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: “ СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ГАЛУЗІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Олександр КОДИМСЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Олександр КОДИМСЬКИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кодимському Олександру Михайловичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Стратегії управління ризиками інформаційної безпеки в галузі критичної інфраструктури”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *методи та засоби управління ризиками інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати теоретичні основи ризик-менеджменту.
   4.2. Дослідити процеси управління ризиками ІБ в галузі критичної інфраструктури.
   4.3. Проаналізувати особливості вдосконалення стратегій управління ризиками ІБ.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ ризик-менеджменту	08.04.2024	
4.	Дослідження процесів управління ризиками ІБ в галузі критичної інфраструктури	22.04.2024	
5.	Аналіз особливостей вдосконалення стратегій управління ризиками ІБ	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Олександр КОДИМСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(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 бакалавра

Направляється здобувач Кодимський О.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Стратегії управління ризиками інформаційної безпеки в галузі критичної інфраструктури"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КОДИМСЬКИЙ Олександр у кваліфікаційній роботі проаналізував теоретичні основи ризик-менеджменту, дослідив процеси управління ризиками ІБ в галузі критичної інфраструктури, вивчив особливості вдосконалення стратегій управління ризиками ІБ.

КОДИМСЬКИЙ Олександр показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів здатність самостійного володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КОДИМСЬКОГО Олександра на оцінку "_____" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кодимський О.М. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОДИМСЬКОГО Олександра
на тему “Стратегії управління ризиками інформаційної безпеки в галузі критичної інфраструктури”

Актуальність. Аналіз стратегій управління ризиками інформаційної безпеки у сфері критичної інфраструктури є надзвичайно важливим завданням з огляду на зростання загроз національній безпеці, громадській безпеці та економічній стабільності. Критичні об'єкти інфраструктури, такі як енергетика, транспорт, охорона здоров'я, все частіше стають об'єктами складних кібератак, що зумовлює необхідність створення надійних систем управління ризиками. Відповідно, необхідно задовольнити нагальну потребу в передових стратегіях для виявлення, оцінки та зменшення ризиків інформаційної безпеки, тим самим підвищуючи стійкість критично важливих систем.

З огляду на зазначене дослідження проблеми дослідження стратегій управління ризиками в галузі критичної інфраструктури є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено особливості стратегій управління ризиками інформаційної безпеки в галузі критичної інфраструктури .
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.
3. Автор опрацював значну джерельну базу: 45 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо вдосконалення стратегій управління ризиками ІБ.

Недоліки.

Доцільно було б приділити більше уваги розробці комплексних методик оцінки ризиків інформаційної безпеки для об'єктів критичної інфраструктури, а також інтеграції цих методик у загальну стратегію управління безпекою

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач КОДИМСЬКИЙ Олександр заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 5 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 56 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження ефективності стратегій управління ризиками інформаційної безпеки у секторах критичної інфраструктури.

Об'єктом дослідження є процеси управління ризиками інформаційної безпеки у галузі критичної інфраструктури.

Предмет дослідження – особливості і методи стратегічного управління ризиками інформаційної безпеки у галузі критичної інфраструктури.

Методи дослідження включають аналіз та синтез, порівняння, класифікацію, експертну оцінку, системний підхід до управління ризиками ІБ в галузі критичної інфраструктури.

Як результат у роботі проаналізовано теоретичні основи ризик-менеджменту, досліджено процесів управління ризиками ІБ в галузі критичної інфраструктури; вивчено особливості вдосконалення стратегій управління ризиками ІБ, а також запропоновано рекомендації щодо вдосконалення стратегій управління ризиками ІБ.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління ризиками інформаційної безпеки в галузі критичної інфраструктури.

Ключові слова: КРИТИЧНА ІНФРАСТРУКТУРА, УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ, ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 5 figures, conclusions and the list of references containing 45 items. The total volume of the work is 56 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to to investigate the effectiveness of information security risk management strategies in the critical infrastructure sectors.

The object of the study is the processes of information security risk management in critical infrastructure.

The subject of the study is the features and methods of strategic information security risk management in critical infrastructure.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to information security risk management in critical infrastructure.

As a result, the work analyzed theoretical foundations of risk management, investigated the processes of information security risk management in the field of critical infrastructure, studied the features of improving information security risk management strategies, and offered recommendations for improving information security risk management strategies.

Field of application. The developed approaches can be used in the planning and implementation of the information security risk management system in the field of critical infrastructure.

Keywords: CRITICAL INFRASTRUCTURE, RISK MANAGEMENT, INFORMATION SECURITY, RISK MANAGEMENT STRATEGIES, CRITICAL INFRASTRUCTURE PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
ПЗ	Програмне забезпечення
СУІБ	Система управління інформаційною безпекою

ВСТУП

Актуальність теми. У сучасному світі критична інфраструктура, як засіб життєзабезпечення суспільства, постійно стикається з кіберзагрозами, що можуть серйозно підірвати національну безпеку і стабільність держав. Забезпечення інформаційної безпеки в секторах критичної інфраструктури є важливішим ніж будь-коли раніше, оскільки наслідки втручання можуть бути катастрофічними. Також необхідність управління інформаційними ризиками вимагає комплексного підходу та використання спеціалізованих технологій та стратегій, щоб адекватно реагувати на постійно змінювані загрози.

Мета роботи полягає в дослідження ефективності стратегій управління ризиками інформаційної безпеки у секторах критичної інфраструктури та розробці рекомендацій щодо їх вдосконалення.

Об'єкт дослідження – процеси управління ризиками інформаційної безпеки в галузі критичної інфраструктури.

Предмет дослідження – особливості і методи стратегічного управління ризиками інформаційної безпеки у галузі критичної інфраструктури.

Для досягнення цієї мети в роботі необхідно виконати наступні ***завдання***:

1. Проаналізувати теоретичні основи ризик-менеджменту.
2. Дослідити процеси управління ризиками ІБ в галузі критичної інфраструктури.
3. Проаналізувати особливості вдосконалення стратегій управління ризиками ІБ.

Методи дослідження включають аналіз та синтез, порівняння, класифікацію, експертну оцінку, системний підхід до управління ризиками ІБ в галузі критичної інфраструктури.

Практичне значення одержаних результатів. Результати дослідження дозволяють сформувати практичні рекомендації для допомоги керівництву організацій критичної інфраструктури у здійсненні обґрунтованих рішень щодо управління ризиками ІБ, спрямованих на зниження вразливості до кіберзагроз та

підвищення загального рівня безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ РИЗИК-МЕНЕДЖМЕНТУ

1.1 Визначення ролі ризик-менеджменту у забезпеченні ІБ

Ризик-менеджмент є основною складовою процесу забезпечення ІБ, що полягає у систематичному підході до виявлення, оцінки, управління та моніторингу ризиків, пов'язаних з інформаційними активами організації. Ефективний ризик-менеджмент допомагає знизити ймовірність виникнення інцидентів безпеки та мінімізувати їхній вплив на організацію.

Одним із найважливіших завдань ризик-менеджменту є виявлення ризиків. Це включає ідентифікацію всіх можливих загроз і вразливостей, які можуть вплинути на інформаційні активи організації. Загрози можуть бути як зовнішніми (наприклад, хакерські атаки, віруси), так і внутрішніми (помилки співробітників, неналежне використання ресурсів).

Під час ідентифікації ризиків важливо розглядати всі можливі сценарії та враховувати всі активи, які можуть бути вразливими до загроз. Це дозволяє створити комплексну картину ризиків, з якими може стикнутися організація. Оцінка ризиків полягає в аналізі ймовірності виникнення кожного ризику та потенційного впливу на організацію. Цей процес дозволяє визначити, які ризики є найбільш критичними і вимагають негайних заходів. Використання кількісних і якісних методів оцінки ризиків дозволяє організації отримати всебічне розуміння ризикового ландшафту [1].

Після виявлення та оцінки ризиків організація повинна розробити стратегії для управління цими ризиками. Це може включати уникнення ризиків, зниження їхньої ймовірності або впливу, перенесення ризиків (наприклад, через страхування) або прийняття ризиків, якщо їхній вплив є допустимим.

Управління ризиками включає впровадження заходів контролю, таких як технічні (фаєрволи, антивірусне програмне забезпечення), організаційні (політики та процедури) та фізичні (контроль доступу до приміщень). Ці заходи допомагають зменшити вразливості та підвищити рівень захисту інформаційних

активів. Крім того, важливо розробити плани реагування на інциденти, які включають дії у випадку виникнення загроз або реалізації ризиків. Ці плани повинні містити чіткі інструкції щодо реагування, залучення відповідальних осіб та необхідні ресурси для усунення загрози.

Ризик-менеджмент не є одноразовим процесом; він вимагає постійного моніторингу та перегляду. Організації повинні регулярно перевіряти ефективність впроваджених заходів і адаптувати їх відповідно до нових загроз та змін у середовищі.

Моніторинг включає регулярні аудити безпеки, тестування систем на вразливості та аналіз інцидентів безпеки. Це дозволяє вчасно виявляти нові загрози та вразливості, які можуть вплинути на інформаційні активи організації. Перегляд політик і процедур дозволяє забезпечити їхню актуальність та відповідність сучасним вимогам безпеки. Наприклад, важливо регулярно оновлювати антивірусне програмне забезпечення, фаєрволи та інші засоби захисту для забезпечення їхньої ефективності [2].

Загальна схема процесу управління ризиками ІБ представлена на рис. 1.1.

Рис 1.1. Загальна схема процесу управління ризиком

Ризик-менеджмент є ключовим елементом стратегії інформаційної безпеки, оскільки він дозволяє організаціям проактивно підходити до захисту своїх інформаційних активів. Ефективний ризик-менеджмент забезпечує:

- захист конфіденційності, цілісності та доступності інформації: зниження ймовірності несанкціонованого доступу, модифікації або знищення даних. Це досягається через впровадження різних заходів контролю, таких як шифрування даних, використання багатофакторної аутентифікації та контроль доступу до інформаційних систем;
- зменшення фінансових втрат: мінімізація витрат, пов'язаних з інцидентами безпеки, такими як витік даних або кібератаки. Ризик-менеджмент дозволяє виявити потенційні загрози на ранніх стадіях та вжити заходів для їх усунення або зниження їхнього впливу. Це може включати витрати на впровадження захисних технологій, навчання персоналу та страхування;
- підвищення довіри з боку клієнтів та партнерів: забезпечення надійного захисту інформації сприяє зміцненню репутації організації. Клієнти та партнери оцінюють здатність організації захищати їхні дані, що може впливати на рішення про співпрацю. Впровадження ефективного ризик-менеджменту допомагає організаціям продемонструвати свою відповідальність та здатність забезпечити безпеку інформації;
- відповідність законодавчим і нормативним вимогам: виконання вимог законодавства у сфері захисту даних і інформаційної безпеки. Це включає дотримання міжнародних стандартів, таких як ISO/IEC 27001, NIST SP 800-30, а також національних вимог. Відповідність нормативним вимогам допомагає уникнути штрафів та інших санкцій, а також забезпечує високий рівень захисту інформації;

Ризик-менеджмент відіграє ключову роль у забезпеченні інформаційної безпеки, дозволяючи організаціям проактивно підходити до захисту своїх інформаційних активів, зменшувати вплив потенційних загроз та забезпечувати стабільну і безпечну роботу. Він сприяє створенню комплексної системи

безпеки, яка враховує всі аспекти діяльності організації та забезпечує високий рівень захисту в умовах постійно змінюваного кіберландшафту [3].

Організаціям важливо впроваджувати ефективні стратегії ризик-менеджменту та регулярно переглядати їх для забезпечення відповідності сучасним вимогам та загрозам. Це включає постійне навчання персоналу, впровадження нових технологій та інструментів захисту, а також адаптацію політик і процедур до змін у зовнішньому середовищі. Впровадження ризик-менеджменту допомагає організаціям створити стійку та надійну систему захисту інформаційних активів, що є важливим для успішної та безпечної діяльності в сучасному цифровому світі.

1.2 Аналіз стандартів та методологій управління ризиками ІБ

Управління ризиками ІБ є складним і багатогранним процесом, який вимагає чітко визначених стандартів та методологій для ефективного впровадження. У цьому розділі ми розглянемо основні стандарти та методології, які використовуються для управління ризиками ІБ, і їхній вплив на забезпечення безпеки в організаціях [4].

ISO/IEC 27001 є одним з найвідоміших міжнародних стандартів для управління ІБ, що визначає вимоги до створення, впровадження, підтримки та постійного покращення СУІБ. Цей стандарт охоплює численні аспекти, включаючи управління ризиками, розробку політик безпеки, управління інцидентами та навчання персоналу. Основною метою ISO/IEC 27001 є допомога організаціям у захисті їхніх інформаційних активів, забезпечуючи конфіденційність, цілісність та доступність інформації. Впровадження СУІБ відповідно до вимог ISO/IEC 27001 починається з ідентифікації та оцінки інформаційних ризиків, що дозволяє організаціям визначити слабкі місця та потенційні загрози для своїх інформаційних систем. На основі проведеної оцінки ризиків розробляються та впроваджуються політики безпеки, що регулюють порядок доступу до інформаційних ресурсів, методи захисту інформації та

процедури реагування на інциденти. Одним з важливих елементів стандарту є управління інцидентами, що включає в себе виявлення, реєстрацію, аналіз та реагування на інциденти інформаційної безпеки. Це дозволяє організаціям оперативно реагувати на порушення безпеки, мінімізуючи їх негативні наслідки та запобігаючи повторенню подібних інцидентів у майбутньому. Навчання персоналу також є ключовим аспектом ISO/IEC 27001, оскільки людський фактор часто стає причиною порушень безпеки. Стандарт передбачає проведення регулярних тренінгів та навчальних програм для підвищення обізнаності співробітників щодо питань інформаційної безпеки та їхньої відповідальності за захист інформаційних активів організації. Постійне покращення СУІБ, яке передбачає регулярний перегляд та оновлення політик, процедур та засобів захисту, є невід'ємною частиною стандарту. Це дозволяє організаціям адаптувати свої системи безпеки до нових загроз та змін у внутрішньому та зовнішньому середовищі. Впровадження та сертифікація за стандартом ISO/IEC 27001 демонструє прихильність організації до високих стандартів інформаційної безпеки, що може підвищити довіру з боку клієнтів, партнерів та регуляторів [5].

NIST (Національний інститут стандартів і технологій США) розробив спеціальну публікацію 800-30, яка надає керівництво з управління ризиками для інформаційних систем. Цей документ включає методи ідентифікації, оцінки та управління ризиками, а також рекомендації щодо впровадження контролю безпеки. NIST SP 800-30 є дуже детальним і охоплює всі аспекти управління ризиками, що робить його корисним інструментом для організацій будь-якого розміру. Публікація пропонує структурований підхід до управління ризиками, що включає в себе аналіз загроз, вразливостей, ймовірності реалізації ризиків та їх можливих наслідків. Завдяки цьому, організації можуть визначати і пріоритетизувати ризики на основі їхньої важливості та впливу на інформаційні системи.

Документ також підкреслює важливість безперервного процесу управління ризиками, який повинен включати регулярний моніторинг та оцінку

ризиків, а також адаптацію до змін у середовищі загроз і вимогах безпеки. У цьому контексті, NIST SP 800-30 рекомендує використання циклу управління ризиками, що складається з етапів підготовки, оцінки ризиків, реалізації заходів з управління ризиками та моніторингу результатів. Керівництво надає конкретні рекомендації щодо вибору та впровадження заходів безпеки, орієнтованих на зменшення ризиків до прийнятного рівня [6].

Важливою особливістю NIST SP 800-30 є його гнучкість та універсальність, що дозволяє застосовувати його до різних типів організацій та інформаційних систем, незалежно від їхнього розміру та складності. Публікація містить детальні описи та приклади, які допомагають організаціям у практичному впровадженні методів управління ризиками. Це включає рекомендації щодо документування процесів управління ризиками, оцінки ефективності впроваджених заходів та забезпечення відповідності нормативним вимогам. Таким чином, NIST SP 800-30 виступає важливим ресурсом для організацій, що прагнуть забезпечити високий рівень інформаційної безпеки та стійкість до ризиків у своїй діяльності. COBIT (Control Objectives for Information and Related Technologies) є фреймворком для управління та контролю інформаційних технологій (IT). Він забезпечує комплексний підхід до управління ризиками IT, включаючи ІБ. COBIT визначає цілі управління ризиками, контролю та управління IT-процесами, що допомагає організаціям досягати своїх бізнес-цілей і знижувати ризики.

Основні стандарти у сфері ризик-менеджменту, в т.ч. управління ризиками ІБ, зображені на рис. 1.2.

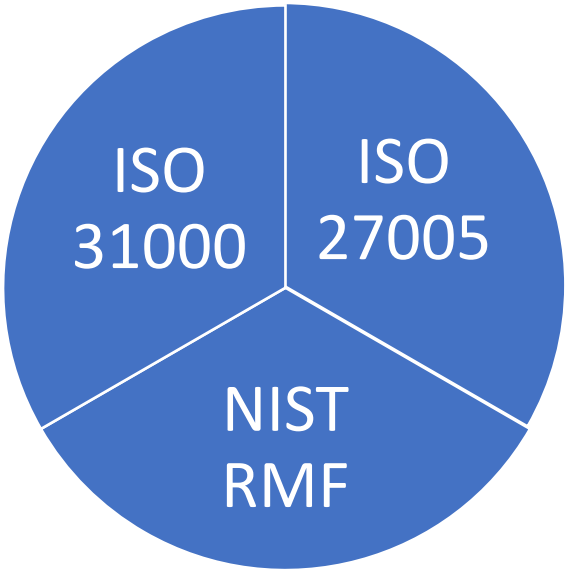

Рис. 1.2 Основні стандарти щодо управління ризиками

FAIR (Factor Analysis of Information Risk) є методологією оцінки ризиків, яка дозволяє кількісно оцінювати ризики інформаційної безпеки. Вона включає аналіз ймовірності та впливу загроз, що дозволяє організаціям приймати обґрунтовані рішення щодо управління ризиками. FAIR використовує статистичні моделі та аналіз сценаріїв для точного визначення рівнів ризику та розробки ефективних заходів захисту [7].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) є методологією оцінки ризиків, розробленою для організацій, які прагнуть покращити свою ІБ. Вона охоплює ідентифікацію важливих активів, вразливостей та загроз, а також розробку стратегій управління ризиками. OCTAVE фокусується на залученні ключових зацікавлених сторін до процесу оцінки ризиків, що забезпечує комплексний підхід до захисту інформаційних активів.

ISO/IEC 27005 є міжнародним стандартом, який надає керівництво щодо управління ризиками в рамках СУІБ, визначеної у стандарті ISO/IEC 27001. Він охоплює процеси ідентифікації, оцінки та обробки ризиків, а також моніторинг і перегляд заходів управління ризиками. Стандарт надає детальні інструкції для

організацій, спрямовані на виявлення та аналіз ризиків, з метою забезпечення конфіденційності, цілісності та доступності інформації. Важливість ISO/IEC 27005 полягає в його здатності допомогти організаціям створити ефективну структуру управління ризиками, яка відповідає їхнім специфічним потребам і умовам.

Процес управління ризиками, описаний у ISO/IEC 27005, починається з ідентифікації ризиків, де організації визначають потенційні загрози та вразливості, які можуть вплинути на їх інформаційні активи. Далі слідує оцінка ризиків, яка включає аналіз ймовірності виникнення ризиків та їх потенційних наслідків. Це дозволяє організаціям пріоритезувати ризики та приймати обґрунтовані рішення щодо заходів для їх зменшення. Обробка ризиків включає розробку та впровадження заходів контролю, спрямованих на мінімізацію ризиків до прийнятного рівня [8].

Моніторинг і перегляд є критичними етапами процесу управління ризиками за ISO/IEC 27005. Організації повинні регулярно перевіряти ефективність впроваджених заходів контролю та вносити необхідні корективи у відповідь на зміни у внутрішньому і зовнішньому середовищі. Це забезпечує безперервне покращення системи управління ризиками та адаптацію до нових викликів і загроз.

ISO/IEC 27005 також підкреслює важливість інтеграції управління ризиками в загальну стратегію управління ІБ організації. Це включає залучення керівництва та всіх рівнів персоналу до процесу управління ризиками, забезпечення належної підтримки та ресурсів для ефективного впровадження заходів безпеки. Завдяки цьому, організації можуть створити комплексний підхід до управління ризиками, який враховує всі аспекти їхньої діяльності та забезпечує надійний захист інформаційних активів.

Кожна з розглянутих методологій має свої сильні та слабкі сторони, і вибір конкретної методології залежить від потреб та ресурсів організації. Наприклад, ISO/IEC 27001 є універсальним стандартом, який підходить для організацій

будь-якого розміру та галузі, тоді як NIST SP 800-30 може бути більш корисним для державних установ та великих підприємств у США [9].

Методології оцінки ризиків, такі як FAIR і OCTAVE, надають гнучкі та деталізовані підходи до управління ризиками, що дозволяє організаціям точно оцінювати свої ризики та розробляти ефективні стратегії захисту. Методологія FAIR (Factor Analysis of Information Risk) орієнтована на кількісну оцінку ризиків, дозволяючи організаціям оцінювати ймовірність та потенційний вплив ризиків з використанням математичних моделей та статистичних даних. Це забезпечує точність і обґрунтованість у прийнятті рішень щодо управління ризиками. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), навпаки, пропонує більш якісний підхід, зосереджуючись на ідентифікації критичних активів, загроз та вразливостей, а також на розробці стратегій для їхнього захисту. Обидві методології враховують контекст і специфіку діяльності організації, її розмір, структуру та рівень зрілості в управлінні ІБ, що є важливим при виборі підходу до оцінки ризиків [10].

При застосуванні методології FAIR, організації можуть використовувати деталізовані сценарії та аналіз факторів ризику, що сприяє розумінню потенційних загроз і шляхів їхнього виникнення. Це дозволяє проводити глибокий аналіз ризиків, включаючи оцінку фінансових наслідків та розробку економічно обґрунтованих заходів безпеки. Методологія OCTAVE, в свою чергу, підкреслює важливість залучення співробітників організації до процесу оцінки ризиків, що сприяє виявленню прихованих загроз і розробці більш реалістичних і дієвих стратегій захисту. Вона також акцентує увагу на створенні культури безпеки всередині організації, що є критичним для ефективного управління ІБ.

Обидві методології підкреслюють необхідність постійного моніторингу та перегляду ризиків у світлі змін у внутрішньому та зовнішньому середовищі. Це дозволяє організаціям залишатися адаптивними та готовими до нових викликів у сфері ІБ. Вибір відповідної методології оцінки ризиків залежить від конкретних потреб і умов організації, проте обидві методології надають потужні інструменти для забезпечення всебічного та ефективного управління ризиками.

Впровадження стандартів та методологій управління ризиками ІБ є критичним кроком для забезпечення належного рівня безпеки. Організації повинні розробити детальний план впровадження, який включає оцінку поточного стану, визначення цілей та завдань, навчання персоналу, впровадження контролю та моніторинг результатів.

Ефективне впровадження стандартів та методологій дозволяє організаціям створити надійну систему управління ризиками, що підвищує їхню здатність протистояти сучасним кіберзагрозам. Крім того, відповідність міжнародним стандартам допомагає організаціям підвищити свою репутацію та забезпечити довіру з боку клієнтів і партнерів [11].

Аналіз стандартів та методологій управління ризиками ІБ є важливим етапом у забезпеченні надійного захисту інформаційних активів організації. Вибір відповідних стандартів та методологій, їхнє ефективне впровадження та постійне вдосконалення допомагають організаціям забезпечувати високий рівень безпеки в умовах постійно змінюваного кіберландшафту.

1.3 Впровадження стандартів ІБ у сфері критичної інфраструктури

Впровадження стандартів ІБ в секторах критичної інфраструктури є особливо важливим і складним завданням через високі вимоги до надійності та безпеки. Критична інфраструктура, така як енергетика, водопостачання, транспорт та здоров'я, вимагає особливого підходу до захисту інформації через можливі наслідки її компрометації. Ось основні аспекти, які слід враховувати при імплементації стандартів у цих сферах:

Підхід до ІБ у критичній інфраструктурі повинен бути інтегрованим і охоплювати як технічні, так і організаційні аспекти. Це включає створення спеціалізованих команд з безпеки, розробку комплексних планів реагування на інциденти, і впровадження систем моніторингу та виявлення загроз [12].

Спеціалізовані команди з безпеки: формування команд, які спеціалізуються на різних аспектах ІБ, включаючи ІТ-безпеку, фізичну безпеку

та реагування на інциденти. Це дозволяє мати експертів у кожній сфері та забезпечує всебічний захист.

Комплексні плани реагування на інциденти: розробка планів, які включають всі можливі сценарії загроз та відповідні дії для їх вирішення. Такі плани повинні бути гнучкими та легко адаптуватися до нових загроз.

Системи моніторингу та виявлення загроз є ключовим компонентом сучасних стратегій ІБ, які допомагають організаціям забезпечувати високий рівень захисту своїх інформаційних активів. Впровадження автоматизованих систем, що постійно здійснюють моніторинг мережі та виявляють підозрілу активність, дозволяє швидко реагувати на потенційні загрози, мінімізуючи ризики та збитки від кіберінцидентів [13].

Сучасні системи моніторингу та виявлення загроз, такі як системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), використовують передові технології штучного інтелекту (ШІ) та машинного навчання (ML) для аналізу мережевого трафіку та поведінкових даних у реальному часі. Ці системи здатні виявляти аномалії, які можуть свідчити про наявність кіберзагроз, таких як несанкціоновані спроби доступу, незвичні передачі даних або інші підозрілі дії.

Важливим аспектом роботи таких систем є їх здатність автоматично реагувати на виявлені загрози. Це може включати блокування шкідливого трафіку, ізоляцію скомпрометованих систем або обмеження доступу до критичних ресурсів. Така автоматизація дозволяє значно зменшити час реакції на інциденти, що є критичним у випадку швидко розповсюджуваних загроз, таких як віруси чи атаки типу "відмова в обслуговуванні" (DDoS) [14].

Крім того, системи моніторингу та виявлення загроз можуть бути інтегровані з іншими засобами безпеки, такими як системи управління інформацією та подіями безпеки (SIEM). Це забезпечує централізоване збирання та аналіз даних з різних джерел, створюючи цілісну картину стану ІБ організації. SIEM-системи дозволяють корелювати події, виявляти складні атаки та забезпечувати ефективне реагування на інциденти.

Впровадження автоматизованих систем моніторингу та виявлення загроз також потребує належної конфігурації та постійного вдосконалення. Це включає налаштування політик виявлення, оновлення сигнатур загроз, а також регулярне тестування та перевірку ефективності системи. Організації повинні забезпечити безперервний процес моніторингу та аналізу результатів роботи систем, а також швидке реагування на виявлені вразливості та інциденти.

Навчання та підвищення обізнаності персоналу щодо використання та управління такими системами є невід'ємною частиною процесу впровадження. Співробітники повинні бути навчені розпізнавати ознаки потенційних загроз та знати, як правильно реагувати на інциденти. Це сприяє створенню ефективної та оперативної команди реагування на інциденти, що здатна забезпечити високий рівень захисту інформаційних активів організації [15].

Таким чином, впровадження автоматизованих систем моніторингу та виявлення загроз є важливим кроком у забезпеченні ІБ. Ці системи надають можливість швидко та ефективно виявляти і реагувати на загрози, підвищуючи стійкість організації до кіберінцидентів та забезпечуючи захист критичних інформаційних ресурсів.

Організації, що входять до складу критичної інфраструктури, повинні проводити регулярні оцінки ризиків, які враховують специфіку їхньої діяльності. Це означає ідентифікацію потенційних внутрішніх і зовнішніх загроз та розробку стратегій для мінімізації цих ризиків.

Використання методик оцінки ризиків: використання методологій, таких як FAIR (Factor Analysis of Information Risk), дозволяє структуровано підходити до оцінки ризиків, враховуючи ймовірність і потенційний вплив загроз [16].

Регулярні оцінки та перегляд ризиків: регулярний перегляд та оновлення оцінок ризиків допомагає врахувати нові загрози та зміни в організаційному середовищі.

Важливо стандартизувати заходи безпеки в усіх аспектах критичної інфраструктури для забезпечення узгодженості та ефективності. Використання

міжнародних та національних стандартів, таких як ISO/IEC 27001 та ISO/IEC 27002, допомагає у цьому процесі.

Узгодженість процедур безпеки: стандартизація допомагає забезпечити, що всі процеси безпеки відповідають загальноприйнятим нормам і можуть бути легко інтегровані між різними підрозділами організації [17].

Постійне вдосконалення стандартів: регулярне оновлення стандартів відповідно до нових викликів і технологій забезпечує актуальність та ефективність заходів безпеки.

Оскільки людський фактор часто є слабкою ланкою в системі ІБ, навчання та підвищення обізнаності персоналу є критично важливими. Регулярні тренінги і симуляції допомагають підвищити готовність до виявлення та реагування на інформаційні загрози.

Проведення тренінгів та семінарів для підвищення обізнаності співробітників щодо актуальних загроз та методів їх виявлення [18].

Відпрацювання сценаріїв інцидентів для покращення практичних навичок реагування та координації дій.

Критична інфраструктура має залишатися на передовій технологічних інновацій, щоб адекватно реагувати на мінливий ландшафт загроз. Впровадження новітніх технологій захисту, таких як ML для аналізу безпеки, може значно покращити здатність організацій протистояти сучасним загрозам.

Використання технологій ШІ та ML для автоматизованого аналізу та виявлення загроз.

Використання блокчейн для забезпечення цілісності та прозорості даних.

Організації, які є частиною критичної інфраструктури, повинні також враховувати вимоги національного та міжнародного законодавства у сфері кібербезпеки, зокрема регулювання в області захисту даних і приватності.

Забезпечення відповідності законодавчим вимогам, таким як GDPR, для захисту даних і приватності.

Розробка та впровадження політик і процедур, що відповідають нормативним вимогам.

Ці елементи разом формують комплексний підхід до імплементації стандартів ІБ у критичній інфраструктурі, який допомагає забезпечити як оперативну стійкість, так і довгострокову безпеку інформації.

Управління ризиками ІБ в галузі критичної інфраструктури є ключовим аспектом забезпечення стійкості та надійності національних важливих систем. Основною метою цього процесу є ідентифікація, оцінка, мінімізація та контроль ризиків, які можуть негативно вплинути на інформаційні ресурси організації (рис. 1.3) [19].

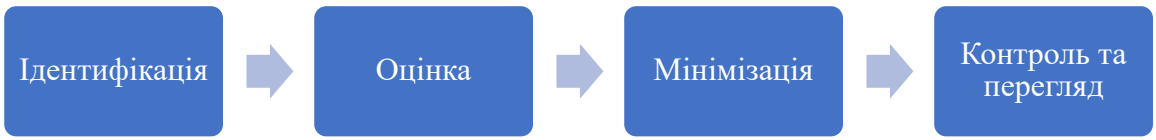

Рис. 1.3 Основні завдання процесу управління ризиками ІБ

Ідентифікація ризиків

Перший крок у стратегії управління ризиками полягає в ідентифікації потенційних загроз і вразливостей, які можуть вплинути на системи. Це може включати зовнішні загрози, такі як хакерські атаки та кіберзлочинність, а також внутрішні загрози, наприклад, ненавмисні помилки співробітників або неефективне управління доступом [20].

Оцінка ризиків

Після ідентифікації ризиків необхідно оцінити їх потенційний вплив та ймовірність виникнення. Це дозволяє організаціям визначити, які ризики є найбільш критичними і вимагають негайних заходів. Використання структурованих методологій оцінки, таких як FAIR (Factor Analysis of Information Risk), може допомогти у цьому процесі.

Мінімізація ризиків

Для мінімізації ризиків організації розробляють та впроваджують різноманітні заходи безпеки. Це може включати технологічні рішення, такі як

шифрування даних та багаторівнева система аутентифікації, а також організаційні заходи, наприклад, політики доступу та регулярне навчання персоналу.

Контроль та перегляд

Контроль за впровадженими заходами є життєво важливим для забезпечення їх ефективності. Організації повинні регулярно перевіряти і переглядати свої стратегії управління ризиками для адаптації до нових загроз або змін у операційному середовищі. Це також включає здійснення аудитів безпеки та використання зворотного зв'язку для постійного покращення [21].

Висновки до розділу 1

У першому розділі нашого дослідження ми розглянули важливість ризик-менеджменту у забезпеченні ІБ, провели аналіз міжнародних і національних стандартів та методологій управління ризиками, а також дослідили особливості імплементації цих стандартів у галузі критичної інфраструктури.

1.Визначення ролі ризик-менеджменту у забезпеченні ІБ. Ризик-менеджмент є фундаментальною складовою процесу захисту інформаційних активів організацій. Його роль полягає у систематичному підході до виявлення, оцінки, управління та моніторингу ризиків, що дозволяє мінімізувати їхній вплив на організацію.

Процес виявлення ризиків охоплює ідентифікацію зовнішніх та внутрішніх загроз, що можуть вплинути на організацію. Це включає аналіз потенційних сценаріїв розвитку подій та визначення вразливих місць.

Ефективне управління ризиками передбачає розробку стратегій для зниження ймовірності або впливу загроз, а також впровадження технічних, організаційних та фізичних заходів контролю. Наприклад, використання сучасного програмного забезпечення для моніторингу мережевої активності або впровадження багатофакторної аутентифікації.

Постійний моніторинг та перегляд ризиків дозволяє організаціям адаптуватися до нових загроз і забезпечувати актуальність заходів безпеки. Регулярні аудити та тестування на проникнення допомагають своєчасно виявляти та усувати вразливості.

2. Аналіз стандартів та методологій управління ризиками ІБ. Різні стандарти, такі як ISO/IEC 27001, NIST SP 800-30 та COBIT, надають організаціям керівництво для створення надійних систем управління ризиками. Ці стандарти охоплюють різні аспекти управління ризиками, від ідентифікації та оцінки до моніторингу та перегляду.

ISO/IEC 27001 забезпечує структуру для створення СУІБ, визначає вимоги до її впровадження та постійного вдосконалення. Впровадження цього стандарту допомагає організаціям захищати свої інформаційні активи та забезпечувати їхню конфіденційність, цілісність та доступність.

NIST SP 800-30 пропонує детальний підхід до оцінки ризиків, що включає ідентифікацію загроз, аналіз вразливостей та оцінку потенційних наслідків. Цей стандарт є корисним інструментом для організацій будь-якого розміру, оскільки надає практичні рекомендації щодо управління ризиками.

COBIT фокусується на управлінні та контролі IT та допомагає організаціям досягати своїх бізнес-цілей, знижуючи ризики, пов'язані з IT.

Методи оцінки ризиків, такі як FAIR та OCTAVE, забезпечують гнучкі та деталізовані підходи до управління ризиками, дозволяючи організаціям точно оцінювати свої ризики та розробляти ефективні стратегії захисту.

FAIR дозволяє кількісно оцінювати ризики, використовуючи статистичні моделі та аналіз сценаріїв для точного визначення рівнів ризику та розробки ефективних заходів захисту.

OCTAVE охоплює ідентифікацію важливих активів, вразливостей та загроз, а також розробку стратегій управління ризиками, що забезпечує комплексний підхід до захисту інформаційних активів.

Вибір відповідних стандартів та методологій залежить від потреб та ресурсів організації, її розміру та специфіки діяльності. Важливо враховувати, як

кожен стандарт або методологія може бути адаптована до конкретних умов та вимог організації.

3. Імплементація стандартів ІБ у галузі критичної інфраструктури. Впровадження стандартів ІБ в секторах критичної інфраструктури є особливо важливим і складним завданням через високі вимоги до надійності та безпеки. Критична інфраструктура включає такі сектори, як енергетика, водопостачання, транспорт та охорона здоров'я, де можливі наслідки компрометації можуть бути катастрофічними.

Підхід до ІБ у критичній інфраструктурі повинен бути інтегрованим і охоплювати як технічні, так і організаційні аспекти, включаючи створення спеціалізованих команд з безпеки, розробку комплексних планів реагування на інциденти, і впровадження систем моніторингу та виявлення загроз. Це забезпечує швидку реакцію на загрози та мінімізацію їхніх наслідків.

Організації повинні проводити регулярні оцінки ризиків, які враховують специфіку їхньої діяльності, та стандартизувати заходи безпеки в усіх аспектах критичної інфраструктури для забезпечення узгодженості та ефективності. Це включає використання передових технологій, таких як ШІ та ML для виявлення аномалій та загроз.

У цілому, розділ 1 підкреслив важливість систематичного підходу до управління ризиками ІБ, який включає визначення ролі ризик-менеджменту, аналіз стандартів та методологій, а також ефективну імплементацію стандартів у критичній інфраструктурі. Це дозволяє організаціям створювати надійні системи захисту, адаптуватися до нових загроз і забезпечувати безперервну роботу в умовах постійно змінюваного кіберландшафту. Завдяки такому підходу, організації можуть забезпечити стабільність та безпеку своїх інформаційних активів, підтримуючи довіру з боку клієнтів та партнерів, а також відповідність нормативним вимогам у галузі ІБ.

Розділ 2 ДОСЛІДЖЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІБ В ГАЛУЗІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Дослідження процесу інтеграції управління ризиками ІБ в систему управління бізнес-ризиками

Інтеграція управління ризиками ІБ в загальну систему управління бізнес-ризиками є ключовим аспектом для забезпечення всебічного захисту організації. Це дозволяє ефективніше виявляти, оцінювати та управляти ризиками, що можуть впливати на бізнес-процеси, репутацію та фінансовий стан компанії.

Інтеграція управління ризиками ІБ з бізнес-ризиками дозволяє організаціям забезпечувати комплексний підхід до захисту активів. Це включає координацію дій між різними підрозділами, що сприяє більш ефективному управлінню ризиками. Такий підхід дозволяє зменшити дублювання зусиль та підвищити загальну ефективність системи управління ризиками [22].

Ключові етапи інтеграції:

1. Аналіз поточного стану: Першим кроком є оцінка існуючих підходів до управління бізнес-ризиками та ІБ. Це включає виявлення основних ризиків, з якими стикається організація, та аналіз поточних методик управління цими ризиками.

2. Визначення взаємозв'язків між бізнес-ризиками та ризиками ІБ: Важливо зрозуміти, як ризики ІБ можуть впливати на загальні бізнес-ризики, і навпаки. Це дозволяє визначити, які аспекти ІБ є критичними для успішної роботи бізнесу.

3. Розробка інтегрованої стратегії управління ризиками: На основі отриманих даних розробляється стратегія, що включає як управління бізнес-ризиками, так і ризиками ІБ. Ця стратегія повинна враховувати специфіку організації та її бізнес-процеси.

4. Впровадження інтегрованої системи управління ризиками: Наступним етапом є впровадження розробленої стратегії. Це включає навчання персоналу,

оновлення політик і процедур, а також впровадження нових технологічних рішень для моніторингу та управління ризиками.

5. Моніторинг та перегляд: Постійний моніторинг інтегрованої системи управління ризиками дозволяє вчасно виявляти нові загрози та адаптувати стратегії управління відповідно до змін у середовищі. Регулярні аудити та аналіз ефективності дозволяють забезпечити актуальність заходів безпеки.

Інтеграція управління ризиками ІБ в загальну систему управління бізнес-ризиками може стикатися з низкою викликів:

- організаційні бар'єри: різні підрозділи можуть мати власні підходи до управління ризиками, що ускладнює координацію зусиль.
- відсутність узгодженості: недостатня узгодженість між бізнес-цілями та цілями ІБ може призвести до неефективного управління ризиками.
- обмежені ресурси: недостатність ресурсів (фінансових, технологічних, людських) може ускладнювати впровадження інтегрованої системи управління ризиками.

Незважаючи на виклики, інтеграція управління ризиками ІБ в систему управління бізнес-ризиками надає значні переваги:

- загальна підвищена ефективність: координація зусиль між підрозділами підвищує ефективність управління ризиками.
- зниження витрат: спільне управління ризиками дозволяє зменшити витрати, пов'язані з дублюванням зусиль та неефективним управлінням.
- підвищення стійкості організації: інтегрований підхід забезпечує більш всебічний захист організації від різних загроз, що підвищує її стійкість до кризових ситуацій [23].

Таким чином, інтеграція управління ризиками ІБ в загальну систему управління бізнес-ризиками є важливим кроком для підвищення ефективності та стійкості організацій у сучасних умовах. Вона забезпечує комплексний підхід до захисту активів, зменшує дублювання зусиль і витрат, а також підвищує загальний рівень безпеки та стабільності бізнесу

2.2 Аналіз методів оцінки ризиків ІБ

Управління ризиками не може бути ефективним без детальної оцінки ризиків. Ця оцінка дозволяє організаціям розуміти потенційні загрози та їх вплив на операції. Для критичної інфраструктури, де відмова або компрометація систем може призвести до серйозних наслідків, точна оцінка ризиків є особливо важливою [24].

Оцінка ризиків може проводитися двома основними методами: якісним та кількісним. Якісний аналіз фокусується на ідентифікації ризиків та оцінці їх відносної серйозності та ймовірності без використання числових значень. Цей метод часто використовується для отримання загального розуміння ризикованого ландшафту та для визначення пріоритетів заходів безпеки. Якісний аналіз зазвичай включає експертні оцінки, опитування та інтерв'ю з ключовими стейкхолдерами для визначення ймовірних загроз, вразливостей та потенційного впливу на організацію.

У рамках якісного аналізу ризики класифікуються за категоріями, такими як високий, середній та низький, що дозволяє організаціям швидко ідентифікувати найбільш критичні ризики та зосередити свої зусилля на їх мінімізації. Методики, такі як SWOT-аналіз (аналіз сильних і слабких сторін, можливостей та загроз) та метод матриці ризиків, часто використовуються для проведення якісної оцінки. Перевагою цього методу є його простота та швидкість, а також можливість включення думок і досвіду різних експертів, що забезпечує всебічне розуміння ризиків [25].

На відміну від якісного, кількісний аналіз ризиків базується на використанні числових значень для оцінки ймовірності та потенційного впливу ризиків. Цей метод використовує статистичні дані, історичні інциденти та моделі для визначення ймовірних сценаріїв і вимірювання ризиків у фінансових або інших числових термінах. Кількісний аналіз дозволяє організаціям більш точно оцінювати ризики та приймати обґрунтовані рішення щодо впровадження заходів безпеки.

Для проведення кількісного аналізу використовуються різноманітні методи, такі як аналіз ймовірностей, аналіз впливу, моделювання Монте-Карло та аналіз вартості і вигоди. Ці методи дозволяють визначити, який фінансовий вплив може мати реалізація певного ризику, і скільки буде коштувати впровадження заходів для його мінімізації. Кількісний аналіз є більш точним та детальним, але він також може бути більш складним і затратним за часом, вимагаючи збору та аналізу великого обсягу даних [26].

Обидва методи оцінки ризиків мають свої переваги та недоліки, і часто використовуються в комбінації для забезпечення найбільш повного і точного розуміння ризикового ландшафту. Якісний аналіз забезпечує швидкий і загальний огляд ризиків, дозволяючи організаціям визначати пріоритетні напрямки для подальшого, більш детального дослідження за допомогою кількісних методів. У свою чергу, кількісний аналіз надає точні дані, необхідні для прийняття обґрунтованих рішень щодо інвестицій у заходи безпеки та управління ризиками. Таким чином, інтеграція якісного та кількісного аналізу забезпечує всебічний підхід до управління ризиками, підвищуючи ефективність захисту інформаційних активів організації [27].

Один із популярних методів кількісного аналізу – це аналіз дерева відмов (Fault Tree Analysis, FTA), який дозволяє аналізувати шляхи, якими можуть відбутися системні відмови. Цей метод допомагає візуалізувати різні шляхи, що можуть призвести до збоїв у системі, та визначити найбільш вразливі точки.

Ще один метод – аналіз впливу на бізнес (Business Impact Analysis, BIA), який визначає потенційні наслідки втрати функціональності та ефективності критичних систем. BIA допомагає організаціям зрозуміти, як різні загрози можуть вплинути на їхню операційну діяльність та фінансові результати, що дозволяє більш точно планувати заходи з мінімізації ризиків [28].

Класифікація методів аналізу ризиків представлена на рис. 2.1.

Рис. 2.1. Методи аналізу ризику

Сучасні технології дозволяють автоматизувати багато аспектів оцінки ризиків. ПЗ для управління ризиками може інтегрувати дані з різних джерел, включно з внутрішніми аудитами та зовнішніми інтелектуальними джерелами, для створення детальної картини загроз. Це ПЗ також може допомогати у визначенні ефективності існуючих заходів безпеки та рекомендувати покращення.

Програмні інструменти можуть автоматично аналізувати великі обсяги даних, виявляти тенденції та аномалії, які можуть свідчити про потенційні загрози. Вони також можуть генерувати звіти та рекомендації для управління ризиками, що дозволяє керівникам приймати більш обґрунтовані рішення [29].

Не можна недооцінювати значення кваліфікованого персоналу у процесі оцінки ризиків. Регулярні тренінги та семінари допомагають підвищити обізнаність співробітників щодо поточних кіберзагроз та методів їх виявлення та мінімізації. Освіта та постійне навчання є ключовими для підтримки культури безпеки в організації.

Персонал, який має достатні знання та навички, може більш ефективно виявляти потенційні загрози та швидко реагувати на інциденти безпеки. Це включає не лише технічне навчання, але й розвиток навичок критичного мислення та прийняття рішень у стресових ситуаціях.

Цей комплексний підхід до оцінки ризиків забезпечує, що критична інфраструктура залишається захищеною від сучасних і майбутніх загроз, і що організація може швидко адаптуватися до змін у кіберзагрозах. Він включає поєднання кількісних та якісних методів оцінки, використання сучасних технологій та програмного забезпечення, а також постійне навчання та розвиток персоналу.

Завдяки такому підходу, організації можуть не лише виявляти та оцінювати ризики, але й ефективно управляти ними, забезпечуючи безперервність операцій та захист інформаційних активів. Це допомагає створити надійну систему управління ризиками, яка підтримує загальну стійкість і безпеку критичної інфраструктури.

2.3 Визначення доцільних стратегій обробки ризиків ІБ

Ефективне управління ризиками ІБ включає розробку та впровадження стратегій обробки ризиків, які допомагають мінімізувати їхній вплив на організацію. У цьому розділі ми розглянемо різні стратегії обробки ризиків ІБ, їхні переваги та недоліки, а також рекомендації щодо їхнього впровадження в організаціях [30].

Далі в розділі проаналізовано основні стратегії обробки ризиків (рис. 2.2).

1. Уникнення ризиків передбачає відмову від діяльності або процесів, які пов'язані з високими ризиками. Це може включати зміну бізнес-процесів, технологій або систем для зменшення ризиків.

Переваги: Повне усунення ризику.

Недоліки: Може призвести до втрати бізнес-можливостей або зниження ефективності операцій.

2. Модифікація ризиків передбачає впровадження заходів для зменшення ймовірності або впливу загроз. Це може включати технічні заходи, такі як встановлення фаєрволів або шифрування даних, а також організаційні заходи, такі як навчання персоналу.

Переваги: Зниження ймовірності виникнення інцидентів та їхнього впливу.

Недоліки: Вимагає постійного моніторингу та оновлення заходів безпеки.

3. Передача ризиків передбачає передачу відповідальності за ризики третім особам, наприклад, через страхування або аутсорсинг. Це дозволяє організації зменшити фінансовий вплив ризиків.

Переваги: Зниження фінансових ризиків.

Недоліки: Не усуває ризик повністю і може бути дорогим.

4. Прийняття ризиків передбачає свідоме визнання та прийняття ризиків, якщо їхній вплив є допустимим для організації. Це може бути доцільно, якщо витрати на зниження або уникнення ризику перевищують потенційні втрати.

Переваги: Економія ресурсів.

Недоліки: Ризик залишається, і організація повинна бути готовою до його реалізації.

Рис. 2.2. Стратегії обробки ризиків

Вибір доцільних стратегій обробки ризиків залежить від ряду факторів, включаючи такі:

- критичність активів: чим важливіший актив, тим більше зусиль слід приділяти його захисту;

- ймовірність та вплив ризиків: важливо оцінити ймовірність виникнення ризику та його потенційний вплив на організацію;
- ресурси організації: вибір стратегії залежить від доступних фінансових, технологічних та людських ресурсів;
- вимоги законодавства та стандартів: важливо враховувати нормативні вимоги, що можуть впливати на вибір стратегії обробки ризиків.

На основі аналізу потенційних стратегій обробки ризиків можна розробити конкретні рекомендації для їхнього впровадження в організаціях:

- розробка плану впровадження: включає визначення відповідальних осіб, етапів впровадження та необхідних ресурсів [31].
- навчання та підвищення обізнаності персоналу: регулярні тренінги та семінари допомагають підвищити рівень обізнаності співробітників щодо питань кібербезпеки та ефективно впроваджувати обрані стратегії.
- моніторинг та перегляд: постійний моніторинг ефективності впроваджених стратегій та їхній регулярний перегляд дозволяють адаптуватися до нових загроз та змін у середовищі.

Ефективне впровадження стратегій обробки ризиків допомагає організаціям мінімізувати вплив загроз на їхню діяльність, забезпечити безпеку інформаційних активів та підвищити стійкість до кіберзагроз. Це є важливою складовою загальної стратегії управління ризиками ІБ, що дозволяє організаціям ефективно функціонувати в умовах постійно змінюваного кіберландшафту [32].

Висновки до розділу 2

У другому розділі дослідження було розглянуто різні аспекти управління ризиками ІБ в галузі критичної інфраструктури. Це включало дослідження процесу інтеграції управління ризиками ІБ в систему управління бізнес-ризиками, аналіз сучасних методик оцінки ризиків ІБ та визначення доцільних стратегій обробки ризиків.

Дослідження процесу інтеграції управління ризиками ІБ в систему управління бізнес-ризиками. Інтеграція управління ризиками ІБ з загальною системою управління бізнес-ризиками є критично важливою для забезпечення комплексного підходу до захисту організації. Такий підхід дозволяє координацію дій між різними підрозділами, що підвищує ефективність управління ризиками та зменшує дублювання зусиль. Основні етапи інтеграції включають аналіз поточного стану, визначення взаємозв'язків між бізнес-ризиками та ризиками ІБ, розробку інтегрованої стратегії, впровадження системи та постійний моніторинг. Впровадження інтегрованої системи управління ризиками дозволяє організаціям підвищити стійкість до кризових ситуацій та забезпечити захист критичних бізнес-процесів.

Далі в розділі наведено аналіз сучасних методик оцінки ризиків ІБ. Сучасні методики оцінки ризиків ІБ включають як кількісний, так і якісний аналіз. Кількісний аналіз дозволяє точно вимірювати ризики та приймати обґрунтовані рішення щодо розподілу ресурсів, тоді як якісний аналіз забезпечує загальне розуміння ризикового ландшафту та допомагає визначити пріоритети для впровадження заходів безпеки.

Використання сучасних аналітичних інструментів, таких як ML та ШІ, дозволяє автоматизувати процес оцінки ризиків, підвищуючи його точність та ефективність. Це включає інструменти розширеної аналітики, які дозволяють швидко виявляти аномалії та тренди, що можуть бути ознаками безпекових інцидентів.

Комбінація кількісних та якісних методик забезпечує всебічне розуміння ризикового ландшафту та допомагає організаціям розробляти ефективні стратегії управління ризиками.

Визначення доцільних стратегій обробки ризиків ІБ. Ефективне управління ризиками ІБ включає розробку та впровадження стратегій обробки ризиків, які допомагають мінімізувати їхній вплив на організацію. Основні стратегії включають уникнення, зниження, перенесення та прийняття ризиків.

Вибір доцільних стратегій залежить від критичності активів, ймовірності та впливу ризиків, ресурсів організації та вимог законодавства. Наприклад, уникнення ризиків може бути доцільним для критичних активів, тоді як перенесення ризиків може бути корисним для зниження фінансових втрат.

Рекомендації щодо впровадження стратегій обробки ризиків включають розробку плану впровадження, навчання персоналу, постійний моніторинг та регулярний перегляд ефективності стратегій.

Другий розділ підкреслив важливість інтегрованого підходу до управління ризиками ІБ, що дозволяє організаціям ефективно захищати свої інформаційні активи та забезпечувати стійкість до кіберзагроз. Використання сучасних методик оцінки ризиків, впровадження інноваційних технологій та розробка ефективних стратегій обробки ризиків є ключовими елементами успішної стратегії управління ризиками.

Цей комплексний підхід допомагає організаціям адаптуватися до постійно змінюваного кіберландшафту, забезпечуючи надійний захист критичних систем та даних. Розробка та впровадження інтегрованих стратегій управління ризиками ІБ є важливим кроком для забезпечення стабільності та безпеки організацій у сучасному цифровому світі.

Розділ 3 ВДОСКОНАЛЕННЯ СТРАТЕГІЙ УПРАВЛІННЯ РИЗИКАМИ ІБ

3.1 Оцінка ефективності поточних стратегій управління ризиками ІБ

Оцінка ефективності поточних стратегій управління ризиками ІБ є ключовим етапом у розробці рекомендацій щодо їх вдосконалення. Цей процес включає аналіз сильних та слабких сторін існуючих підходів, виявлення прогалин і визначення областей, які потребують покращення.

Першим кроком є комплексна ревізія існуючих політик, процедур та інструментів управління ризиками. Важливо визначити, наскільки добре поточні методики відповідають сучасним вимогам ІБ та чи здатні вони ефективно реагувати на змінювані кіберзагрози. Для цього можна використовувати такі показники:

- повнота охоплення ризиків: чи враховуються всі критичні активи та потенційні вектори атак? Важливо перевірити, чи охоплюють поточні методики всі можливі сценарії загроз, включаючи фізичні та кіберзагрози [33];
- актуальність методик: чи оновлюються політики і процедури відповідно до останніх тенденцій в кібербезпеці? Важливо враховувати, як часто переглядаються та оновлюються політики та процедури, і чи включають вони останні рекомендації від провідних організацій у сфері кібербезпеки;
- ефективність процедур оцінки ризиків: наскільки ефективно організація може ідентифікувати, оцінити та впоратися з ризиками? Це включає аналіз використання методологій оцінки ризиків, таких як ISO 31000 або NIST SP 800-30.;
- чи використовуються інструменти для автоматизації процесу оцінки ризиків, такі як програми для управління ризиками, і як добре вони інтегровані з іншими системами безпеки.

Після аналізу існуючих стратегій важливо ідентифікувати слабкі місця у системах ІБ. Це можуть бути технічні недоліки, такі як застаріле ПЗ, недостатньо

захищені мережі, або організаційні прогалини, наприклад, недостатнє навчання персоналу або відсутність чітких процедур у випадку інцидентів:

- технічні недоліки, наприклад, застаріле обладнання або ПЗ, яке не підтримується виробником, може бути вразливим до атак. Виявлення таких недоліків дозволяє організаціям планувати оновлення та модернізацію своїх систем;
- організаційні прогалини включають недостатнє навчання персоналу щодо новітніх загроз та методів їх запобігання, а також відсутність чітких інструкцій та політик для реагування на інциденти.

Також критично важливо перевірити, наскільки поточні стратегії відповідають національним та міжнародним стандартам ІБ, таким як ISO/IEC 27001, NIST, або GDPR для захисту даних. Відповідність цим стандартам не тільки забезпечує більшу безпеку, але й допомагає зберігати довіру клієнтів та партнерів [34].

Міжнародні стандарти, наприклад, ISO/IEC 27001 вимагає регулярного аудиту системи управління ІБ, що допомагає виявляти недоліки та впроваджувати покращення. В Україні стандарти ІБ також включають ДСТУ ISO/IEC 27001, який адаптований до національних особливостей. Важливо перевірити відповідність цим стандартам для забезпечення законності та відповідності місцевим нормативним вимогам.

На основі проведеної оцінки можна розробити конкретні рекомендації для покращення. Це можуть бути технічні удосконалення, як-от впровадження більш сучасних захисних технологій, оновлення застарілого обладнання або впровадження більш строгих процедур аутентифікації.

Технічні удосконалення включають впровадження сучасних технологій, таких як багатофакторна аутентифікація, шифрування даних та системи виявлення вторгнень [35].

Організаційні заходи передбачають здебільшого підвищення рівня обізнаності співробітників щодо питань кібербезпеки через регулярні тренінги

та семінари, розробку чітких реагувань на інциденти та зміцнення політики внутрішнього контролю.

3.2 Особливості впровадження сучасних технологічних рішень для управління ризиками ІБ

Сучасні технологічні рішення відіграють ключову роль у підвищенні ефективності управління ризиками ІБ. Використання інноваційних технологій, таких як ШІ та ML, блокчейн і розширені аналітичні інструменти, може значно покращити здатність організацій виявляти та реагувати на загрози.

ШІ та ML можуть революціонізувати спосіб, яким організації виявляють та реагують на кіберзагрози. Використання цих технологій дозволяє системам ІБ автоматично аналізувати великі обсяги даних для виявлення аномалій, що можуть вказувати на кібератаки. Завдяки ШІ та ML, системи можуть навчатися на основі історичних даних та виявляти шаблони, що можуть бути ознаками потенційних загроз. Це суттєво підвищує швидкість і точність виявлення загроз, знижуючи навантаження на людські ресурси та мінімізуючи ймовірність пропуску критичних інцидентів [36].

Один з ключових аспектів застосування ШІ та ML в ІБ – це можливість моніторингу та аналізу трафіку мережі в реальному часі, логів і поведінкових даних користувачів. Алгоритми ML можуть автоматично ідентифікувати аномалії, такі як незвичні спроби доступу, зміни в шаблонах поведінки користувачів або аномальні передачі даних, які можуть свідчити про спробу кібератаки. Це дозволяє своєчасно реагувати на загрози, запобігаючи їх розвитку до масштабних інцидентів.

Крім того, ШІ та ML можуть бути використані для автоматизації реагування на інциденти. Наприклад, системи можуть автоматично вживати заходів для ізоляції підозрілих активностей, блокування шкідливих IP-адрес або обмеження доступу до вразливих систем, що значно зменшує час реакції та обмежує потенційні збитки. Впровадження таких технологій також дозволяє

створювати проактивні системи захисту, які здатні прогнозувати можливі загрози на основі аналізу трендів і поведінкових моделей [37].

Інтеграція ШІ та ML у системи ІБ також сприяє підвищенню ефективності процесу управління інцидентами та ризиками. Ці технології можуть автоматизувати рутинні завдання, такі як класифікація інцидентів, аналіз журналів подій і створення звітів, що дозволяє фахівцям зосередитися на більш складних і стратегічних аспектах безпеки.

Загалом, застосування ШІ та ML в ІБ відкриває нові можливості для організацій у боротьбі з кіберзагрозами, забезпечуючи більш ефективний, швидкий і проактивний підхід до захисту інформаційних активів. Ці технології допомагають створити адаптивні системи, здатні до постійного навчання та вдосконалення, що є критично важливим в умовах швидкого розвитку кіберзагроз:

- аналіз даних: ШІ та ML можуть автоматично аналізувати потоки даних та виявляти аномалії, які можуть бути ознаками кібератаки. Це дозволяє швидше реагувати на загрози та зменшити залежність від людського фактору [38];
- прогнозування загроз: технології ML можуть використовувати історичні дані для прогнозування можливих загроз та розробки заходів для їх запобігання.
- технологія блокчейн забезпечує високий рівень безпеки для транзакцій та даних завдяки своїй децентралізованій та незмінній природі. Вона може бути використана для забезпечення цілісності та прозорості в обробці даних, що важливо для критичних інфраструктур.
- цілісність даних: блокчейн забезпечує незмінність записів, що гарантує цілісність даних. Це особливо важливо для забезпечення довіри до даних та збереження їхньої історії.
- безпека транзакцій: Використання блокчейн для управління ланцюгами постачання, зберігання даних та забезпечення безпеки електронних трансакцій.

Сучасні аналітичні інструменти дозволяють організаціям швидко ідентифікувати тенденції та шаблони, що можуть бути ознаками безпекових інцидентів. Це включає використання великих даних (Big Data) та інструментів візуалізації для аналізу та представлення інформації у зручному форматі:

- візуалізація даних: інструменти візуалізації дозволяють представити складні дані у зрозумілому форматі, що полегшує прийняття рішень на основі аналітичних результатів.
- моделювання сценаріїв: використання передових алгоритмів для моделювання можливих сценаріїв та прогнозування наслідків різних типів атак.

Впровадження сучасних технологій вимагає розробки плану дій, який включає етапи впровадження, навчання персоналу та оцінку ефективності нових рішень [39].

Важливо почати з пілотних проектів для оцінки ефективності нових технологій у реальних умовах перед їх повномасштабним впровадженням. Слід забезпечити навчання персоналу для роботи з новими інструментами та технологіями. Також варто проводити постійний моніторинг та оцінку ефективності впроваджених технологій для забезпечення їхньої відповідності потребам організації.

3.3 Розробка рекомендацій щодо вдосконалення стратегій управління ризиками ІБ

Удосконалення стратегій управління ризиками ІБ є критично важливим для забезпечення стійкості та захисту організацій від кіберзагроз. У цьому розділі детально розглянуто розробку рекомендацій для вдосконалення цих стратегій, враховуючи аналіз існуючих методик, впровадження сучасних технологічних рішень та підвищення обізнаності персоналу [40].

Перш за все, важливо здійснити ретельний аналіз існуючих методик управління ризиками. Це включає оцінку поточних процесів ідентифікації,

оцінки та обробки ризиків, що застосовуються в організації. Застосування міжнародних стандартів, таких як ISO/IEC 27005 та NIST SP 800-30, може стати основою для формування ефективних стратегій. Оцінка вразливостей, загроз та потенційного впливу ризиків на бізнес-процеси дозволить визначити пріоритетні напрями для вдосконалення. Організації також можуть скористатися методологіями FAIR і OCTAVE для більш детального та гнучкого підходу до аналізу ризиків.

Впровадження сучасних технологічних рішень є ще одним важливим аспектом удосконалення стратегій управління ризиками. Використання ШІ та ML дозволяє автоматизувати процеси моніторингу та виявлення аномалій. Ці технології здатні аналізувати великі обсяги даних у реальному часі, виявляти незвичні патерни та потенційні загрози, що значно підвищує швидкість і точність реагування. Використання таких інструментів, як системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), інтегрованих з ШІ та ML, може значно посилити захист ІС [41].

Не менш важливим є підвищення обізнаності персоналу щодо питань ІБ. Навчання співробітників має бути регулярним і включати як базові знання про кіберзагрози, так і спеціалізовані тренінги з реагування на інциденти. Проведення симуляцій та практичних вправ допомагає персоналу бути готовими до реальних загроз і діяти ефективно у критичних ситуаціях. Важливо також формувати культуру безпеки, де кожен співробітник розуміє свою роль у забезпеченні захисту інформаційних активів.

Розробка рекомендацій для вдосконалення стратегій управління ризиками ІБ повинна також включати постійний моніторинг та перегляд впроваджених заходів. Регулярні аудити, оцінка ефективності заходів безпеки та оновлення стратегій відповідно до нових загроз і технологій є невід'ємними елементами цього процесу. Організації повинні бути готовими адаптувати свої стратегії у відповідь на зміни у зовнішньому та внутрішньому середовищі.

Вдосконалення стратегій управління ризиками ІБ вимагає комплексного підходу, що включає аналіз існуючих методик, впровадження сучасних

технологій та підвищення обізнаності персоналу. Лише інтегруючи ці компоненти, організації можуть забезпечити надійний захист своїх інформаційних активів та підвищити свою стійкість до кіберзагроз.

Першим кроком у процесі вдосконалення стратегій є оцінка поточного стану системи управління ризиками ІБ. Це включає детальний аналіз існуючих політик, процедур та інструментів, які використовуються для ідентифікації, оцінки та управління ризиками [42].

Аудит існуючих політик та процедур. Регулярні аудити допомагають виявити слабкі місця та недоліки в поточних підходах до управління ризиками. Важливо переглянути всі наявні документи, включаючи політики безпеки, плани реагування на інциденти та процедури оцінки ризиків.

Аналіз використання технологій. Вивчення того, які технології використовуються для управління ризиками, їх ефективність та можливість модернізації. Наприклад, чи використовуються сучасні аналітичні інструменти для моніторингу загроз і чи є необхідність у впровадженні нових технологій, таких як ШІ або ML.

На основі результатів оцінки необхідно розробити нові або вдосконалити існуючі політики та процедури, щоб вони відповідали сучасним вимогам та загрозам.

Політики повинні враховувати новітні кіберзагрози та технологічні інновації. Регулярне оновлення політик забезпечує їхню актуальність та відповідність сучасним вимогам ІБ.

Важливо мати детальні плани реагування на різні типи інцидентів, включаючи визначення відповідальних осіб, необхідні ресурси та кроки для усунення загроз. Ці процедури повинні бути чітко документовані та регулярно перевірятися через тренування та симуляції [43].

Сучасні технології відіграють ключову роль у підвищенні ефективності управління ризиками ІБ. Важливо інтегрувати новітні технологічні рішення, які можуть значно покращити здатність організацій виявляти та реагувати на загрози:

- використання ШІ та ML дозволяє системам ІБ автоматично аналізувати великі обсяги даних для виявлення аномалій, що можуть вказувати на кібератаки. Ці технології можуть навчатися на основі історичних даних та постійно покращувати свої алгоритми виявлення загроз.
- технологія блокчейн забезпечує високий рівень безпеки для трансакцій та даних завдяки своїй децентралізованій та незмінній природі. Вона може бути використана для забезпечення цілісності та прозорості в обробці даних, що важливо для критичних інфраструктур [44].
- розширена аналітика та великі дані (Big Data): сучасні аналітичні інструменти дозволяють організаціям швидко ідентифікувати тенденції та шаблони, що можуть бути ознаками безпекових інцидентів. Це включає використання інструментів візуалізації для представлення даних у зручному форматі, що полегшує прийняття рішень на основі аналітичних результатів.

Не можна недооцінювати значення кваліфікованого персоналу у процесі управління ризиками ІБ. Регулярні тренінги та підвищення обізнаності співробітників є критично важливими для забезпечення ефективності нових стратегій:

- проведення регулярних тренінгів та семінарів допомагає підвищити рівень обізнаності співробітників щодо новітніх загроз та методів їх запобігання. Це включає навчання з використання нових інструментів та технологій, а також практичні вправи для відпрацювання процедур реагування на інциденти;
- сертифікація: заохочення співробітників до отримання сертифікацій у сфері кібербезпеки, таких як CISSP, CISM, CEH, допомагає підвищити їхню кваліфікацію та знання. Сертифікація також сприяє підвищенню мотивації та професійного розвитку персоналу;
- культура безпеки: створення культури безпеки в організації, де кожен співробітник розуміє свою роль у забезпеченні ІБ. Це включає регулярні комунікації про важливість безпеки, відзначення успіхів у сфері кібербезпеки та активне залучення всіх співробітників до заходів з безпеки.

Постійний моніторинг та перегляд ефективності впроваджених стратегій дозволяють організаціям адаптуватися до нових загроз і забезпечувати актуальність заходів безпеки:

- регулярні аудити: проведення регулярних аудитів для оцінки ефективності політик та процедур. Це включає внутрішні та зовнішні аудити для виявлення недоліків та визначення шляхів їх усунення [45];
- аналіз інцидентів: після кожного інциденту важливо проводити детальний аналіз, щоб визначити, що сталося, як інцидент був виявлений, які заходи були вжиті та як можна покращити процес реагування в майбутньому;
- відгуки та зворотний зв'язок: регулярне отримання зворотного зв'язку від співробітників щодо ефективності впроваджених заходів безпеки та процедур. Це дозволяє вчасно виявляти проблеми та впроваджувати необхідні зміни.

Розробка рекомендацій щодо вдосконалення стратегій управління ризиками ІБ вимагає систематичного підходу, що включає оцінку поточного стану, розробку нових політик та процедур, впровадження сучасних технологій, навчання персоналу та постійний моніторинг. Цей комплексний підхід допомагає організаціям ефективно протистояти сучасним кіберзагрозам, забезпечуючи надійний захист своїх інформаційних активів. Виконання цих рекомендацій сприяє підвищенню стійкості організацій до кіберзагроз та підтриманню довіри з боку клієнтів та партнерів.

Висновок до розділу 3

У третьому розділі було зосереджено увагу на трьох ключових аспектах для удосконалення стратегій управління ризиками ІБ: оцінці ефективності поточних стратегій, впровадженні сучасних технологічних рішень та розробці конкретних рекомендацій щодо вдосконалення цих стратегій. Цей розділ підкреслив важливість постійного вдосконалення та адаптації підходів до

управління ризиками для забезпечення високого рівня захисту інформаційних активів у сучасному динамічному кіберландшафті.

Оцінка ефективності поточних стратегій управління ризиками ІБ:

- проведений аналіз існуючих політик, процедур та інструментів управління ризиками дозволив виявити їхні сильні та слабкі сторони. Важливою частиною цього процесу було визначення прогалин і слабких місць, які потребують вдосконалення;
- виявлено, що багато організацій стикаються з технічними недоліками, такими як застаріле обладнання або програмне забезпечення, та організаційними прогалинами, такими як недостатнє навчання персоналу;
- відповідність міжнародним та національним стандартам, таким як ISO/IEC 27001 та NIST, залишається ключовим критерієм для оцінки ефективності стратегій.

Особливості впровадження сучасних технологічних рішень для управління ризиками ІБ:

- сучасні технологічні рішення, такі як ШІ, ML та блокчейн, мають значний потенціал для покращення управління ризиками ІБ;
- використання ШІ та ML дозволяє автоматизувати процес виявлення аномалій та загроз, скорочуючи час реакції та зменшуючи залежність від людського фактору;
- технологія блокчейн забезпечує високий рівень безпеки для трансакцій та даних завдяки своїй децентралізованій та незмінній природі;
- розширена аналітика та використання великих даних дозволяють швидко ідентифікувати тенденції та шаблони, що можуть бути ознаками інцидентів ІБ, полегшуючи прогнозування та запобігання майбутнім загрозам.

Розробка рекомендацій щодо вдосконалення стратегій управління ризиками ІБ:

- на основі проведеного аналізу розроблено рекомендації для вдосконалення стратегій управління ризиками, що включають технічні удосконалення, оновлення політик та процедур, а також навчання персоналу;
- запропоновано впровадження сучасних технологій, таких як багатофакторна аутентифікація, шифрування даних та системи виявлення вторгнень, для підвищення рівня безпеки;
- постійне навчання та підвищення кваліфікації персоналу через регулярні тренінги та семінари є критично важливими для ефективного впровадження нових стратегій;
- постійний моніторинг та регулярний перегляд ефективності впроваджених стратегій дозволяють організаціям адаптуватися до нових загроз та забезпечувати актуальність заходів безпеки.

Розділ 3 підкреслив важливість комплексного підходу до вдосконалення стратегій управління ризиками ІБ. Проведений аналіз та розроблені рекомендації допомагають організаціям забезпечити високий рівень захисту інформаційних активів, адаптуватися до постійно змінюваного кіберландшафту та підтримувати стійкість до сучасних кіберзагроз.

Впровадження нових політик, використання передових технологій та постійне навчання персоналу створюють надійну систему управління ризиками, що відповідає сучасним викликам і потребам організацій. Завдяки таким заходам, організації можуть забезпечити стабільність та безпеку своїх інформаційних активів, підтримуючи довіру з боку клієнтів та партнерів, а також відповідність нормативним вимогам у галузі ІБ.

ВИСНОВКИ

Дослідження охопило ключові аспекти управління ризиками ІБ у галузі критичної інфраструктури. Було розглянуто вимоги міжнародних та вітчизняних стандартів, досліджено стратегії управління ризиками та методики їх оцінки, а також розроблено рекомендації щодо удосконалення існуючих підходів.

Перший розділ присвячено аналізу ролі ризик-менеджменту в забезпеченні ІБ, а також дослідженню вимог міжнародних та національних стандартів (ISO/IEC 27005, NIST SP 800-30) і методологій управління ризиками ІБ (FAIR, OCTAVE). Визначено, що ризик-менеджмент є фундаментальною складовою процесу захисту інформаційних активів організацій та побудови СУІБ, та включає в себе такі етапи, як виявлення, оцінку, управління та моніторинг ризиків. Ефективне управління ризиками передбачає розробку стратегій для зниження ймовірності або впливу загроз, а також впровадження технічних, організаційних та фізичних заходів захисту.

В другому розділі проаналізовано різні аспекти управління ризиками ІБ в галузі критичної інфраструктури, включаючи інтеграцію управління ризиками ІБ в систему управління бізнес-ризиками, аналіз сучасних методик оцінки ризиків та визначення доцільних стратегій обробки ризиків.

Було визначено, що інтеграція управління ризиками ІБ з загальною системою управління бізнес-ризиками забезпечує комплексний підхід до захисту організації. Важливі етапи інтеграції включають аналіз поточного стану, визначення взаємозв'язків між бізнес-ризиками та ризиками ІБ, розробку інтегрованої стратегії та її впровадження.

Було досліджено сучасні кількісні та якісні методики аналізу ризиків, було визначено їхні переваги та недоліки. Було досліджено використання сучасних аналітичних інструментів, таких як ШІ та ML, що дозволяє автоматизувати процес оцінки ризиків, підвищуючи його точність та ефективність. Було проаналізовано особливості вибору доцільної стратегій обробки ризиків ІБ, зокрема, уникнення, модифікації, передачі та прийняття ризиків. Для вибору

застосовуються такі фактори, як рівень критичності активів, ймовірності та впливу ризиків, ресурсів організації та вимог законодавства.

В третьому розділі проаналізовано способи оцінки ефективності поточних стратегій управління ризиками ІБ, методи впровадження сучасних технологічних рішень та розроблено рекомендації щодо вдосконалення цих стратегій.

Аналіз існуючих політик, процедур та інструментів управління ризиками дозволив виявити сильні та слабкі сторони процесу, а також визначити прогалини, які потребують вдосконалення. При цьому забезпечення відповідності міжнародним та національним стандартам залишається ключовим критерієм для оцінки ефективності стратегій.

Було розроблено рекомендації щодо вдосконалення стратегій управління ризиками ІБ:

- використання технологій, таких як ШІ, ML та блокчейн, для підвищення ефективності управління ризиками;
- використання сучасних аналітичних інструментів для швидкої ідентифікації загроз та реагування на них;
- впроваджувати технічні удосконалення;
- забезпечити своєчасне оновлення політик та процедур;
- забезпечити належний рівень навчання персоналу;
- постійний моніторинг ефективності впроваджених стратегій.

Загалом, дослідження підкреслює важливість комплексного та інтегрованого підходу до управління ризиками ІБ в галузі критичної інфраструктури. Використання міжнародних та національних стандартів, сучасних технологій та методик оцінки ризиків, а також розробка конкретних рекомендацій щодо вдосконалення стратегій управління ризиками дозволяє організаціям забезпечити високий рівень захисту своїх інформаційних активів. Це сприяє підвищенню стійкості організацій до кіберзагроз, забезпеченню стабільності їхньої роботи та підтриманню довіри з боку клієнтів та партнерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аніловська Г. Я., Марушко Н. С., Стоколоса Т. М. Інформаційні системи і технології у фінансах : навч. посіб. Львів : Магнолія 2006. 2015. с. 312
2. Богуш В. М. Юдін О. К. Інформаційна безпека держави. Харків: Консум. 2004. с.508
3. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. 2021. URL: https://er.nau.edu.ua/handle/NAU/53733
4. Перехрест Л. М. Банківський ризик-менеджмент. *Актуальні проблеми економіки*. 2009. № 10 (100). С. 122–128.
5. Поліщук Є. А. Ризик-менеджмент інвестиційного проекту. *Формування ринкових відносин в Україні*. 2011. № 11 (126). С. 76–80.
6. Поляков Р. Стратегічний ризик-менеджмент як нова парадигма управління бізнесом. *Фінансовий ринок України*. 2005. № 12. С. 30–32.
7. Рудич О. О. Теоретичні засади формування ризик-менеджменту підприємства. *Інвестиції: практика та досвід*. 2017. № 24, груд. С. 56–60.
8. Горбань О. Г. Теоретичні основи формування сучасної моделі менеджменту. 2019. URL: https://er.knutd.edu.ua/handle/123456789/15666
9. Левко М. М. Системний підхід до визначення ролі та місця митної безпеки у забезпеченні економічної безпеки держави. *Науковий вісник НЛТУ України. Серія економічна*. 2016. Вип. 26.2. С. 95–103.
10. Горбачова І. В., Осовська Г. В. Управління підприємницькими ризиками в умовах глобальних змін. *Міжнародне економічне співробітництво: аналіз стану, реалії і проблеми*. 2024. URL: https://doi.org/10.36059/978-966-397-363-0-56
11. Розширення базової термінології у сфері захисту критичної інформаційної інфраструктури держави : thesis / Ю. О. Дрейс та ін. 2017. URL: http://er.nau.edu.ua/handle/NAU/33979

12. Деякі питання подання інформації у сфері захисту критичної інфраструктури : Постанова Каб. Міністрів України від 14.10.2022 р. № 1175. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-п#Text

13. Бєлай С. В. Особливості нормативно-правового регулювання повноважень складових сектору безпеки і оборони України у сфері захисту критичної інфраструктури. *«Закарпатські правові читання. сталий розвиток та інституційна спроможність в умовах війни: національний та міжнародно-правовий аспекти»*. 2024. URL: https://doi.org/10.36059/978-966-397-377-7-21

14. Зибарева О. В. Управління ризиками бізнес-проєктів в умовах цифровізації. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2023. № 10. URL: https://doi.org/10.54929/2786-5738-2023-10-04-09

15. 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

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

17. Гуменюк В. В., Humenuk V. Методи підвищення ефективності управління ризиками інформаційної безпеки підприємства. 2019. URL: http://elartu.tntu.edu.ua/handle/lib/30728

18. 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

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

20. Basin D., Schaller P., Schläpfer M. Risk management. *Applied information security*. Berlin, Heidelberg, 2011. P. 117–145. URL: https://doi.org/10.1007/978-3-642-24474-2_8

21. Risk assessment. *Information security cost management*. 2006. P. 135–148. URL: https://doi.org/10.1201/9781420013832-17

22. Security risk management. *Information security management*. 2010. P. 317–390. URL: https://doi.org/10.1201/9781439882634-13

23. М'ячин В. Г., Митрофанов В. Ю. Методи інтегральної оцінки ризиків підприємства. *Міжнародне економічне співробітництво: аналіз стану, реалії і проблеми*. 2024. URL: https://doi.org/10.36059/978-966-397-363-0-15

24. Ропаєва А. Г. Моделювання оцінювання ризиків інформаційної безпеки. 2018. URL: http://essuir.sumdu.edu.ua/handle/123456789/69480

25. Зянько В. В., Перерва Т. В. Методи оцінки ризиків функціонування підприємства. 2019. URL: http://ir.lib.vntu.edu.ua//handle/123456789/24393

26. Сєвєрінов О. В., Переметчик О. В. Комбінований метод аналізу ризиків інформаційної безпеки. 2020. URL: http://openarchive.nure.ua/handle/document/14289

27. А. Давидюк. Підходи до впровадження процесу управління ризиками інформаційної безпеки на об'єктах критичної інфраструктури. *Наук.-практ. конф. Забезпечення інформаційної безпеки держави у воєнній сфері: проблеми та шляхи їх вирішення*. 2020. Київ. URL: https://www.researchgate.net/publication/358783191_Pidhodi_do_vprovadzenna_procesu_upravlinna_rizikami_informacijnoi_bezpeki_na_ob%27ektah_kriticnoi_infrastrukturi

28. Analysis of methods for assessing and managing cyber risks and information security / O. Potii et al. *Radiotekhnika*. 2021. No. 206. P. 5–24. URL: https://doi.org/10.30837/rt.2021.3.206.01

29. Czuryk M. Cybersecurity and Protection of Critical Infrastructure. *Studia Iuridica Lublinensia*. 2023. Vol. 32, no. 5. P. 43–52. URL: https://doi.org/10.17951/sil.2023.32.5.43-52

30. Effectiveness of cybersecurity audit / S. Slapničar et al. *International Journal of Accounting Information Systems*. 2022. Vol. 44. P. 100548. URL: https://doi.org/10.1016/j.accinf.2021.100548

31. Watney M. Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. *European Conference on Cyber Warfare and Security*. 2022. Vol. 21, no. 1. P. 319–327. URL: https://doi.org/10.34190/eccws.21.1.196

32. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions / Ö. Aslan et al. *Electronics*. 2023. Vol. 12, no. 6. P. 1333. URL: https://doi.org/10.3390/electronics12061333

33. Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures / G. M. Makrakis et al. 2021. URL: https://www.researchgate.net/publication/354493711_Vulnerabilities_and_Attacks_Against_Industrial_Control_Systems_and_Critical_Infrastructures

34. N. Belloir, W. Ouerdane, O. Pastor, É. Frugier, L.-A. de Barmon. A Conceptual Characterization of Fake News: A Positioning Paper. Research Challenges in Information Science. 2022. URL: https://link.springer.com/chapter/10.1007/978-3-031-05760-1_41

35. Класифікація об'єктів критичної інформаційної інфраструктури держави / О. Г. Корченко та ін. 2018. URL: http://er.nau.edu.ua/handle/NAU/33201

36. Маєтний М. І. Моделі правового регулювання в сфері забезпечення безпеки критичної інформаційної інфраструктури. *Європейські перспективи*. 2021. № 2. С. 77–83. URL: https://doi.org/10.32782/ep.2021.2.13

37. Хамленко І. І. Філософія інформаційної безпеки. 2013. URL: http://er.nau.edu.ua/handle/NAU/10788

38. Кубрак О. В. Деякі аспекти інформаційної безпеки та інформаційної культури. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи*. 2023. URL: https://doi.org/10.32782/ppss.2023.1.63

39. Палагнюк Д. М., Тищук Д. С., Березюк О. В. Принципи забезпечення інформаційної безпеки. 2018. URL: http://ir.lib.vntu.edu.ua//handle/123456789/24491

40. Machine learning and blockchain technologies for cybersecurity in connected vehicles / J. Ahmad et al. WIREs Data Mining and Knowledge Discovery. 2023. URL: https://doi.org/10.1002/widm.1515

41. On the Integration of Artificial Intelligence and Blockchain Technology: a Perspective about Security / A. Kuznetsov et al. IEEE Access. 2024. P. 1. URL: https://doi.org/10.1109/access.2023.3349019

42. Crispin George. The Essence of Risk Identification in Project Risk Management: An Overview. International Journal of Science and Research (IJSR). 2020. Vol. 9, Issue 2. URL: https://www.researchgate.net/publication/339593332_The_Essence_of_Risk_Identification_in_Project_Risk_Management_An_Overview

43. Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation / M. G. Cains et al. *Risk Analysis*. 2021. URL: https://doi.org/10.1111/risa.13687

44. Aldawood H., Skinner G. Reviewing Cyber Security Social Engineering Training and Awareness Programs–Pitfalls and Ongoing Issues. Future Internet. 2019. Vol. 11, no. 3. P. 73. URL: https://doi.org/10.3390/fi11030073

45. Cyber security management model for critical infrastructure / T. Limba et al. *Entrepreneurship and Sustainability Issues*. 2017. Vol. 4, no. 4. P. 559–573. URL: https://doi.org/10.9770/jesi.2017.4.4(12)