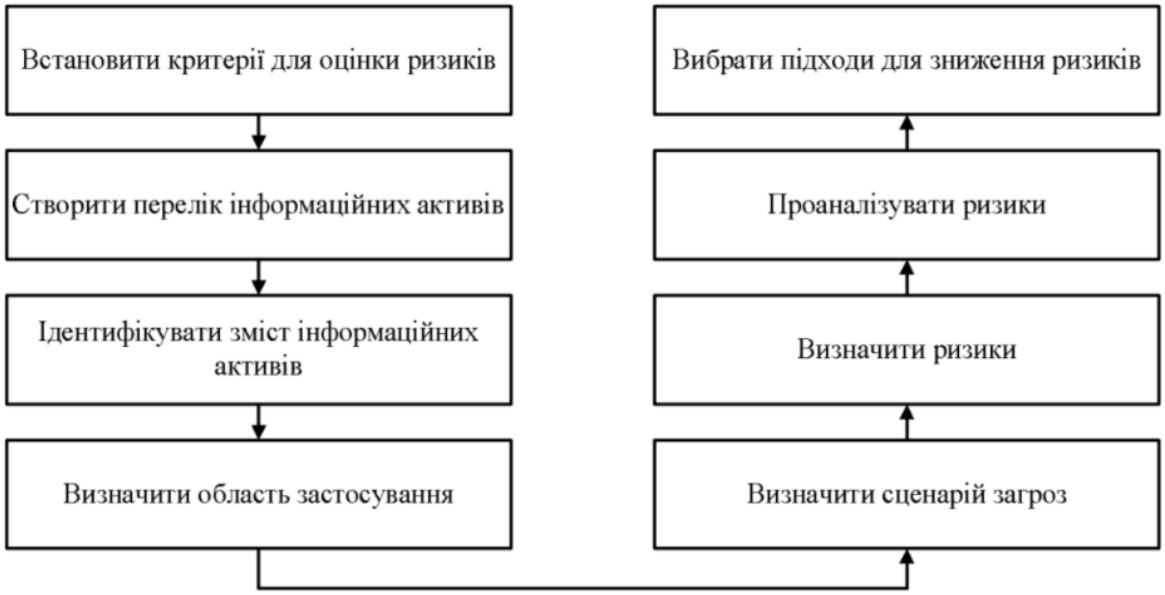

Рис. 1.3 Алгоритм методики OCTAVE

На підставі проведеного аналізу можна стверджувати, що оптимальним варіантом для вибору методу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування системи управління інформаційною безпекою є, зокрема, адаптація та вдосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів. Крім того, при виборі конкретного методу оцінки ризиків інформаційної безпеки важливо враховувати ряд існуючих факторів.

Висновки до розділу 1

Управління ризиками інформаційної безпеки є невід’ємною складовою ефективного функціонування сучасних організацій. Забезпечення безпеки інформації вимагає системного підходу, який охоплює ідентифікацію, оцінку та керування ризиками з метою забезпечення безперервності бізнес-процесів та захисту конфіденційної інформації організації.

Традиційні та інноваційні методи управління ризиками надають організаціям інструменти для виявлення, аналізу та обробки потенційних загроз інформаційній безпеці. Від традиційних підходів, таких як оцінка загроз та вразливостей, до використання аналізу великих даних та штучного інтелекту – усі ці методи спрямовані на підвищення рівня захисту інформації в умовах зростаючих загроз та технологічних викликів.

Система стандартів та нормативних документів, зокрема ISO/IEC 27001, NIST SP800-30, OCTAVE, визначає рамки та вимоги для ефективного управління ризиками інформаційної безпеки організації. Їх використання дозволяє організаціям створювати системи управління ризиками, які враховують сучасні виклики та відповідають високим стандартам безпеки.

Загалом ефективне управління ризиками інформаційної безпеки вимагає комплексного підходу, використання різноманітних методів та відповідність вимогам стандартів і нормативів. Застосування цих принципів дозволить організаціям успішно впроваджувати стратегії управління ризиками для забезпечення стійкості та безпеки їх інформаційних ресурсів.

Розділ 2 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1. Ідентифікація ризиків інформаційної безпеки організації

Ідентифікація ризиків інформаційної безпеки є критичним етапом в управлінні інформаційною безпекою організації. Зростання комплексності інформаційних систем та збільшення кількості загроз створює необхідність ефективного і систематичного підходу до ідентифікації потенційних ризиків, які можуть вплинути на конфіденційність, цілісність та доступність інформації.

Мета ідентифікації ризиків полягає в пошуку, розпізнаванні та описі ризиків, які можуть перешкоджати досягненню організацією своїх цілей. Під час ідентифікації ризиків важливе значення має важливість, відповідність та актуальність інформації, яка використовується. [18]

Неідентифіковані ризики можуть вплинути негативно на подальшу роботу інших етапів управління ризиками. Аналіз, оцінка та обробка ризиків напряму залежать від їх ідентифікації і не можуть бути проведені належним чином, якщо можливі загрози та вразливості, що можуть спричинити втрати, не були визначені.

Найважливішим етапом в процесі ідентифікації ризиків є встановлення контексту та сфери застосування. Для визначення контексту необхідно з’ясувати всі теми, що дотичні до мети організації, зацікавлених сторін та їх вимог до інформаційної безпеки організації. Якщо дослідження виявиться або занадто поверхневим, або занадто вузьконаправленим, суттєві елементи можуть бути не взяті до уваги, що слугуватиме неповній ідентифікації. [19]

Контекст поділяється на два типи: зовнішній та внутрішній. Зовнішній контекст включає всі аспекти за межами сфери впливу організації – це стосується законодавства, постачальників, конкурентів та клієнтів [20].

Внутрішній контекст включає всі аспекти в межах впливу організації: цілі, стратегії, процеси та процедури організації та ін. У таблиці 2.1 наведені приклади аспектів.

Таблиця 2.1

Перелік можливих аспектів контекстів

Тип контексту	Приклади аспектів
Зовнішній	Суспільство та культура
	Політичне середовище
	Нормативне середовище
	Конкурентна ситуація
	Постачальники, підрядники та аудитори
	Зацікавлені сторони, включаючи власників та інвесторів
Внутрішній	Культура організації
	Аудит та оцінка ризиків
	Інформаційні системи та потоки
	Цілі, стратегії та принципи організації
	Стандарти, інструкції та моделі, що використовуються
	Відповідальні особи за ризики

Масштаб процесу управління ризиками повинен бути чітко виражен, так як може відрізнятися від масштаду СУІБ. Для точного опису де варто і де не варто застосовувати ідентифікацію ризиків, необхідно визначити межі та сферу застосування СУІБ, а також визначити взаємозв’язки та залежності між діяльністю і функціями організації та діяльністю і функціями інших організацій.

Опис можливих наслідків інцидентів безпеки для діяльності організації з точки зору конфіденційності, цілісності та доступності інформації може, в принципі, дуже відрізнятися для різних людей і при повторенні процесу ідентифікації ризиків. Для того, щоб відповідати вимогам послідовності, порівнянності та відтворюваності результатів цього процесу ці описи повинні

бути структуровані та стандартизовані. [21] Це робиться за допомогою критеріїв подальших дій, які повинні бути детально і з достатньою точністю визначені до початку ідентифікації ризиків. Критерії подальших дій мають центральне значення для процесу аналізу ризиків, який слідує за процесом ідентифікації ризиків. У таблиці 2.2 наведені критерії подальших дій, структурованих відповідно до наслідків для конфіденційності, цілісності та доступності інформації.

Таблиця 2.2

Критерії подальших дій

Властивість інформації	Наслідки
Конфіденційність	Порушення конфіденційності внутрішніх або зовнішніх користувачів
	Втрата конкурентної переваги
	Втрата лідерства у сфері технологій
Цілісність	Неправильна подача через протиріччя в даних
	Неможливість підготовки коректної річної фінансової звітності
	Неможливість виконувати юридичні зобов'язання
Доступність	Зменшення кількості послуг
	Недоступність послуг
	Переривання бізнесу

Для забезпечення впевненості в надійності та якості ідентифікації ризиків процес ідентифікації ризиків повинен ґрунтуватися на достатньо детальних методах та засобах, щоб повторні ідентифікації ризиків призводили до цілісних, порівнянних та відтворюваних результатів.

Повторне застосування процесу ідентифікації ризиків може допомогти виявити проблеми з обраними методами та засобами (які проявляються у вигляді невідповідностей або суперечностей).[22]

Незалежно від обраних методів та засобів, процес ідентифікації ризиків повинен гарантувати, що

- всі ризики розглядаються з необхідним рівнем деталізації
- результати були узгодженими та зрозумілими для третіх сторін
- його результати є ідентичними, коли різні люди ідентифікують ризики в одному і тому ж контексті;
- результати повторних ідентифікацій ризиків є співставними

Організація може використовувати низку методів для виявлення невизначеностей, які можуть вплинути на одну або більше цілей. [23] Слід враховувати такі чинники та взаємозв'язки між ними:

- матеріальні та нематеріальні джерела ризику;
- причини та події;
- загрози
- вразливості;
- зміни в зовнішньому та внутрішньому контексті;
- ознаки ризиків, що виникають;
- характер і цінність активів і ресурсів;
- наслідки та їхній вплив на цілі організації;
- обмеженість знань і достовірність інформації;
- часові чинники;
- упередження, припущення та переконання тих, хто бере участь в оцінці ризиків.

Організація повинна виявляти ризики, незалежно від того, перебувають чи ні їхні джерела під її контролем. Слід враховувати, що може бути два і більше сценаріїв розвитку подій, які можуть призвести до різних наслідків, що мають матеріальний або нематеріальний характер.

Для виявлення ризиків зазвичай використовують два методи:

- Метод, заснований на подіях;

- Метод, заснований на ідентифікації активів, загроз і вразливостей.[24]

При методі, заснованому на подіях, ризики визначаються шляхом аналізу подій та їхніх наслідків. Події, що розглядаються, можуть відбуватися в минулому або, як передбачається, можуть відбутися в майбутньому. У першому випадку вони можуть включати архівні дані, у другому – ґрунтуватися на теоретичному аналізі, обґрунтованих думках та експертних оцінках, а також на вимогах зацікавлених сторін.

Ідентифікація ризиків при цьому підході починається з розгляду питань "Хто?", "Що?", "Де?", "Коли?" і "Чому?" для опису подій. Після цього визначаються причини та наслідки цих подій, з чого можна отримати глибше розуміння ризиків і, таким чином, вказати на основні загрози та вразливості.

Наслідки, які не можуть бути віднесені до цілей організації, не впливають на ризики і тому можуть бути проігноровані. Однак, якщо такі наслідки визначаються як такі, що фактично можуть спричинити виникнення ризиків, це вказує на те, що в переліку цілей організації є прогалини, які слід виправити.[25]

У методі, що заснований на ідентифікації активів, загроз і вразливостей, аналізують всі ці аспекти та наслідки, що пов’язані з ними. Ці наслідки виникають, коли загрози використовують слабкі сторони активів або групи таких активів і таким чином завдають шкоди організації. Розглянемо детальніше кожен аспект цього методу:

- Ідентифікація активів

Актив – це сукупність знань або даних, які є організованими, керованими та цінними для організації, тому потребують особливого захисту. Первинні активи – це інформація або бізнес-процеси, а вторинні активи – це пов'язані з ними IT-системи, інфраструктура та людські ресурси.

Організації повинні ідентифікувати основні активи та вторинні активи, які можуть впливати на первинні активи, як правило, надаючи детальну

інформацію про право власності на активи, їхнє місцезнаходження та функції.[26]

Вторинні активи зазвичай мають вразливості, які можуть бути використані загрозами, що мають на меті завдати шкоди первинним активам. Для кожного активу має бути призначена особа, відповідальна за його зберігання, обслуговування та безпеку. Ця відповідальна особа часто також є найбільш підходящою особою для визначення цінності активу;

- Ідентифікація загроз

Загроза інформаційній безпеці є сукупністю умов і факторів, що створюють реальну небезпеку порушення інформаційної безпеки. Під загрозою інтересам суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або побічно призвести до нанесення шкоди інтересам даних суб'єктів [27]

Ідентифікація загроз дозволяє виявляти потенційні проблеми та слабкі місця в інформаційних системах перед тим, як вони призведуть до інцидентів із порушенням інформаційної безпеки. Це дозволяє приймати запобіжні заходи та уникати серйозних наслідків;

- Ідентифікація вразливостей

Вразливість інформаційної безпеки - це слабке місце або дефект в системі, мережі, програмному забезпеченні чи іншому компоненті інформаційної технології, яке може бути використане для порушення цілісності, конфіденційності або доступності інформації. Вразливості можуть бути використані зловмисниками або несанкціонованими користувачами для незаконного доступу до інформації чи здійснення інших атак на систему.

Для ідентифікації вразливостей компанії проводиться оцінка безпеки для кожного інформаційного активу та визначення можливих вразливостей. Відповідальні особи розглядають технічні аспекти, включаючи програмне та апаратне забезпечення, а також організаційні аспекти.[28]

Важливо розрізняти безпосередній вплив на інформаційну безпеку та наслідки для ділової діяльності організації в результаті втрати конфіденційності, цілісності або доступності інформації. Вплив та наслідки повинні бути визначені та описані з достатньою точністю для кожної окремої події, в якій загроза використовує вразливість активу або засобу.

Найважливішою перевагою є те, що цей причинно-орієнтований підхід дозволяє систематично пов'язувати наслідки подій зі слабкими місцями активів і засобів. Це створює умови для того, щоб у подальшому процесі управління ризиками вибирати заходи цілком конкретно і цілеспрямовано, а також точно оцінювати їхню необхідну масштабність і ступінь впровадження. Це забезпечує як ефективність, так і результативність СУІБ. Цей підхід також може гарантувати, що всі відповідні ризики будуть враховані.

Недоліком цього підходу є потенційно великі зусилля. Визначити відповідні цінності не завжди легко. Кожна цінність може мати одну або кілька вразливостей, кожна з яких може бути використана однією або кількома загрозами.[29]

2.2 Оцінка ризиків інформаційної безпеки організації

Оцінка ризиків інформаційної безпеки є важливим етапом у забезпеченні ефективного управління безпекою в організації. Цей процес дозволяє визначити, які загрози можуть виникнути, оцінити їх потенційні наслідки та імовірність виникнення, і визначити стратегії для зменшення ризиків.

Структура керування ризиком забезпечує політикою, процедурами та організаційними заходами щодо запроваджування керування ризиком на всіх рівнях в організації. Організація має розробити, як частину цієї структури, політику чи стратегію, щоб мати змогу вирішувати, коли та як потрібно провадити загальне оцінювання ризику. [30]

Зокрема, необхідно, щоб особи, які виконують загальне оцінювання ризиків, мали чітке уявлення щодо наступних аспектів:

— оточення та стратегічних цілей організації;

— масштабу та характеру припустимих ризиків, а також ефективних методів обробки неприйнятних ризиків;

— взаємозв'язку загального оцінювання ризиків із бізнес-процесами організації;

— використання методів та методик для проведення загального оцінювання ризиків та їх внеску у процес управління ризиками;

— структури відповідальності, повноважень і звітності, пов'язаних із проведенням загального оцінювання ризиків;

— наявності необхідних ресурсів для виконання загального оцінювання ризиків;

— процедур звітності про результати загального оцінювання ризиків та їх критичного аналізу.

Ризики, які ставлять під загрозу безперервність діяльності компанії, вимагають іншого ставлення та заходів контролю, ніж незначні ризики. У рамках процесу оцінки здійснюється аналіз усіх визначених ризиків, оцінюється ймовірність їх реалізації та розмір можливих збитків.

Процедура оцінки ризиків інформаційної безпеки спрямована на ідентифікацію потенційних загроз та вразливостей в інформаційних системах та ресурсах організації. [31] Цей процес сприяє виявленню можливих ризиків для безпеки даних і впровадженню заходів для їх зменшення чи ефективного управління.

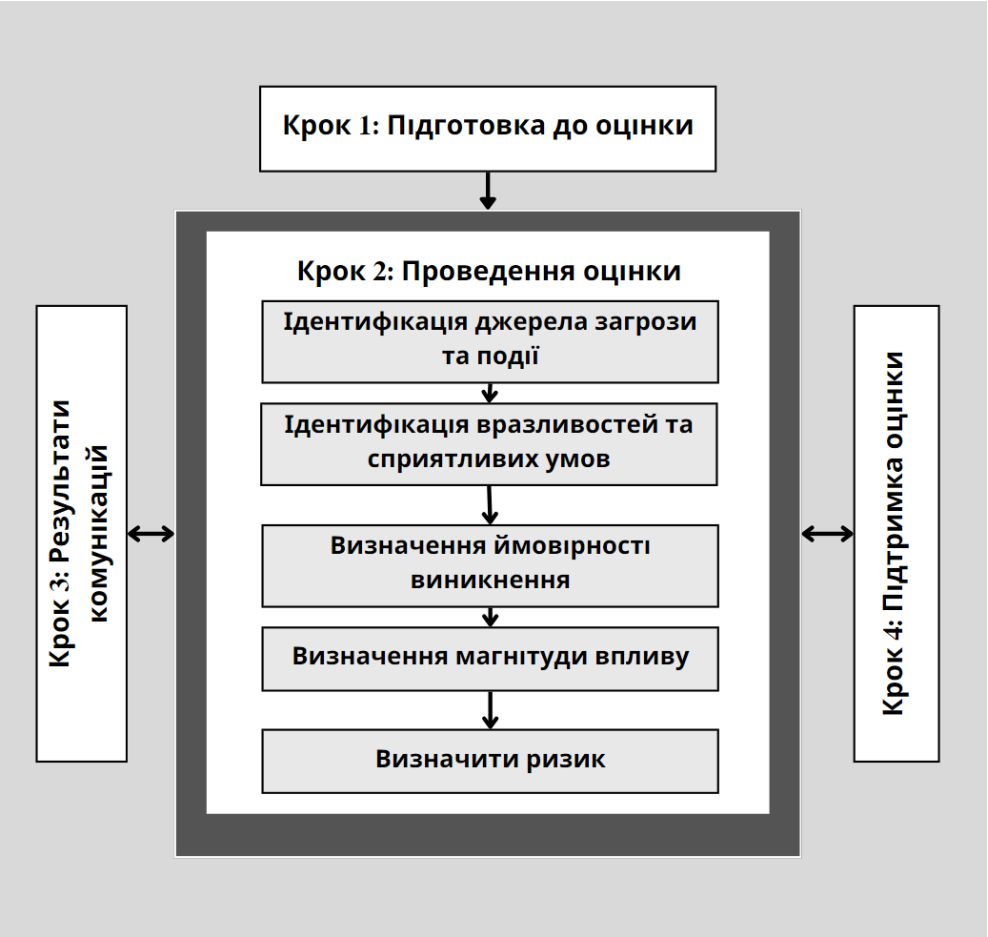

Рис. 2.1 Процес оцінки ризиків

Перший етап у процесі оцінки ризиків - це підготовка до проведення оцінки. Мета цього етапу полягає в установленні контексту для оцінювання ризиків. Цей контекст формується на основі результатів, отриманих на етапі визначення структури ризику під час процесу управління ризиками. Структура ризику включає, зокрема, організаційну інформацію щодо політики та вимог до проведення оцінювання ризиків, конкретні методології оцінювання, процедури відбору факторів ризику, обсяг оцінювання, деталізацію аналізу, ступінь формальності та вимоги, які сприяють систематичному та повторюваному визначенню ризиків в межах організації.[32]

Організації застосовують стратегію управління ризиками настільки, наскільки це можливо в практичному розумінні, для отримання інформації, необхідної для підготовки до оцінки ризиків. Процес підготовки до оцінювання ризиків включає в себе наступні завдання:

• Визначення мети оцінювання;

• Визначення області застосування оцінювання;

• Визначення припущень та обмежень, пов'язаних із проведенням оцінки;

• Визначення джерел інформації, які будуть використані як вхідні дані для оцінки; і

• Визначення моделі ризику та аналітичних підходів (тобто методів оцінки та аналізу), які будуть використовуватися під час проведення оцінювання.[33]

Другий етап у процесі оцінки ризиків - це проведення самої оцінки. Метою цього етапу є формування переліку ризиків інформаційної безпеки, які можуть бути систематизовані за рівнем ризику і використані для прийняття рішень щодо реагування на ці ризики. З метою досягнення цієї мети організації аналізують загрози та вразливості, враховуючи вплив та ймовірність, а також невизначеність, пов'язану з процесом оцінки ризиків.

Цей етап також включає збір необхідної інформації в рамках кожного завдання і виконується відповідно до контексту оцінки, визначеного на етапі "Підготовка" процесу оцінки ризиків. Очікується, що оцінка ризиків повинна адекватно враховувати всі аспекти загроз згідно з конкретними визначеннями, вказівками і напрямками, встановленими на етапі підготовки. Однак на практиці адекватне охоплення всього простору загроз може вимагати узагальнення джерел загроз, загрозливих подій та вразливостей, забезпечуючи повне охоплення та оцінку конкретних джерел, подій та вразливостей лише за необхідністю для досягнення цілей оцінки ризиків.[34] Проведення оцінки ризиків включає реалізацію наступних конкретних завдань:

- Визначення джерел загроз, які мають відношення до організації.
- Визначення подій загроз, які можуть бути ініційовані цими джерелами.
- Виявлення вразливостей в організації, які можуть бути використані джерелами загроз через конкретні події загроз, а також умов, які можуть впливати на успішну експлуатацію цих вразливостей.

- Визначення ймовірності того, що виявлені джерела загроз ініціюватимуть конкретні події загроз, а також ймовірність того, що ці події будуть успішними.
- Визначення негативних наслідків для операцій та активів організації, окремих осіб, інших організацій та держави в результаті використання вразливостей джерелами загроз (через конкретні події загроз).
- Визначення ризиків інформаційної безпеки як комбінації ймовірності використання вразливостей джерелами загрози та наслідків такого використання, включаючи будь-які невизначеності, пов'язані з визначенням ризиків. [35]

Третім етапом у процесі оцінки ризиків є передача результатів оцінки та обмін інформацією, пов'язаною з ризиками. Мета цього етапу полягає в забезпеченні, щоб особи, що приймають рішення в організації, мали відповідну інформацію, пов'язану з ризиками, необхідну для обґрунтування та прийняття рішень щодо ризиків. Інформування та обмін інформацією включають наступні конкретні завдання:

- Передача результатів оцінки ризиків;
- Обмін інформацією, отриманою під час проведення оцінки ризиків, для підтримки інших аспектів управління ризиками. [36]

Методи оцінки ризиків в інформаційній безпеці можна класифікувати на кількісні та якісні підходи. Кожен підхід має свої переваги та обмеження, і вибір конкретної методології залежить від потреб організації, характеру інформаційних активів та інших чинників.

До кількісних методів відносяться Квантитативний Аналіз Ризиків та Метод Монте-Карло.

QRA – це метод, який використовується для систематичного розрахунку ризиків від небезпечних подій. Він передбачає прогнозування розміру наслідків, пов'язаних з небезпекою, і частоти, з якою можна очікувати, що небезпека може виникнути. Потім ці аспекти об'єднуються для отримання числових значень ризику . QRA включає розгляд усіх ідентифікованих

небезпечних подій з метою кількісної оцінки загального рівня ризику. Подібні небезпечні події часто групуються і оцінюються разом як граничні або репрезентативні події. Існує ціла низка програмних пакетів сторонніх розробників для моделювання наслідків, оцінки частоти або повного аналізу ризиків, але багато з цих розрахунків також часто проводяться за допомогою електронних таблиць. [37]

Рис. 2.2 Структура процесу кількісного аналізу ризиків

Процес починається з виявлення значних і високих ризиків за допомогою якісного аналізу. Ці ризики повинні бути досліджені на предмет дублювання, схожості тригерів, впливу на вартість та/або графік та інших взаємозв'язків. Ризики, що мають спільну першопричину і можуть виникати разом, вирішуються шляхом кореляції ризиків, які пов'язані між собою. Збір високоякісних даних про ризики може бути складним завданням, оскільки їх

немає в жодній історичній базі даних, і їх слід збирати шляхом інтерв'ю, семінарів та іншими способами з використанням експертних оцінок.

Далі необхідна відповідна модель проекту як основа для кількісного аналізу ризиків. Моделі проекту, які найчастіше використовуються в кількісному аналізі ризиків, включають календарний план проекту (для часу) і постатейний кошторис витрат (для вартості). Кількісний аналіз ризиків особливо чутливий до повноти і правильності моделі проекту, яка використовується. Після цього застосовується процес Монте-Карло для моделювання ймовірнісної вартості та/або графіка проекту. [38]

Імітаційне моделювання є ключовим елементом, який дозволяє дослідникам зменшити ризик і вартість змін. Імітаційне моделювання за методом Монте-Карло (МНК) - це комп'ютеризований математичний метод, який надає особі, що приймає рішення, ряд можливих результатів і ймовірності їх настання, показуючи нижню і верхню межу можливостей разом з усіма можливими наслідками для проміжних рішень. У цьому дослідженні МНК використовується для генерації пов'язаних випадкових величин для загроз і вразливостей відповідно до їх визначеного розподілу, що дозволяє фахівцям бачити всі можливі результати і оцінювати наслідки ризику, щоб приймати кращі рішення в умовах невизначеності. [39]

До якісних методів належать Матриця ризиків та Метод Дерева Рішень

Матриця ризиків співвідносить активи, вразливості, загрози та засоби контролю організації та визначає важливість різних засобів контролю, що відповідають активам організації.

У поєднанні це призводить до створення матриці 4 x 4, з якої зчитується отриманий клас ризику. Оцінка окремих полів як "низький", "нормальний", "високий", "дуже високий" та їх колір залежить від конкретної організації та її готовності йти на ризик. [40]

ступінь захисту / ймовірність виникнення	НИЗЬКИЙ	НОРМАЛЬНИЙ	ВИСОКИЙ	ДУЖЕ ВИСОКИЙ
ДУЖЕ ЙМОВІРНИЙ	НИЗЬКИЙ	СЕРЕДНІЙ	ВИСОКИЙ	ДУЖЕ ВИСОКИЙ
ЙМОВІРНИЙ	НИЗЬКИЙ	СЕРЕДНІЙ	ВИСОКИЙ	ВИСОКИЙ
МОЖЛИВИЙ	НИЗЬКИЙ	НИЗЬКИЙ	СЕРЕДНІЙ	СЕРЕДНІЙ
НЕМОЖЛИВИЙ	НИЗЬКИЙ	НИЗЬКИЙ	НИЗЬКИЙ	НИЗЬКИЙ

Рис. 2.3 Приклад представлення матриці ризиків 4х4

Дерева рішень - це прогнозні моделі, які використовуються в машинному навчанні, статистиці та інтелектуальному аналізі даних. В інтелектуальному аналізі даних дерева рішень дуже популярні і широко використовуються для вирішення кількох завдань. Вони дуже популярні, тому що засновані на логіці і легко інтерпретуються. Дерева рішень - це комбінація математичних і обчислювальних методів, які можна використовувати для опису та узагальнення наборів даних. Ці моделі, засновані на деревах рішень, відображають спостереження за елементом, щоб зробити висновок про цільове значення елемента. Елементи представлені в гілках, а цільові значення представлені в листі дерева. У деревовидній моделі, якщо існує скінченна множина значень цільової змінної, то такі моделі називаються деревами класифікації. У моделі деревовидної структури мітки класів представлені листям, а кон'юнкції ознак - гілками. У деревах рішень, якщо цільова змінна приймає неперервне значення, то такі дерева називаються деревами регресії. Воно використовується для опису даних і може представляти рішення. В аналізі рішень його можна використовувати для прийняття рішень. Діяльність з прийняття рішень можна простежити як послідовність простих рішень. У класифікаторі, заснованому на дереві рішень, база знань фіксується в добре організованому вигляді. [41]

Вибір конкретної методології для оцінки ризиків повинен залежати від конкретних умов та цілей організації. Кількісні методи надають точні та кількісні результати, в той час як якісні методи можуть бути швидшими та простішими у використанні. Важливо враховувати специфіку галузі та рівень доступу до даних для ефективного впровадження методологій оцінки ризиків в інформаційній безпеці.

2.3 Технології мінімізації ризиків інформаційної безпеки організації

Мінімізація ризиків інформаційної безпеки в організації вимагає комплексного підходу, який включає в себе використання технологій, організаційних заходів та здійснення культурних змін усередині компанії.

Організаціям рекомендовано використовувати декілька технологічних аспектів, що будуть мінімізувати ризики інформаційної безпеки. Для цього підійдуть Системи контролю та моніторингу, Захист передачі даних, Аутентифікація та авторизація, Захист від зловмисного ПЗ, Навчання та обзнаність персоналу, Автоматизація безпекових заходів.

Системи контролю та моніторингу (СКМ) в інформаційній технології використовуються для постійного відстеження стану різних компонентів інфраструктури, мереж, програм та служб з метою забезпечення їх ефективності та безпеки. Основні завдання систем контролю та моніторингу включають виявлення аномалій, вирішення проблем, попередження витрат ресурсів та забезпечення відповідності встановленим стандартам і політикам. До цих систем відносяться Системи управління інцидентами та Системи виявлення вторгнень.[42]

Системи управління інцидентами в інформаційній безпеці призначені для ефективного виявлення, реагування та вирішення інцидентів безпеки в організації. Ці системи грають ключову роль у забезпеченні відновлення послуг та даних в разі інциденту та управління подіями, що впливають на безпеку.

Для опису процесу формування СМІБ використовується класична модель безперервного удосконалення процесів (рис. 4.1), що отримала назву від циклу Шухарта-Демінга - модель PDCA (Плануй, Plan - Виконуй, Do - Перевіряй, Check - Дій, Act). Стандарт ISO/IEC 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. [43]

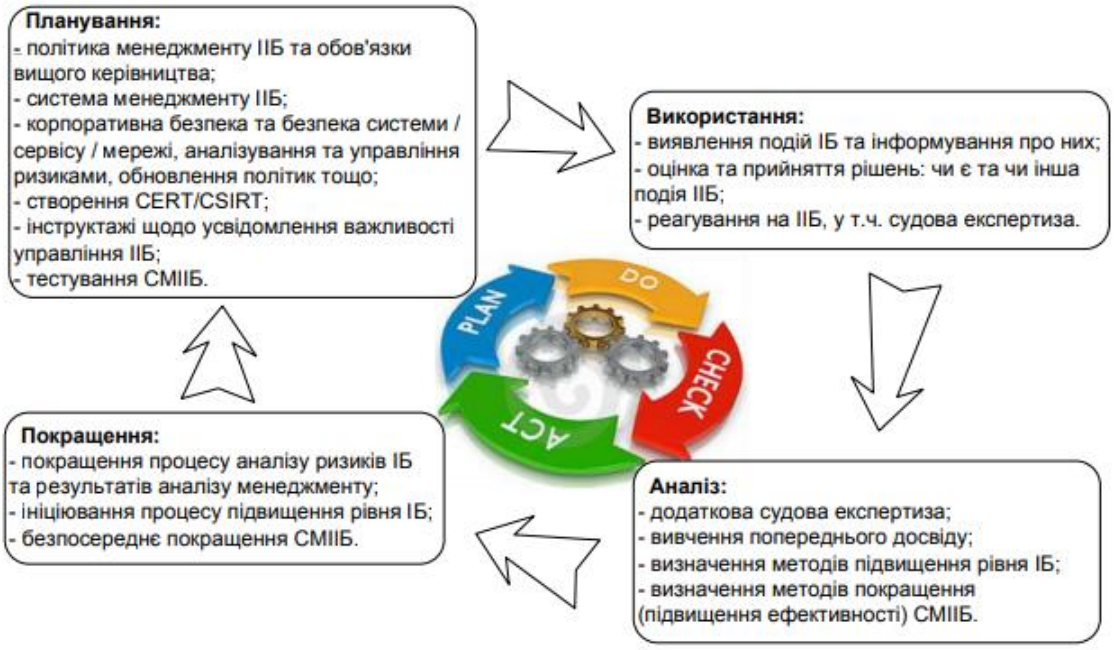

Рис. 2.4 – Етапи формування СМІІБ відповідно до моделі PDCA

Виявлення вторгнень - це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі, та їх аналіз на наявність ознак вторгнень, які визначаються як спроби порушити конфіденційність, цілісність, доступність або обійти механізми безпеки комп'ютера або мережі. Вторгнення спричиняються зловмисниками, які отримують доступ до систем з Інтернету, авторизованими користувачами систем, які намагаються отримати додаткові привілеї, на які вони не уповноважені, та авторизованими користувачами, які зловживають наданими їм привілеями. Системи виявлення вторгнень (IDS) - це програмні або апаратні продукти, які автоматизують цей процес моніторингу та аналізу. [44]

Під час передачі даних через мережі, інтернет або інші канали можуть виникати загрози їх конфіденційності, цілісності та доступності, що

автоматично робить захист передачі даних критично важливим аспектом інформаційної безпеки. Для забезпечення ефективного захисту передачі даних використовуються різні технології та методи, одні з яких VPN та Шифрування даних.

VPN - це топологія, розроблена для забезпечення безпеки мережевих з'єднань. Це головним чином спрямовано на те, щоб відокремити несанкціоновані хости для отримання доступу до мережі.

Звичайна мережа, відома як загальнодоступна мережа Інтернет, призначена для обміну даними з різним рівнем конфіденційності між великою кількістю людей і організацій. Для того, щоб захистити ці комунікації, була створена технологія тунелювання, а віртуальні приватні мережі є однією з найбільш використовуваних технологій. За допомогою ефективних протоколів віртуальної приватної мережі, VPN успішно забезпечує безпеку як для публічної мережі, так і для невеликих мереж, таких як домашня мережа. З іншого боку, віртуальні приватні мережі, такі як промислові або корпоративні мережі, також розділяються віртуальною приватною мережею. [45]

Шифрування даних - це процес перетворення відкритого тексту в зашифровану форму (нечитабельну), доступ до якої може отримати лише уповноважена особа/особи. Безпека даних є невід'ємною частиною діяльності особи/організації; вона може бути досягнута за допомогою різних методів. Зашифровані дані є безпечними протягом певного часу, але ніколи не думайте, що вони захищені назавжди. З часом існує ймовірність злому даних хакером. Підроблені файли передаються так само, як і зашифровані дані. На ринку існує багато алгоритмів для шифрування даних. Ключ шифрування відіграє головну роль у загальному процесі обробки даних.

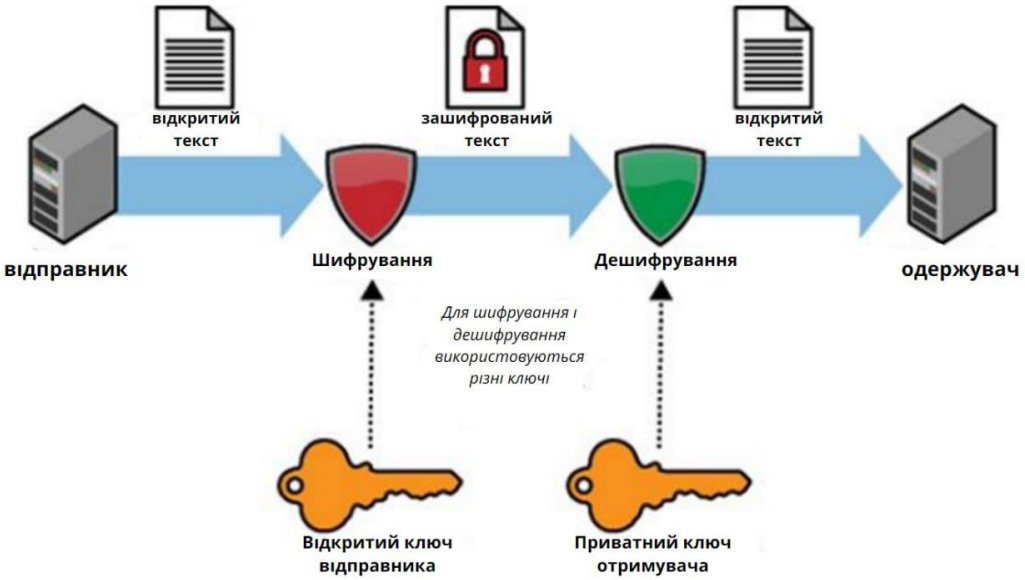

Рис. 2.5 Процес шифрування і дешифрування

Вивчення різних алгоритмів показує, що стійкість моделі залежить від управління ключами, типу криптографії, кількості ключів, кількості бітів, що використовуються в ключі. Всі ключі базуються на математичних властивостях. Ключі з більшою кількістю бітів вимагають більше часу на обчислення, що просто означає, що системі потрібно більше часу для шифрування даних. Шифрування даних AES є більш математично ефективним і елегантним криптографічним алгоритмом, але його основна перевага полягає в можливості вибору різної довжини ключа. [46]

Процеси аутентифікація та авторизації допомагають контролювати доступ до ресурсів та забезпечують, що тільки вірні користувачі можуть отримати доступ до визначених функцій інформаційної системи.

Автентифікація - це процес доведення того, що користувач з цифровою ідентичністю, який запитує доступ, є законним власником цієї ідентичності. Залежно від випадку використання, "ідентичність" може представляти людину або не-людину; може бути як індивідуальною, так і організаційною; і може бути перевірена в реальному світі в різному ступені, в тому числі не перевірена взагалі.

Авторизація – це процес визначення прав користувача на доступ до функціональних можливостей комп'ютерної програми та рівня, на якому цей

доступ має бути наданий. У більшості випадків "орган" визначає і надає доступ, але в деяких випадках доступ надається через невід'ємні права (наприклад, доступ пацієнта до його/її медичних даних). Авторизація – це оцінка того, який доступ або права повинна мати особа у певному середовищі. [47]

Мінімізувати ризики за допомогою автентифікації та авторизації можна через багатофакторну автентифікацію та рольову модель доступу.

Багатофакторна автентифікація - це все більш поширений захід безпеки, який впроваджується в онлайн-сервісах, щоб допомогти підтвердити особу користувача, який бажає отримати доступ до наданого контенту. Окрім традиційного імені користувача та пароля, MFA - це метод автентифікації, який вимагає від користувача введення певного додаткового коду або даних, якими володіє лише він сам.

Багатофакторна автентифікація є одним з найнадійніших способів захисту онлайн-акаунтів від зловмисників. Якщо хакер дізнається ім'я користувача та пароль, він не зможе отримати доступ до облікового запису, оскільки не зможе отримати або використати дані MFA, якщо MFA буде увімкнена в обліковому записі. Таким чином, це швидкий спосіб для компанії підвищити безпеку облікових записів своїх користувачів, не надаючи користувачеві більше інформації для запам'ятовування. [48]

Ролева модель доступу (Role-Based Access Control, RBAC) - це підхід до управління правами доступу, при якому права присвоюються користувачам на основі їх ролей в організації або системі. RBAC спрощує адміністрування та забезпечує більший контроль над безпекою, роблячи систему більш гнучкою та масштабованою.

Основні компоненти ролевої моделі доступу:

Ролі (Roles): Ролі визначають набір прав доступу, які пов'язані з певною функцією чи позицією в організації. Кожен користувач присвоюється одній або кільком ролям.

Користувачі (Users): Кожен користувач системи має свою унікальну ідентифікацію та може бути присвоєний одній або декільком ролям.

Операції (Operations): Користувачі можуть запитувати доступ до дій або процесів, що виконуються в обчислювальному середовищі.

Об’єкти (Objects): Користувачі може попросити доступ до об'єкта, статичного файлу, набору даних, веб-сайту або будь-якого іншого ресурсу.

Правила доступу (Permissions): Правила доступу визначають ті операції чи ресурси, до яких може мати доступ користувач на основі його ролі.

Сесії (Sessions): Визначають активні сесії користувачів та їхній поточний стан доступу. [49]

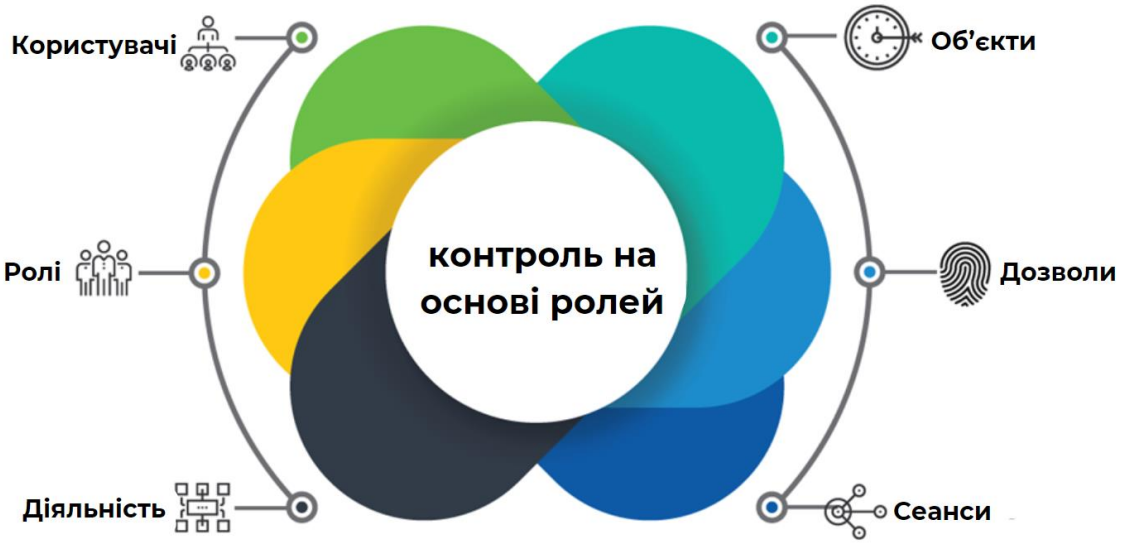

Рис. 2.6 Ключові компоненти контролю на основі ролей

Захист від зловмисного програмного забезпечення є надзвичайно важливим завданням для забезпечення безпеки інформаційних систем та манамізації ризиків. Зловмисне програмне забезпечення може призвести до втрати конфіденційної інформації, нанести шкоду функціонуванню системи, або використовувати ресурси комп'ютера без дозволу.

Антивірусне програмне забезпечення – це клас програм, призначених для запобігання, виявлення та видалення шкідливих програм на окремих комп'ютерних пристроях, мережах та IT-системах. Антивірусне програмне забезпечення, що було спочатку розроблене для виявлення і видалення вірусів

з комп'ютерів, може також захищати від широкого спектру загроз, включаючи інші типи шкідливого програмного забезпечення, такі як клавіатурні шпигуни, викрадачі браузерів, троянські програми, хробаки, руткіти, шпигунські програми, рекламні програми, ботнети і програми-вимагачі. [50]

Антивірусне програмне забезпечення зазвичай виконує такі основні функції:

- Сканування каталогів або окремих файлів на наявність відомих шкідливих шаблонів, що вказують на наявність шкідливого програмного забезпечення;
- Дозвіл користувачам планувати сканування, щоб воно виконувалося автоматично;
- Дозвіл користувачам ініціювати нові перевірки в будь-який час;
- Видалення виявленого шкідливого програмного забезпечення. Деякі антивірусні програми роблять це автоматично у фоновому режимі, тоді як інші повідомляють користувачів про зараження і запитують їх, чи хочуть вони очистити файли.

Для того, щоб всебічно перевірити систему, антивірусне програмне забезпечення, як правило, повинно мати привілейований доступ до всієї системи. Це робить антивірусне програмне забезпечення поширеною мішенню для зловмисників, і в останні роки дослідники виявили віддалене виконання коду та інші серйозні вразливості в антивірусних програмних продуктах. Для того, щоб всебічно перевірити систему, антивірусне програмне забезпечення, як правило, повинно мати привілейований доступ до всієї системи. Це робить антивірусне програмне забезпечення поширеною мішенню для зловмисників. [51]

Навчання та підвищення обізнаності персоналу є ключовими аспектами в забезпеченні ефективної інформаційної безпеки в організації. Люди виступають як перший ланцюг у системі безпеки, і їхнє правильне навчання дозволяє уникнути багатьох загроз та помилок. Організація регулярних семінарів та тренінгів, в які входять в тому числі і симуляції, а також перевірки

засвоєння матеріалу персоналом, надає можливість співробітникам вивчати новий матеріал, оновлювати свої знання і розвивати навички, що є ключовим для підтримки їхньої ефективності на робочому місці. [52]

Висновки до розділу 2

Підсумовуючи, важливо відзначити, що процес визначення потенційних загроз та вразливостей в інформаційних системах та ресурсах є критичним етапом у розробці стратегій управління ризиками. Здійснюючи ідентифікацію ризиків, необхідно не лише визначити джерела загроз та можливі події, але й урахувати вразливості, ймовірності виникнення подій та наслідки їх реалізації. Цей аналіз створює основу для подальшого ефективного управління ризиками та прийняття обгрунтованих стратегічних рішень щодо зменшення, передбачення та контролю інформаційних загроз. Результати ідентифікації ризиків формують важливий інформаційний фундамент для подальшого процесу оцінки ризиків та розробки ефективних заходів забезпечення інформаційної безпеки в організації.

У контексті оцінки ризиків інформаційної безпеки організації важливо визнати, що цей процес визначає ключові аспекти загроз, ймовірностей та потенційних наслідків, сприяючи розробці стратегій управління ризиками. Аналізуючи результати оцінки, виявлено, що інформаційна безпека вимагає комплексного підходу, що враховує якість інфраструктури, так і поведінкові аспекти користувачів. Ідентифікація та оцінка ризиків стають важливим етапом у розробці стратегій запобігання та реагування на потенційні загрози. Використання адекватних моделей оцінювання та аналітичних підходів сприяє збалансованому управлінню ризиками, забезпечуючи оптимальне поєднання заходів із збереженням інформаційної цілісності та доступності. В цілому, оцінка ризиків інформаційної безпеки визначає невід'ємну роль у створенні ефективної стратегії інформаційного забезпечення, спрямованої на забезпечення стійкості та надійності організаційних інформаційних систем.

У контексті використання технологій мінімізації ризиків інформаційної безпеки організації важливо підкреслити, що впровадження сучасних підходів та інноваційних рішень в цьому напрямку відіграє ключову роль у підвищенні стійкості та ефективності захисту інформації. Використання передових технологій, таких як шифрування, системи ідентифікації та автентифікації, а також системи виявлення та відновлення інцидентів, сприяє надійній захисті конфіденційності, цілісності та доступності інформаційних ресурсів. Важливо також підкреслити, що успішна реалізація технологій мінімізації ризиків вимагає системного підходу, врахування специфіки організаційної інфраструктури та постійного моніторингу з метою вчасного виявлення та вирішення потенційних загроз. Ці технологічні ініціативи є необхідною складовою організаційного стратегічного управління ризиками і грають ключову роль у підтримці інформаційної безпеки в умовах постійно зростаючого рівня цифрової загрози.

Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ В УПРАВЛІННІ РИЗИКАМИ ОРГАНІЗАЦІЇ

3.1 Рекомендації щодо вибору та впровадження технологій в організації

У сучасному динамічному світі ефективне впровадження технологій стає ключовим елементом успішної діяльності організацій. Розмаїття технологічних рішень та інноваційних підходів відкриває безліч можливостей для покращення ефективності, оптимізації процесів та забезпечення конкурентоспроможності. Проте, вибір та впровадження технологій вимагають ретельного аналізу, компетентності та врахування специфіки самої організації.

Хочу розглянути ключові рекомендації, спрямовані на вибір та ефективне впровадження технологій в організаційному середовищі. Зокрема, розгляну аспекти відбору оптимальних технічних рішень, стратегії інтеграції, а також питання забезпечення безпеки та сталого розвитку технологічного стеку організації. Описані рекомендації сприятимуть виробленню обґрунтованих стратегій вибору та використання технологій, спрямованих на досягнення поставлених бізнес-цілей та підвищення конкурентоспроможності.

Щоб успішно впроваджувати інновації та забезпечувати конкурентоспроможність, необхідно здійснити ретельний вибір ефективного впровадження технологій.

На рівні з загальним забезпеченням інформаційної безпеки організації керівнкии служб ІБ також повинні забезпечити дотримання політик та особистих правил безпеки всіма співробітниками, навіть якщо їх робота напряму не пов’язана з ІБ. [53]

Впровадження технологій в організацію – довгий і ретельний процес. Неправильний вибір стеку технологій для ваших бізнес-цілей може призвести до серйозних проблем, тому організації починають з загальних питань.

Поступово конкретизуючи питання, відповідальні особи обирають найкращу технологію впровадження і пропонують її керівництву. Також важливо слідкувати за трендами та новими дослідженнями в галузі управління ризиками організації аби підтримувати цю систему в нормальному стані. [54]

Процес вибору технології рекомендується починати з визначення потреб організації. Це дозволяє уникнути непотрібних витрат і спрямовує увагу на технології, які найкращим чином задовольнять конкретні вимоги та цілі. На цьому етапі треба визначити з якими загрозами стикається організація та, відповідно, вимоги до функціональності технології захисту. Також важливою інформацією буде проаналізовані бізнес-процеси, існуючі системи та ресурси. Створення стратегічного плану разом із зацікавленими сторонами буде враховувати майбутні потреби та тенденції в організації, тому також є дуже важливою частиною вибору технології. [55]

Дослідження різноманітних технологій, що могли б вирішити проблеми організації, є наступним підготовчим етапом. Він допоможе визначити пріоритетних проблем, проаналізувати наявні рішення та проконсультуватися з експертами, що можуть надати об’єктивні поради.

Після того, як було прийнято рішення про впровадження нової технології, потрібно розробити план її впровадження. Призначення особи або команди, яка розробить графік проекту, прискорить процес збору необхідних ресурсів, проконтролює адміністративні деталі та вирішить суперечливі пріоритети.

Наближаючись до кінця розробки, може бути гарною ідеєю створити пілотну програму. Таким чином, ви зможете легше продемонструвати нову технологію іншим відділам організації, а також вирішити будь-які проблеми. [56]

Навчання інших працівників користуватися новою технологією – це важливий процес, який може допомогти організації підвищити ефективність та продуктивність. Після всіх виконаних рекомендацій, компанія може запустити технологію.

3.2 Перспективи розвитку технологічних рішень в галузі управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки (ІБ) є важливим завданням для будь-якої організації, яка обробляє конфіденційну інформацію. Технологічні рішення відіграють ключову роль у цьому процесі, допомагаючи організаціям виявляти, оцінювати та реагувати на ризики ІБ.

В сучасному цифровому світі, де технології швидко розвиваються, питання забезпечення інформаційної безпеки стають важливішими, ніж будь-коли. Організації по всьому світу стикаються зі зростаючими загрозами та ризиками, пов'язаними з кібербезпекою. У цьому контексті важливо розглядати перспективи розвитку технологічних рішень в галузі управління ризиками інформаційної безпеки. [57]

Рис. 3.1 – Інструменти, які компанії використовують для управління ризиками

Розширення можливостей штучного інтелекту, використання аналітики великих даних, інтеграція блокчейн-технологій та інші інноваційні підходи обіцяють перетворити способи, якими ми взаємодіємо з цими викликами та змушують переосмислити стратегії захисту важливої інформації. У даному контексті дослідження перспектив розвитку технологічних рішень в цій галузі

виявляється надзвичайно актуальним та ключовим для підтримки стійкості та безпеки в сучасному цифровому середовищі.

Управління ризиками за допомогою штучного інтелекту використовує алгоритми машинного навчання для прогнозування майбутніх ризиків на основі історичних даних. Аналізуючи минулі інциденти безпеки та порушення нормативних вимог, ШІ може виявляти тенденції та вразливості, допомагаючи організаціям упереджувати ризики ще до того, як вони матеріалізуються. [58.]

Блокчейн має низку потенційних переваг, які можуть допомогти різним організаціям зменшити, а в деяких випадках і усунути ризики, які несуть у собі існуючі системи. Прихильники блокчейну наголошують на перевагах записів даних, які важко змінити, що сприяє збереженню записів і доказів.

Технології блокчейн наражають установи на знайомі ризики. Але ці ризики мають нові нюанси. Наприклад, хоча блокчейн і обіцяє ефективність, треба дивитися на те, як він працює. Блокчейн працює двома способами: без дозволу та з дозволом. [59]

Хмарна безпека стає ключовою перспективою розвитку технологічних рішень в галузі управління ризиками інформаційної безпеки. За останні кілька років росте популярність хмарних сервісів, що приводить до збільшення кількості конфіденційної інформації, зберіганої в хмарних середовищах. Відтак, виникає необхідність вдосконалення засобів захисту цих даних та управління з ними.

Хмарна безпека охоплює широкий спектр технологій та методів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних в хмарних обчисленнях. Вона включає в себе ідентифікацію та аутентифікацію користувачів, шифрування даних, контроль доступу, моніторинг активності та інші засоби захисту.

Щоб максимізувати переваги та мінімізувати ризики хмарних обчислень і кібербезпеки для управління ризиками, важливо узгодити свої стратегії з бізнес-цілями і схильністю до ризику, оцінити ризики і можливості, впровадити засоби контролю і заходи, відстежувати ефективність і

дотримання нормативних вимог, а також вчитися на власному досвіді. Регулярний перегляд цих стратегій може забезпечити їхню актуальність та ефективність. Однією з ключових переваг хмарної безпеки є масштабованість та гнучкість. [60]

Висновки до розділу 3

Розділ, присвячений рекомендаціям щодо використання технологій в управлінні ризиками організації, дозволив визначити ключові аспекти, які слід враховувати при виборі та впровадженні технологій у цьому контексті. Рекомендації щодо вибору та впровадження технологій в організації вказують на важливість врахування конкретних потреб та вимог організації при виборі відповідних рішень. Перспективи розвитку технологічних рішень в управлінні ризиками інформаційної безпеки свідчать про те, що високотехнологічні підходи, такі як штучний інтелект та хмарні технології, можуть відігравати ключову роль у нейтралізації сучасних кіберзагроз та удосконаленні процесів безпеки.

Очікується, що технологічні рішення в галузі управління ризиками ІБ будуть продовжувати розвиватися в найближчі роки. Це дозволить організаціям ефективніше захищати свою інформацію від кіберзагроз.

ШІ та машинне навчання будуть використовуватися для автоматизації завдань управління ризиками ІБ, таких як виявлення загроз, оцінка ризиків та розробка планів реагування.

Хмарні безпекові технології будуть продовжувати використовуватися для управління ризиками ІБ. Хмарні сервіси ІБ пропонують ряд переваг, включаючи доступність, масштабованість та зниження витрат.

Зростання об'єднання технологій. Технології управління ризиками ІБ будуть все більше об'єднуватися з іншими технологіями, такими як кібербезпека, управління бізнес-процесами та управління ризиками. Це

дозволить організаціям отримувати більш комплексний погляд на ризики ІБ та розробляти більш ефективні заходи реагування.

ВИСНОВКИ

Процеси управління ризиками інформаційної безпеки та вимірювання їх показників є дуже важливою темою в контексті сучасних викликів і тенденцій у сфері інформаційної безпеки.

Дипломна робота з управління ризиками інформаційної безпеки організації представляє собою комплексне дослідження, спрямоване на розкриття та вивчення ключових аспектів цієї важливої теми. Робота включає три основних розділи, кожен із яких спрямований на вивчення конкретних аспектів управління ризиками інформаційної безпеки.

Розглянуто фундаментальні поняття та теоретичні аспекти, пов'язані з управлінням ризиками. Автор вивчає основні підходи, методи та стандарти, що визначаються для визначення, оцінки та управління ризиками інформаційної безпеки.

Проаналізовано конкретні виклики, з якими стикаються організації в процесі визначення та управління ризиками, зокрема, в контексті внутрішніх та зовнішніх факторів.

Надано конкретні поради та рекомендації щодо використання сучасних технологій у сфері управління ризиками. Запропоновано виважений підхід до вибору та впровадження технологій, які можуть ефективно підтримати процеси управління ризиками інформаційної безпеки.

У висновку до цієї дипломної роботи важливо підкреслити, що вивчення та розуміння різних аспектів управління ризиками інформаційної безпеки в сучасному світі є надзвичайно актуальним завданням для будь-якої організації. Застосування наукових підходів та використання сучасних технологій можуть ефективно забезпечити надійний захист інформації та знизити ризики для бізнесу. Ця робота стане корисним внеском у розвиток та впровадження ефективних стратегій управління ризиками інформаційної безпеки в сучасному бізнес-середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стандарти в галузі управління ризиками інформаційної безпеки : тези. В. О. Залога та ін. 2014. URL: http://essuir.sumdu.edu.ua/handle/123456789/40088

2. Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави. П. Сніцаренко та ін. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. 2022. с. 47–55. URL: https://doi.org/10.33099/2304-2745/2022-2-75/47-55

3. Соколовська А. А. Система управління інцидентами інформаційної безпеки : thesis. 2021. URL: http://ir.stu.cn.ua/123456789/22662

4. Козаченко П., Панаско О. Управління інцидентами в контексті інформаційної безпеки підприємства. Specialized and multidisciplinary scientific researches. 2020. URL: https://doi.org/10.36074/11.12.2020.v2.33

5. Варжанський І. Актуальні проблеми і можливості планування політики інформаційної безпеки в Україні. XI Міжнародна науково-практична конференція «Сучасні проблеми управління: трансформація публічного управління у постковідному світі». Київ, Україна, 2021. URL: https://doi.org/10.20535/spu2021.249171

6. Кравченко К. О. Забезпечення інформаційної безпеки у системах комплексного управління підприємством. Адаптивні системи автоматичного управління. 2011. Т. 1, № 18. С. 71–80. URL: https://doi.org/10.20535/1560-8956.18.2011.33481

7. Терещенко Л. Управління ризиками інформаційних систем: етапи процесу управління ризиками. Економіка та суспільство. 2021. № 31. URL: https://doi.org/10.32782/2524-0072/2021-31-12

8. Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій. Foreign trade: economics, finance, law. 2022. Т. 125, № 6. С. 73–82. URL: https://doi.org/10.31617/3.2022(125)05

9. Варжанський І. Актуальні проблеми і можливості планування політики інформаційної безпеки в Україні. XI Міжнародна науково-практична конференція «Сучасні проблеми управління: трансформація публічного управління у постковідному світі». Київ, Україна, 2021. URL: https://doi.org/10.20535/spu2021.249171

10. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / С. О. Гнатюк та ін. Ukrainian information security research journal. 2012. Т. 14, № 1 (54). URL: https://doi.org/10.18372/2410-7840.14.2073 [3]

11. Грінченко Є. М., Колмик О. О. Методи управління інформаційними ризиками. Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених “Комп’ютерна інженерія і кібербезпека: досягнення та інновації”. Кропивницький: 2018.

12. Управління ризиками та захист даних. URL:https://iitd.com.ua/upravlenie-riskami-i-zashchita-dannyh/

13. Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах. URL: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdf

14. Кузьо, Марко Олегович. Порівняльний аналіз методик оцінювання ризиків інформаційної безпеки у вищих навчальних закладах. URL: http://elartu.tntu.edu.ua/handle/lib/30729

15. ISO/IEC 27005:2015. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

16. NIST 800-30. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

17. Shevchuk I. B., Starukh A. I., Vaskiv O. M. Business risk management techniques and expert methods of their evaluation. № 2. 2020. URL: https://www.business-inform.net/export_pdf/business-inform-2020-2_0-pages-295_306.pdf

18. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови [Чинний від 01.01.2019]. 2018.

19. Шадська У. С. Аналіз ризиків під час обробки персональних даних: що важливо знати? : посібник. Київ : *Компринт*, 2021. 68 с. URL : https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

20. What Is ISO 9001. *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/what-iso-9001-continuum-grc

21. Столєтов Ю. В. Управління ризиками, як елемент державного регулювання зовнішньоекономічної діяльності. *Державне управління: удосконалення та розвиток*. 2011. № 10. URL : http://www.dy.nayka.com.ua/?op=1&z=340

22. Brandenburg. G. ISO27005 series part 2: Context Establishment. *CTRL Disrupt* : веб-сайт. URL : https://ctrl-disrupt.nl/-insights-news/iso27005-series-part-2-context-establishment

23. Step 2: Risk Assessment. *United Nations Development Programme*. URL : https://info.undp.org/sites/ERM/SitePages/Step%202%20-%20Risk%20Assessment.aspx

24. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. [Чинний від 17.08.2023]. 2023.

25. Березуцький В.В., Адаменко М.І. Небезпечні виробничі ризики та надійність : посібник. Харків : НТУ «ХПІ», 2016. 385 с.

26. Why ISO 27005 risk management is the key to achieving ISO 27001 certification. *IT Governance* : веб-сайт. URL : https://www.itgovernance.co.uk/blog/why-iso-27005-risk-management-is-key-to-iso-27001

27. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці. *Державне управління*. 2019. № 2 (66).

28. Understanding vulnerabilities. *National Cyber Security Centre* : веб-

сайт. URL : https://www.ncsc.gov.uk/information/understanding-vulnerabilities

29. Литюга Ю. В., Позняк С. В. Процесне управління ризиками розвитку підприємства як джерело його конкурентоспроможності. Дніпро : *Ефективна економіка*, 2015. № 9. URL : http://www.economy.nayka.com.ua/?op=1&z=4612

30. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. Київ, 2015.

31. S. Ali Torabi, Ramin Giahi. An enhanced risk assessment framework for business continuity management systems. *Safety Science*. 2016. Vol. 89. P. 201-218. URL : https://www.sciencedirect.com/science/article/abs/pii/S0925753516301266

32. Five Steps of the Risk Management Process. *360factors* : веб-сайт. URL : https://www.360factors.com/blog/five-steps-of-risk-management-process/

33. Preparation of risk assessment for money laundering and terrorist financing. Kalkofnsvegur, 2022. URL : https://en.fme.is/media/utgefid-efni/Preparation-of-risk-assessment.pdf

34. Risk Assessment Process Manual. ARCS, 2020. URL : https://www.arcsinfo.org/content/documents/risk_assessment_process_manual.pdf

35. Introduction to SP 800 30 revision 1. *Cyvatar* : веб-сайт. URL : https://cyvatar.ai/nist-csf-sp-800-30

36. Quantitative Risk Assessment (QRA). *Risktec essential*. URL : https://www.risktec.tuv.com/wp-content/uploads/2018/11/Risktec-QRA-brochure-i1.0-med-res-single-pages.pdf

37. Jurie Steyn. Quantitative Risk Analysis for Projects. *OTC*, 2018. URL : https://www.ownerteamconsult.com/wp-content/uploads/2020/03/Insight-Article-050-Quantitative-Risk-Analysis.pdf

38. S. M. H. Bamakan, M. Dehghanimohammadabadi. A Weighted Monte Carlo Simulation Approach to Risk Assessment of Information Security Management System. International Journal of Enterprise Information Systems. 2016. URL : https://www.researchgate.net/publication/289556184

39. Risikomanagement in der Informationssicherheit. *Verband der Automobilindustrie*. 2021. URL : https://www.vda.de/dam/jcr:152a90b4-fd97-4f5c-88aa-4c45f506ceef/Whitepaper%20Risikomanagement%20in%20der%20Informationssicherheit.pdf?mode=view

40. D. P. Gaikwad. Intrusion Detection System Using Ensemble of Decision Trees and Genetic Search Algorithm as a Feature Selector. *International journal of information security science*. 2020. Vol.9. No.2, P.104-113. URL : https://dergipark.org.tr/en/download/article-file/2160168

41. C. Bulla, M. Birje. Cloud Monitoring System: Basics, Phases and Challenges. *International Journal of Recent Technology and Engineering*. Vol. 8 Issue 3. 2018. P. 4732-4746. URL : https://www.researchgate.net/publication/344629700_Cloud_Monitoring_System_Basics_Phases_and_Challenges

42. Аудит та управління інцидентами інформаційної безпеки : посібник. / Корченко О.Г. та ін. Київ : НА СБУ, 2014. URL : https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

43. ISO 27001 Clause 6.1.2 Information security risk assessment process. *Infocerts* : веб-сайт. URL : https://infocerts.com/iso-27001-clause-6-1-2-information-security-risk-assessment-process/

44. NIST Special Publication on Intrusion Detection System

45. Z. Nagy, M. K. Wali. Virtual private network impacts on the computer network performance with different traffic generators. *IOP Conference Series Materials Science and Engineering*. 2020. URL : https://www.researchgate.net/publication/343585636

46. Dr. Kiramat ullah, A. Khurum, Z. Haider. Securing Data Encryption. URL : https://core.ac.uk/download/pdf/275586829.pdf

47. M. Epping, M. Morowczynski. Authentication and Authorization. 2021. URL :https://www.researchgate.net/publication/359387651_Authentication_and_Author

ization

48. J. Williamson, K. Curran. Best Practice in Multi-factor Authentication. *Semiconductor Science and Information Devices*. 2021. № 3(1). URL : https://www.researchgate.net/publication/351852137_Best_Practice_in_Multi-factor_Authentication

49. C. BasuMallick. What Is Role-Based Access Control? Definition, Key Components, and Best Practices. *Spiceworks* : веб-сайт. URL : https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-role-based-access-control

50. B. Lutkevich. Malware definition. *TechTarget*. URL : https://www.techtarget.com/searchsecurity/definition/malware

51. Anti virus : лекційний матеріал. URL : https://gppanchkula.ac.in/wp-content/uploads/2020/04/Antivirus-software.pdf

52. Training & Awareness Procedure. *IGS*. 2020. URL : https://henhamugley.essex.sch.uk/wp-content/uploads/2019/11/Training-and-Awareness-Procedure.docx.pdf

53. Role of Digital Transformation for Achieving Sustainability: Mediated Role of Stakeholders, Key Capabilities, and Technology / R. Martínez-Peláez et al. *Sustainability*. 2023. №15(14). URL : https://www.mdpi.com/2071-1050/15/14/11221

54. 7 Tips to Choose the Best Technology for Your Company. *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/7-tips-choose-best-technology-your

55. Perspectives on transforming cybersecurity. *Digital McKinsey and Global Risk Practice*. 2019. URL : https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

56. How to Implement New Technology in Your Organization. *CR-T* : веб-сайт. URL : https://www.cr-t.com/blog/how-to-implement-new-technology-in-

your-organization/

57. Infographic: Technology in Risk Management in the Banking Sector. *Decide* : веб-сайт. URL : https://decidesoluciones.es/en/infographic-technology-in-risk-management/

58. The Role of Artificial Intelligence in Automated Risk Assessments. *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/role-artificial-intelligence-automated-risk-assessments-cyberarrow#:~:text=AI-driven%20risk%20assessments%20leverage,mitigate%20risks%20before%20they%20materialize

59. Blockchain risk management. *Deloitte* : веб-сайт. URL : https://www2.deloitte.com/mt/en/pages/risk/articles/mt-blockchain-risk-management.html

60. What are the emerging risks and opportunities of cloud computing and cybersecurity for risk management? *Linkedin* : веб-сайт. URL : https://www.linkedin.com/advice/3/what-emerging-risks-opportunities-cloud-computing#best-practices-for-cloud-computing-and-cybersecurity