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: “РОЗРОБЛЕННЯ МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ ОБ’ЄКТІВ 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

_____ Сергій МУСІЄНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Сергій МУСІЄНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
Д.е.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент 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

Мусієнку Сергію Юрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Розроблення моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н, доцент.
(ІПРІЗВИЩЕ, 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: *інформаційна безпека підприємства, методи та засоби забезпечення інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Аналіз кібербезпеки об’єктів критичної інфраструктури.
4.2. Дослідження моделей управління ризиками кібербезпеки.
4.3. Розроблення моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури.

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 кібербезпеки об’єктів критичної інфраструктури.	08.04.2024	
4.	Дослідження моделей управління ризиками кібербезпеки.	22.04.2024	
5.	Розроблення моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури	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 ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Сергій МУСІЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(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 Мусієнко С.Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Розроблення моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач МУСІЄНКО Сергій у кваліфікаційній роботі проаналізував особливості управління інформаційною безпекою об'єктів критичної інфраструктури, дослідив основні засоби та методи захисту інформації на об'єктах критичної інфраструктури, вивчив засоби підвищення ефективності захисту інформації, розробив модель управління ризиками об'єктів критичної інфраструктури та практичні рекомендації по її удосконаленню з урахуванням особливостей організації.

МУСІЄНКО Сергій 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 МУСІЄНКА Сергія на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Мусієнко С.Ю. 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 МУСІЄНКА Сергія
на тему “Розроблення моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури ”

Актуальність.

Зростання важливості об'єктів критичної інфраструктури у забезпеченні життєдіяльності людини, суспільства і держави потребує удосконалення їх захисту. Зростання цифровізації цих систем призводить до збільшення їхньої вразливості перед кіберзагрозами. У зв'язку з цим, управління ризиками кібербезпеки стає надзвичайно важливим аспектом захисту об’єктів критичної інфраструктури та потребує удосконалення існуючих моделей кіберзахисту та пошуку сучасних підходів з метою реагування на нові кіберзагрози.

Позитивні сторони.

1. У роботі досліджені сучасні моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури , визначені їх позитивні сторони та властивості. За результатами аналізу наукової літератури визначена потреба в удосконаленні сучасних моделей кіберзахисту для врахування розвитку кіберзагроз. Розроблена модель управління ризиками, яка дозволяє врахувати всі взаємопов’язані компоненти кібербезпеки організацій з їх конкретними особливостями.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблені логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу наукових публікацій та проаналізував сучасні дослідження кібербезпеки об’єктів критичної інфраструктури.

4. За результатами дослідження розроблені рекомендації з удосконалення моделі з урахуванням особливостей організацій.

Недоліки.

У роботі доцільно було б приділити більше уваги застосуванню штучного інтелекту для автоматизації розробленої моделі.

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

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

Рецензент: _____ _____ _____
науковий ступінь, вчене звання *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена оцінці ефективності засобів та методів захисту інформації на підприємстві. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 71 аркуш, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури.

Об'єктом дослідження є управління ризиками кібербезпеки об'єктів критичної інфраструктури.

Предмет дослідження – модель управління ризиками кібербезпеки об'єктів критичної інфраструктури.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи контент-аналізу та синтезу при дослідженні наукових праць з тематики роботи, порівняння при аналізі сучасних моделей управління ризиками об'єктів критичної інфраструктури, моделювання при створенні моделі.

Як результат у роботі проаналізовано особливості кібербезпеки об'єктів критичної інфраструктури, досліджено моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури, способи впровадження та вдосконалення моделі управління ризиками кібербезпеки, розроблено практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при аналізі загроз для розробки моделей управління ризиками у контексті об'єктів критичної інфраструктури.

Ключові слова: КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ, МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ, ОЦІНКА ВРАЗЛИВОСТЕЙ, АНАЛІЗ ТА ОЦІНКА РИЗИКІВ.

ABSTRACT

The qualification work is devoted to the assessment of the effectiveness of information security tools and methods at an enterprise. The work consists of an introduction, three chapters containing 6 figures, conclusions and the list of references containing 45 items. The total volume of the work is 71 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop a model for cybersecurity risk management of critical infrastructure facilities.

The object the study is the management of cyber security risks of critical infrastructure objects.

The subject of the study is model of cyber security risk management of critical infrastructure objects.

Research methods. In order to solve the above-mentioned scientific task, the methods of content analysis and synthesis were used in the study of scientific works on the subject of the work, comparison in the analysis of modern models of risk management of critical infrastructure objects, modeling in the creation of a model.

As a result, the work analyzed the peculiarities of critical infrastructure cybersecurity, investigated models of cybersecurity risk management of critical infrastructure, methods of implementing and improving the model of cybersecurity risk management, developed practical recommendations.

Field of application. The developed approaches can be used in the analysis of threats to develop a risk management model in the context of critical infrastructure.

Keywords: CRITICAL INFRASTRUCTURE CYBERSECURITY, CYBERSECURITY RISK MANAGEMENT, RISK MANAGEMENT MODEL, VULNERABILITY ASSESSMENT, RISK ANALYSIS AND ASSESSMENT.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, в якому зростає залежність сучасного суспільства від інформаційних технологій та кіберпростору, тема розробки моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури є важливою, як ніколи. Об'єкти критичної інфраструктури, є ключовими для функціонування держави та суспільства. Кіберзагрози можуть призвести до значних економічних збитків, порушення життєдіяльності населення та загроз національній безпеці. Тому розробка ефективної моделі управління ризиками кібербезпеки є критично важливою для забезпечення стабільного та безперебійного функціонування цих об'єктів.

З огляду на зазначене дослідження оцінки ефективності засобів та методів захисту інформації на підприємстві є актуальним науковим завданням.

Мета роботи - розробка моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури.

Об’єкт дослідження - управління ризиками кібербезпеки об’єктів критичної інфраструктури.

Предмет дослідження – модель управління ризиками кібербезпеки об’єктів критичної інфраструктури.

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

1. Проаналізувати кібербезпеку об’єктів критичної інфраструктури.

2. Дослідити модель управління ризиками кібербезпеки.

3. Розробити модель управління ризиками кібербезпеки об’єктів критичної інфраструктури.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи контент-аналізу та синтезу при дослідженні наукових праць з тематики роботи, порівняння при аналізі сучасних моделей управління ризиками об’єктів критичної інфраструктури, моделювання при створенні моделі.

Як результат у роботі проаналізовано особливості кібербезпеки об’єктів

критичної інфраструктури, досліджено моделі управління ризиками кібербезпеки об’єктів критичної інфраструктури, способи впровадження та вдосконалення моделі управління ризиками кібербезпеки, розроблено практичні рекомендації.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити правильну оцінку ризиків кібербезпеки для об'єктів критичної інфраструктури. Результати дослідження можуть допомогти оптимізувати систему управління ризиками, спираючись на оцінку існуючих методів та рекомендації щодо їх покращення. Це дозволить підвищити захищеність критично важливих об'єктів від кіберзагроз та забезпечити безперебійне функціонування життєво важливих систем.

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

Розділ 1 ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури

Тема кібербезпеки об'єктів критичної інфраструктури надзвичайно важлива в сучасному світі, оскільки багато сфер нашого життя стали залежними від комп'ютеризації та мережевого зв'язку. Об'єкти критичної інфраструктури включають в себе електростанції, водні споруди, транспортні системи, банківські системи, комунікаційні мережі та багато інших.

Однак залежність від інформаційних технологій також вносить ризики. Кіберзлочинці, терористи та інші зловмисники можуть використовувати цю залежність для здійснення кібератак, спрямованих на об'єкти критичної інфраструктури. Навіть короткочасне втручання в роботу таких систем може мати серйозні наслідки для безпеки та економіки країни.

Для забезпечення кібербезпеки об'єктів критичної інфраструктури необхідно вживати комплекс заходів. Це включає в себе захист мережевих з'єднань, регулярне оновлення програмного забезпечення, використання сучасних засобів шифрування даних, а також впровадження систем виявлення та реагування на кіберзагрози.

Окрім технічних заходів, важливо також підвищувати обізнаність персоналу щодо кібербезпеки, проводити тренування та симуляції кібератак для підвищення реагування на події.

Співпраця на міжнародному рівні також є ключовою. Багато об'єктів критичної інфраструктури мають транскордонний характер, тому співпраця між країнами у сфері кібербезпеки стає критично важливою для ефективного захисту.

Кібербезпека об'єктів критичної інфраструктури вимагає комплексного підходу, включаючи технічні заходи, підвищення обізнаності персоналу та міжнародну співпрацю. Тільки за умови такого підходу можна забезпечити надійний захист цих важливих об'єктів від кіберзагроз.

Один із ключових аспектів забезпечення кібербезпеки об’єктів критичної інфраструктури (рис.1.1) полягає у наявності відповідного законодавства, яке визначає правові рамки та вимоги щодо захисту цих об’єктів від кіберзагроз. Це може включати в себе прийняття спеціальних законів або внесення відповідних поправок до існуючих законів, що регулюють сферу інформаційної безпеки та критичної інфраструктури. Законодавча база може також визначати обов’язкові вимоги щодо впровадження конкретних заходів забезпечення кібербезпеки, а також відповідальність за їх невиконання.

Рис. 1.1. Ключові аспекти нормативно-правового забезпечення кібербезпеки об’єктів критичної інфраструктури

Законодавча база є фундаментом для забезпечення кібербезпеки об'єктів критичної інфраструктури і встановлює правові рамки та вимоги щодо їх захисту від кіберзагроз.

Деякі країни встановлюють спеціальні закони, спрямовані на захист критичної інфраструктури від кіберзагроз. Ці закони можуть визначати об'єкти критичної інфраструктури, обов'язковість впровадження конкретних заходів кібербезпеки, а також відповідальність за порушення цих вимог.

У багатьох країнах існуючі закони, які регулюють сферу інформаційної безпеки, можуть бути розширені або доповнені поправками, що стосуються захисту критичної інфраструктури. Це може включати встановлення нових вимог до організацій, які управляють такими об'єктами, або розширення повноважень відповідних державних органів [1].

Законодавча база також може включати посилання на національні та міжнародні стандарти та рекомендації з кібербезпеки. Наприклад, організації можуть бути вимушені дотримуватися конкретних стандартів безпеки даних або використовувати рекомендації відповідних організацій, таких як Міжнародна організація зі стандартизації (ISO) або Національний інститут стандартів і технологій (NIST).

Деякі країни також можуть мати окремі закони або акти, що стосуються кібербезпеки загалом. Ці закони можуть встановлювати загальні принципи та вимоги, які застосовуються до всіх секторів, включаючи й об'єкти критичної інфраструктури.

Крім внутрішньодержавного законодавства, країни також можуть брати участь у міжнародних угодах та конвенціях, спрямованих на забезпечення кібербезпеки. Ці угоди можуть встановлювати стандарти та правила для міжнародного співробітництва у сфері кібербезпеки та обміну інформацією про загрози.

Окрім законодавства, існують також міжнародні та національні нормативні документи та стандарти, які встановлюють вимоги до кібербезпеки об’єктів критичної інфраструктури. Ці нормативні документи можуть містити рекомендації щодо застосування конкретних технологій, методів або процесів для забезпечення безпеки інформації та інфраструктури. Деякі з них можуть бути

обов’язковими для впровадження певних суб’єктів, які управляють об’єктами критичної інфраструктури.

Норми та стандарти є важливими складовими для забезпечення кібербезпеки об'єктів критичної інфраструктури. Вони встановлюють конкретні вимоги, процедури та рекомендації, які повинні виконуватися для захисту інфраструктури від кіберзагроз [2].

Організації, такі як Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (IEC), розробляють стандарти з кібербезпеки, які мають міжнародне визнання. Наприклад, ISO/IEC 27001 встановлює вимоги до систем керування інформаційною безпекою, включаючи об'єкти критичної інфраструктури. Ці стандарти надають рамки для впровадження ефективних систем захисту інформації та інфраструктури.

Багато країн розробляють власні національні стандарти з кібербезпеки, які доповнюють міжнародні норми та враховують специфіку своєї національної інфраструктури та законодавства. Ці стандарти можуть бути розроблені державними органами, національними стандартизаційними організаціями або іншими зацікавленими сторонами.

Окрім стандартів, існують також рекомендації та керівництва від різних організацій та агентств, які спрямовані на покращення кібербезпеки об'єктів критичної інфраструктури. Наприклад, Національний інститут стандартів і технологій (NIST) США розробляє Кібербезпековий керівництво та інші документи з кібербезпеки, які надають детальні поради та методики захисту.

Деякі галузі можуть мати спеціалізовані стандарти з кібербезпеки, які враховують особливості конкретного сектора. Наприклад, в галузі медичних технологій можуть бути розроблені стандарти для захисту медичних пристроїв від кіберзагроз.

У деяких випадках стандарти та норми можуть бути обов'язковими для виконання певними суб'єктами, які управляють об'єктами критичної інфраструктури. Це може бути встановлено законодавством або регуляторними органами.

Нормативно-правове забезпечення кібербезпеки також передбачає наявність механізмів контролю за дотриманням встановлених вимог та відповідальності за їх порушення. Це може включати проведення регулярних аудитів безпеки, встановлення процедур звітування про інциденти кібербезпеки, а також визначення санкцій для суб’єктів, які порушили встановлені правила та вимоги.

Механізми контролю та відповідальності важливі для забезпечення ефективності та відповідального ставлення до кібербезпеки об'єктів критичної інфраструктури.

Регулярні аудити безпеки дозволяють перевіряти відповідність систем кібербезпеки встановленим стандартам і вимогам. Вони можуть бути проведені внутрішніми або зовнішніми аудиторами, які оцінюють ефективність заходів забезпечення безпеки та ідентифікують потенційні проблеми або слабкі місця [3].

Організації, які управляють об'єктами критичної інфраструктури, повинні мати процедури звітування про інциденти кібербезпеки. Це дозволяє вчасно виявляти та реагувати на кіберзагрози, а також аналізувати причини та наслідки інцидентів для уникнення їх повторення в майбутньому.

Використання спеціалізованих систем моніторингу та виявлення загроз дозволяє оперативно виявляти потенційні кіберзагрози та атаки на об'єкти критичної інфраструктури. Ці системи можуть використовувати аналіз поведінки, сигнатурне виявлення, інтелектуальний аналіз та інші методи для виявлення аномальної активності.

Організації та особи, які управляють об'єктами критичної інфраструктури, несуть відповідальність за забезпечення адекватного рівня кібербезпеки. Це може включати встановлення чітких ліній відповідальності, розробку політик та процедур безпеки, надання необхідних ресурсів та підтримки для здійснення заходів забезпечення безпеки.

У випадку порушення вимог та політик забезпечення кібербезпеки можуть бути застосовані відповідні санкції. Це може включати дисциплінарні заходи

проти співробітників, фінансові штрафи для організацій або навіть правову відповідальність у випадках серйозних порушень.

З огляду на те, що багато об’єктів критичної інфраструктури мають транскордонний характер, нормативно-правове забезпечення кібербезпеки також може передбачати міжнародне співробітництво. Це включає обмін інформацією про кіберзагрози та інциденти, спільне розроблення стандартів та нормативних документів, а також спільні заходи з протидії кіберзлочинності на міжнародному рівні.

Міжнародне співробітництво у сфері кібербезпеки є критично важливим для ефективного захисту об'єктів критичної інфраструктури через їх транскордонний характер та глобальний вплив.

Країни та міжнародні організації можуть обмінюватися інформацією про виявлені кіберзагрози та інциденти. Це дозволяє швидко виявляти нові загрози та розробляти ефективні стратегії відповіді на них [4].

Країни можуть спільно працювати над розробленням міжнародних стандартів та нормативних документів з кібербезпеки, які будуть застосовуватися на всій території. Це допомагає уніфікувати підходи до захисту критичної інфраструктури та підвищує її загальний рівень безпеки.

Країни можуть проводити спільні навчання та тренування з протидії кіберзагрозам, щоб підвищити навички та готовність своїх кадрів до реагування на кібератаки та інциденти.

Країни можуть обмінюватися кращими практиками з кібербезпеки та взаємно використовувати досвід у сфері захисту критичної інфраструктури. Це допомагає вдосконалювати власні підходи до кібербезпеки та підвищує загальний рівень захисту.

Країни можуть укладати міжнародні договори та угоди з метою спільного реагування на кіберзагрози та забезпечення кібербезпеки об'єктів критичної інфраструктури. Ці документи можуть включати механізми співпраці, обміну інформацією та взаємодопомоги у разі кібератак.

Ефективне забезпечення кібербезпеки об'єктів критичної інфраструктури вимагає комплексного підходу, який включає нормативно-правове регулювання, стандартизацію, механізми контролю та відповідальності, а також міжнародне співробітництво. Нормативно-правове забезпечення встановлює правові рамки та вимоги для захисту, стандарти та рекомендації визначають конкретні заходи безпеки, а механізми контролю та відповідальності забезпечують їх ефективну реалізацію. Міжнародне співробітництво важливо для обміну досвідом та ресурсами у протидії кіберзагрозам та забезпеченні колективної безпеки. Лише взаємодія на всіх рівнях - від національних до міжнародних - може гарантувати надійний захист критичної інфраструктури в умовах постійної еволюції кіберзагроз.

1.2 Аналіз тенденцій розвитку кіберзагроз у контексті критичної інфраструктури

Аналіз тенденцій розвитку кіберзагроз (рис.2.1) у контексті критичної інфраструктури включає дослідження актуальних тенденцій та еволюції загроз, які можуть впливати на безпеку цієї інфраструктури.

Рис. 1.2. Ключові аспекти аналізу тенденцій розвитку кіберзагроз критичної інфраструктури

Дослідження новітніх кіберзагроз, таких як атаки розподіленого відмову в обслуговуванні (DDoS), розкрадання даних, віруси та шкідливі програми, а також атаки на промислові системи керування (ICS), є ключовим для розуміння потенційних загроз для критичної інфраструктури [5].

Аналіз новітніх кіберзагроз є важливою складовою у забезпеченні кібербезпеки об'єктів критичної інфраструктури. Він передбачає дослідження останніх тенденцій та розвитку загроз в цій області.

Аналіз новітніх кіберзагроз охоплює різноманітні типи загроз, такі як віруси, шкідливі програми, розкрадання даних, атаки відмови в обслуговуванні (DDoS), фішинг, а також атаки на промислові системи керування (ICS) та критичні інфраструктурні об'єкти.

Аналіз включає вивчення методів, які використовуються зловмисниками для здійснення кібератак. Це може включати експлуатацію вразливостей програмного забезпечення, використання соціального інженерінгу, введення в оману користувачів та інші техніки.

Аналіз допомагає виявити потенційні вразливості в системах критичної інфраструктури та їх можливі використання для здійснення атак. Це включає вивчення вразливих точок в мережах, програмному забезпеченні, апаратурі та процесах.

Аналіз також включає вивчення джерел та походження кіберзагроз. Це можуть бути зловмисники, кіберзлочинці, державні актори, хактивісти та інші суб'єкти, які мають інтерес у проведенні кібератак.

Аналіз допомагає розуміти механізми поширення кіберзагроз та їх потенційні наслідки для критичної інфраструктури. Це може включати швидке поширення через мережу, вплив на додаткові системи та послуги, а також можливість дальшого розповсюдження через цільові об'єкти [6].

Важливо вивчати методи, якими користуються зловмисники для здійснення кібератак на критичну інфраструктуру. Це може включати

використання вразливостей програмного забезпечення, соціального інженерінгу, фішингу та інших методів.

Аналіз методів атак - це дослідження та оцінка різних методів, якими зловмисники можуть здійснити кібератаки на об'єкти критичної інфраструктури. Цей процес включає в себе докладне вивчення та розуміння різноманітних технік та інструментів, які використовуються зловмисниками для отримання несанкціонованого доступу до систем та даних.

Експлуатація вразливостей програмного забезпечення: Зловмисники можуть використовувати вразливості в програмному забезпеченні для здійснення атак. Це може включати використання відомих вразливостей, відмовлення в обслуговуванні (DoS) атаки, впровадження шкідливого програмного забезпечення через вразливості у веб-додатках або інших програмах.

Соціальний інженерінг - це процес використання маніпуляційних технік для отримання конфіденційної інформації від людей. Зловмисники можуть використовувати соціальний інженерінг для введення в оману співробітників та отримання доступу до систем або даних [7].

Фішинг - це вид атаки, при якому зловмисники намагаються отримати конфіденційну інформацію, таку як паролі або особисті дані, шляхом використання підроблених електронних листів, веб-сайтів або повідомлень.

Зловмисники можуть розробляти та розповсюджувати віруси, черви та інші шкідливі програми, які можуть використовувати для отримання несанкціонованого доступу до систем або для шкоди їхній роботі.

Зловмисники можуть використовувати спеціалізовані техніки для атак на промислові системи керування, такі як SCADA-системи, які використовуються в критичних секторах, таких як енергетика, транспорт або водопостачання.

Ці атаки спрямовані на перевантаження або відключення систем, послуг або мереж шляхом високої кількості запитів або трафіку. Вони можуть призвести до недоступності об'єктів критичної інфраструктури.

Аналіз тенденцій допомагає оцінити ризики для конкретних об'єктів критичної інфраструктури. Це дозволяє ідентифікувати потенційні загрози та визначити їх вплив на роботу систем.

Оцінка ризиків у контексті кібербезпеки критичної інфраструктури - це процес визначення та оцінки потенційних загроз, вразливостей та наслідків, які можуть виникнути внаслідок кібератак або інцидентів безпеки. Цей процес включає в себе детальний аналіз та оцінку кіберризиків з метою ідентифікації, квантифікації та управління ними.

Ідентифікація загроз та вразливостей включає аналіз потенційних загроз та вразливостей, які можуть вплинути на критичну інфраструктуру. Це може бути внаслідок програмних атак, атак фізичного доступу, витоку конфіденційної інформації, технічних вад або неправильного конфігурування систем.

Після ідентифікації загроз і вразливостей проводиться оцінка потенційних наслідків цих ризиків. Це включає аналіз можливих фінансових, оперативних, репутаційних та правових наслідків кібератак для критичної інфраструктури та її користувачів.

Оцінка ризиків також включає визначення рівня ймовірності та впливу кожної ідентифікованої загрози. Це допомагає визначити, які ризики є найбільш серйозними та потенційно шкідливими для критичної інфраструктури [8].

Після оцінки ризиків розробляються стратегії управління ризиками для зменшення або прийняття ризику. Це може включати розробку заходів забезпечення безпеки, резервування, перекладання ризику, а також страхування.

Оцінка ризиків є динамічним процесом, і вона повинна регулярно оновлюватися та переглядатися з урахуванням змін у загрозах, вразливостях, технологіях та стратегіях захисту. Також важливо моніторити ефективність прийнятих заходів та вносити корективи за необхідності.

На основі аналізу тенденцій можна робити прогнози щодо майбутніх кіберзагроз і розвивати стратегії та заходи безпеки для їх запобігання.

Прогнозування майбутніх загроз у сфері кібербезпеки критичної інфраструктури - це процес аналізу та ідентифікації потенційних майбутніх

загроз та ризиків, з якими можуть зіткнутися системи та інфраструктура в майбутньому. Цей процес включає в себе використання різноманітних методів та джерел інформації для передбачення можливих напрямків розвитку загроз та розробки стратегій захисту.

Прогнозування майбутніх загроз починається з аналізу трендів та паттернів, які спостерігаються в сучасних кібератаках та інцидентах. Це може включати аналіз таких факторів, як типи атак, цільові об'єкти, методи атак та використані засоби.

Прогнозування також передбачає вивчення нових технологій та їх потенційних впливів на кібербезпеку. Наприклад, розвиток Інтернету речей (IoT), штучного інтелекту (AI) та квантового обчислення може відкривати нові можливості для кібератак, які потрібно передбачити та узгодити [9].

Прогнозування майбутніх загроз включає моніторинг активності кіберзлочинців та груп, що впливають на кібербезпеку. Це може включати аналіз їхніх тактик, технік та процедур, а також оцінку їхніх потенційних мотивацій та цілей.

Для прогнозування майбутніх загроз можуть використовуватися прогностичні моделі та аналітичні інструменти, які дозволяють передбачати можливі сценарії розвитку подій на основі історичних даних та поточних тенденцій.

Співпраця з іншими суб'єктами кібербезпеки та обмін інформацією є також важливими компонентами прогнозування майбутніх загроз. Це дозволяє отримувати доступ до розширених джерел інформації та аналізувати спільно зі знавцями галузі.

Важливо слідкувати за новими технологіями та трендами в галузі кібербезпеки, такими як штучний інтелект, блокчейн та Інтернет речей, оскільки вони можуть стати об'єктом нових кіберзагроз.

Моніторинг нових технологій та трендів у сфері кібербезпеки є важливим елементом забезпечення безпеки критичної інфраструктури. Цей процес передбачає постійний аналіз розвитку технологій, методів атак та заходів захисту

для виявлення нових загроз та ефективних стратегій захисту. Ось більш детальна інформація про моніторинг нових технологій та трендів:

Це включає вивчення нових технологій, які використовуються у кіберпросторі, таких як штучний інтелект, блокчейн, квантові обчислення, Інтернет речей (IoT), машинне навчання та інші. Важливо розуміти, як ці технології можуть бути використані як для забезпечення безпеки, так і для зловживання [10].

Моніторинг нових технологій включає аналіз потенційних нових загроз, які можуть виникнути в результаті використання цих технологій. Наприклад, зростання кількості підключених до Інтернету речей може збільшити потенційні вектори атак на критичну інфраструктуру.

Моніторинг нових технологій також включає слідкування за трендами атак та зловживанням вже існуючих технологій для здійснення кібератак. Наприклад, зловмисники можуть використовувати нові методи атак, такі як атаки через штучний інтелект або зламання системи машинного навчання.

Моніторинг нових технологій включає проведення досліджень та аналізу нових загроз та розвитку в області кібербезпеки. Це може включати аналіз публікацій, наукових статей, конференцій та інших джерел інформації про нові технології та їх потенційні впливи на безпеку.

На основі моніторингу нових технологій розробляються стратегії захисту, спрямовані на протидію новим загрозам та ефективне захищення критичної інфраструктури. Це може включати розробку нових заходів безпеки, вдосконалення захисту вже існуючих систем та реагування на нові загрози шляхом розробки відповідних стратегій захисту.

Геополітичний контекст також може впливати на кібербезпеку критичної інфраструктури через можливість державних атак або кібервійни [11].

Вивчення геополітичного контексту в контексті кібербезпеки критичної інфраструктури - це аналіз політичних, економічних, соціальних та технологічних факторів у різних частинах світу, що можуть впливати на кіберзагрози, рівень кібербезпеки та стратегії захисту.

Вивчення геополітичного контексту включає аналіз поточних геополітичних конфліктів та напруженостей, оскільки вони можуть мати прямий вплив на кібербезпеку. Наприклад, кібератаки можуть бути використані як інструмент в геополітичних конфліктах для здійснення шпигунства, військової розвідки чи дестабілізації опонентів.

Вивчення геополітичного контексту також передбачає оцінку рівня кіберзагроз у різних регіонах світу. Це включає вивчення активності кіберзлочинців, діяльності державних агентів, а також рівня кібербезпеки в різних країнах.

Геополітичний контекст також включає аналіз стандартів та регуляцій у сфері кібербезпеки різних країн та регіонів. Різні країни можуть мати власні законодавчі та регуляторні рамки для забезпечення кібербезпеки, що може впливати на заходи захисту та стратегії управління ризиками[12].

Вивчення геополітичного контексту також включає співпрацю з іншими країнами та міжнародними організаціями у сфері кібербезпеки. Це може включати обмін інформацією про загрози, спільні вправи та навчання, а також спільні ініціативи зі створення стандартів та політик кібербезпеки.

Вивчення геополітичного контексту допомагає розуміти геостратегічні тенденції та перспективи розвитку кіберзагроз у різних регіонах світу. Це дозволяє адаптувати стратегії захисту та управління ризиками до специфіки кожного регіону та прогнозувати майбутні загрози [13].

Аналіз тенденцій розвитку кіберзагроз є важливим етапом у розробці стратегій та заходів забезпечення кібербезпеки критичної інфраструктури. Він дозволяє розуміти сучасні та потенційні загрози, визначати пріоритети та розробляти ефективні заходи захисту.

Аналіз тенденцій розвитку кіберзагроз у контексті критичної інфраструктури виявляється ключовим етапом в забезпеченні стійкості та безпеки сучасних систем. Проведення досліджень та аналізу актуальних тенденцій у цій сфері дозволяє краще розуміти загрози, які стикаються із критичною інфраструктурою, та розробляти ефективні стратегії захисту.

Заснований на цьому аналіз дозволяє виявити нові типи атак, вразливості та потенційні сценарії загроз, що дозволяє забезпечити більш глибоке розуміння ризиків та розробити відповідні заходи протидії. Такий підхід сприяє зміцненню стійкості та надійності критичної інфраструктури в умовах постійно змінюючого кіберландшафту.

1.3 Залежність інформаційних об’єктів захисту від типу потенційних загроз

Залежність інформаційних об’єктів захисту від типу потенційних загроз визначається рядом факторів (рис. 1.3), що включають характер самої загрози, уразливості конкретного об'єкта, його значення та важливість для функціонування критичної інфраструктури.

Рис. 1.3. Фактори, якими визначається залежність інформаційних об’єктів захисту від типу потенційних загроз

Різні типи загроз, такі як виток інформації, вірусні атаки, деніал-оф-сервіс (DoS), фішинг, а також кібершпигунство та кібертероризм, можуть мати різний

вплив на інформаційні об'єкти захисту. Наприклад, витік конфіденційної інформації може призвести до серйозних фінансових та репутаційних втрат для організації.

Характер загрози в контексті кібербезпеки охоплює широкий спектр можливих небезпек, які можуть виникнути внаслідок кібератак або кіберінцидентів [14].

Тип атаки – це перший елемент, який визначає характер загрози. Атаки можуть бути спрямовані на конфіденційність, цілісність або доступність інформації. Наприклад, зловмисники можуть впровадити вірус або програмне забезпечення-шифрувальник для заблокування доступу до файлів (атака на доступність), використовуючи соціальну інженерію для отримання доступу до конфіденційних даних (атака на конфіденційність), або змінити дані в системі (атака на цілісність).

Джерело атаки вказує на те, хто стоїть за атакою. Джерелом можуть бути кіберзлочинці, державні агенти, хакерські групи або навіть внутрішні загрози зсередини організації.

Методи атаки описують, як саме виконується атака. Це може бути використання вразливостей програмного забезпечення, соціальна інженерія, атаки через мережу, фішинг, атаки з використанням вредоносного ПЗ і багато іншого.

Масштаб інциденту може бути локальним, коли атака впливає лише на окрему систему чи організацію, або глобальним, коли вона має великий вплив на багато організацій або навіть цілі галузі.

Деякі атаки можуть бути спрямовані на певні типи даних або систем, такі як фінансова інформація, медичні записи, енергетичні системи тощо.

Це те, що може статися внаслідок атаки, такі як втрата даних, витрати на відновлення, репутаційні та юридичні проблеми, або навіть загроза для безпеки.

Рівень захисту та стійкість інформаційного об'єкта до конкретних типів загроз може суттєво варіюватися залежно від наявних уразливостей. Наприклад, застосування захисних заходів, таких як шифрування даних та мережеві

брандмауери, може зменшити ризик витоку інформації або атаки з боку зовнішніх зловмисників [15].

Уразливості об'єкта захисту є слабкими місцями чи вразливими точками в системі, які можуть бути використані для здійснення атаки або незаконного доступу. Вони можуть бути викликані різними факторами і можуть бути результатом недоліків у дизайні, розробці або експлуатації системи.

Уразливості можуть бути різноманітними і включати в себе такі види, як:

- уразливості програмного забезпечення: недоліки або помилки в програмному коді, які можуть бути використані зловмисниками для здійснення атак;
- уразливості мережевої безпеки: недоліки у конфігурації мережевого обладнання або програмного забезпечення, які можуть призвести до незаконного доступу або витоку інформації;
- соціальна інженерія: використання маніпуляційних технік для отримання недозволеного доступу до системи шляхом маніпуляції користувачів або співробітників;
- фізичні уразливості: недоліки у фізичній безпеці приміщень або обладнання, які дозволяють зловмисникам отримати фізичний доступ до системи.

Уразливості можуть бути виявлені в результаті різних дій:

- помилки в програмному коді: недоліки або помилки, допущені під час розробки програмного забезпечення;
- вразливості мережевої конфігурації: неналежна конфігурація мережевого обладнання або програмного забезпечення, така як відкриті порти або слабкі паролі;
- слабкі місця в соціальній інженерії: недостатня увага до кібербезпеки з боку персоналу, що може призвести до розголошення конфіденційної інформації.

- фізичні недоліки: недостатня фізична безпека приміщень або обладнання, що може дозволити зловмисникам отримати доступ до системи через фізичний доступ.

Уразливості можуть мати різний вплив на систему, включаючи можливість витоку конфіденційної інформації, порушення цілісності даних або навіть повний відмов системи [16].

Деякі інформаційні об'єкти можуть мати критичне значення для нормального функціонування критичної інфраструктури. Наприклад, системи управління енергорозподілом чи транспортні мережі можуть бути суттєво уразливими до кібератак через їх критичне значення для забезпечення безперебійності роботи суспільства.

Значення об'єкта для функціонування інфраструктури визначається його критичністю та важливістю для нормальної роботи системи чи організації. Для критичної інфраструктури, такої як енергетика, транспорт, медицина, телекомунікації, банківська сфера тощо, значення об'єктів для їх функціонування може бути вирішальним.

Деякі об'єкти можуть надавати послуги або інфраструктуру, без яких функціонування суспільства може бути суттєво ускладненим або навіть припинитися. Наприклад, енергетичні системи, системи водопостачання та каналізації, системи транспорту, телекомунікаційні мережі тощо.

Об'єкти критичної інфраструктури можуть мати значний економічний вплив, який виражається у великій кількості грошей, що обертаються, та впливі на господарську діяльність країни чи регіону.

Деякі об'єкти можуть бути важливими для забезпечення безпеки, здоров'я та добробуту громадян. Наприклад, медичні установи, системи екстреної допомоги, а також системи зв'язку для забезпечення комунікації під час кризових ситуацій [17].

Об'єкти критичної інфраструктури можуть мати стратегічне значення для національної безпеки та суверенітету країни. Їхнє функціонування може бути

об'єктом уваги з боку державних органів та зловмисників, що робить їх особливо цільовими для атак.

Необхідність безперебійного функціонування критичної інфраструктури може впливати на інші сектори економіки та життя суспільства. Відмова одного об'єкта може мати ланцюгову реакцію на інші системи та послуги.

Інформаційні об'єкти, які легко доступні для атаки через недостатній рівень захисту або відкритий доступ до мережі Інтернет, можуть бути особливо вразливими до різних типів кіберзагроз.

Ступінь доступності для атаки вказує на те, наскільки легко зловмисникам може бути доступ до об'єкта для виконання кібератаки або порушення безпеки. Ця ступінь може залежати від різних факторів, які варіюються від технічних аспектів до соціальних та організаційних.

Об'єкти з більшим числом вразливостей, таких як недопрацьований програмний код, неналежно налаштовані мережеві системи або слабкі паролі, можуть бути більш доступними для атак.

Об'єкти з низьким рівнем захисту, такі як відсутність антивірусного програмного забезпечення, мережеві системи без фірмового брандмауера або відсутність мультифакторної аутентифікації, можуть бути легше доступними для атак.

Деякі конфігурації систем можуть зробити їх більш уразливими до атак. Наприклад, відкриті мережеві порти або неналежно налаштовані правила доступу можуть забезпечити зловмисникам легший доступ до системи.

Об'єкти, які мають високий рівень відкритості, такі як системи, які повністю доступні через Інтернет без будь-яких обмежень, можуть бути більш схильними до атак.

Об'єкти, де користувачі або персонал не мають достатнього рівня обізнаності з кібербезпекою і не дотримуються найбільших практик безпеки, можуть бути більш легкодоступними для атак.

Зловмисники можуть використовувати соціальну інженерію, щоб отримати доступ до об'єкта шляхом маніпулювання людьми, наприклад, через фішинг або інші маніпуляційні техніки.

Розуміння потенційних наслідків кіберзагроз для конкретного інформаційного об'єкта є ключовим для визначення необхідного рівня захисту та розробки відповідних стратегій захисту [18].

Можливі наслідки загроз для об'єкта критичної інфраструктури можуть бути серйозними та мають потенційно значний вплив на безпеку, економіку та суспільство в цілому.

Якщо об'єкт критичної інфраструктури стає жертвою кібератаки, втрата конфіденційної інформації може мати серйозні наслідки. Наприклад, витік особистих даних клієнтів банку або медичних записів пацієнтів може призвести до порушення приватності та негативно вплинути на репутацію організації.

Атаки, спрямовані на порушення цілісності даних, можуть призвести до зміни, пошкодження або знищення інформації. Це може призвести до втрати даних, неправильних рішень при прийнятті рішень та негативного впливу на операційну діяльність.

Деніал-оф-сервіс (DoS) або дистриб'юваний деніал-оф-сервіс (DDoS) атаки можуть призвести до перерв у роботі сервісів або систем, що може мати серйозні наслідки для ефективності роботи організацій та задоволення потреб користувачів.

Кібератаки можуть призвести до значних фінансових втрат через втрату доходу внаслідок перерв у роботі, витрати на відновлення систем та компенсації за втрату даних або послуг.

Атаки на критичні інфраструктурні системи, такі як енергетичні мережі, транспортні системи або системи водопостачання, можуть мати серйозні наслідки для безпеки та здоров'я громадян, економіки та суспільства в цілому.

Кібератаки можуть призвести до втрати довіри споживачів, партнерів або інших стейкхолдерів через недостатню захищеність даних, перерви в обслуговуванні або інші проблеми.

Урахування цих факторів дозволяє краще зрозуміти залежність інформаційних об'єктів захисту від типу потенційних загроз та розробити ефективні заходи для їх захисту в контексті критичної інфраструктури.

Аналіз залежності інформаційних об'єктів захисту від типу потенційних загроз у контексті критичної інфраструктури демонструє важливість ретельного розуміння характеристик загроз та уразливостей систем. Розглядаючи різноманітні фактори, такі як типи загроз, ступінь захищеності об'єктів, їх значення для функціонування інфраструктури та можливі наслідки атак, можна краще зрозуміти ризики та розробити ефективні стратегії захисту. Цей аналіз дозволяє ідентифікувати найбільш критичні точки у системах та встановити пріоритети для впровадження заходів забезпечення безпеки. Врахування цих аспектів сприяє збільшенню стійкості критичної інфраструктури до кіберзагроз і забезпечує надійність її функціонування в умовах постійно змінюючогося кіберландшафту.

Висновки до розділу 1

Аналіз наукової літератури показав, що кібербезпека об'єктів критичної інфраструктури стає все більш актуальною та важливою в сучасному цифровому світі, де залежність від технологій надзвичайно велика. Від енергетичних мереж та транспортних систем до фінансових установ та медичних установ, критична інфраструктура є основним фундаментом суспільства, а її безпека стає пріоритетом для забезпечення стабільності та безпеки. Однак, критична інфраструктура також стає об'єктом постійної загрози кібератак. Зловмисники постійно шукають вразливості, щоб отримати доступ до систем, викликати відмови, викрасти конфіденційні дані або нанести інші види шкоди. Тому розуміння, аналіз та захист критичної інфраструктури від кіберзагроз стає надзвичайно важливим завданням для організацій та урядів.

За результатами аналізу встановлено, що для забезпечення ефективного захисту критичної інфраструктури необхідно вживати комплексних заходів, які включають в себе нормативно-правове забезпечення, створення стандартів та

норм, механізми контролю та відповідальності, а також міжнародне співробітництво. Необхідно проводити аналіз тенденцій розвитку кіберзагроз, вивчати нові методи атак та розвивати стратегії прогнозування майбутніх загроз. Важливо також враховувати значення об'єктів для функціонування інфраструктури та їхню ступінь доступності для атак. Знання цих факторів допомагає визначити пріоритети у захисті та готовності до реагування на потенційні загрози. Це вимагає співпраці між різними стейкхолдерами, постійного моніторингу нових технологій та трендів, а також глибокого розуміння геополітичного контексту. Тільки через такий підхід можна забезпечити стійкість та надійність критичної інфраструктури в умовах постійної кіберзагрози.

Розділ 2 РОЗРОБЛЕННЯ МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

2.1 Аналіз та оцінка ризиків кібербезпеки

Для оцінки ризику необхідно визначити саме поняття ризику та його компонентів. Ризик кібербезпеки - це потенційна можливість зазнати шкоди або збитків внаслідок кібератаки або витоку даних вашої організації. Він передбачає виявлення потенційних загроз і вразливостей у цифрових системах і мережах організації. Ризик визначається вдома ключовими елементами: імовірність та вплив.

Імовірність – це ймовірність того, що подія загрози використає вразливість, притаманну активу або системі. На цю ймовірність впливають різні фактори, в тому числі можливість виявлення, використання та відтворюваність. Можливість виявлення стосується того, наскільки легко вразливість може бути виявлена або на неї можуть натрапити потенційні суб'єкти загрози. Можливість використання стосується ступеня, до якого вразливість може бути використана зловмисниками для виконання зловмисних дій. Відтворюваність пов'язана з постійністю, з якою вразливість може бути використана за схожих умов [19].

Вплив означає величину шкоди, що виникає в результаті успішного використання вразливості в результаті загрозливої події. Ця шкода може проявлятися на різних рівнях – від національного до індивідуального. Розуміння потенційного впливу порушення кібербезпеки має вирішальне значення для організацій, щоб оцінити серйозність можливих наслідків і відповідно визначити пріоритети для їх пом'якшення.

Якщо заглибитися глибше, то подія загрози охоплює будь-яку подію, коли суб'єкт загрози, використовуючи вектор загрози, взаємодіє з активом у спосіб, що становить потенційну загрозу. Ці події характеризуються тактикою, методами і процедурами (TTPs), що застосовуються суб'єктами загрози. І

навпаки, вразливість – це слабке місце в конструкції, впровадженні чи експлуатації активу або у внутрішньому контролі процесу.

Комплексна оцінка кожного з цих компонентів дозволяє організаціям отримати цілісне розуміння ризиків кібербезпеки та розробити надійні стратегії для зменшення потенційних загроз. Проактивно усуваючи вразливості та враховуючи потенційні наслідки загрозливих подій, організації можуть посилити свій захист кібербезпеки та захистити свої активи, дані та операції від зловмисників.

В оцінці ризиків кібербезпеки ключову роль відіграють два основні елементи: події загрози та вразливості.

Події загрози – ці події пов'язані з суб'єктом загрози, який використовує вектор загрози, взаємодіючи з активом у спосіб, що створює потенційний ризик. Ці події можуть варіюватися від спроб вторгнення в мережу до атак соціальної інженерії, спрямованих на маніпулювання людьми з метою розкриття конфіденційної інформації. Розуміння природи та складності загрозливих подій має вирішальне значення для організацій, щоб передбачити потенційні ризики та відповідним чином зміцнити свій захист.

Вразливості – вразливості - це слабкі місця в розробці, впровадженні або функціонуванні активу або у внутрішніх засобах контролю процесу. Виявлення вразливостей має важливе значення для розуміння того, де можуть статися потенційні порушення або компрометації. Ці слабкі місця можуть виникати з різних джерел, включаючи помилки в програмному забезпеченні, неправильні конфігурації або неадекватні протоколи безпеки. Проактивно виявляючи та усуваючи вразливі місця, організації можуть зменшити вразливість до потенційних загроз та підвищити свою стійкість до кібератак [20].

Комплексна оцінка ризиків кібербезпеки передбачає розуміння та оцінку як загрозливих подій, так і вразливостей. Оцінюючи ймовірність загрозливих подій, що використовують вразливості, та враховуючи наслідки, організації можуть розробити надійні стратегії для зменшення потенційних ризиків та посилення загальної захищеності від кібератак. Такий проактивний підхід

дозволяє організаціям випереджати нові загрози і захищати свої активи, дані та операції від зловмисників.

Встановлення рівня допустимого ризику є обов'язковим для організацій, щоб ефективно управляти потенційними ризиками та орієнтуватися на них відповідно до своїх бізнес-цілей. Рівень прийнятного ризику забезпечує основу для прийняття рішень та розподілу ресурсів в організації.

Визначаючи толерантність до ризику, керівництво повинно сформулювати чіткі вказівки та межі щодо типів і рівнів ризику, які організація готова прийняти. Чітко визначена система толерантності до ризиків повинна охоплювати кілька ключових елементів:

1. *Очікування щодо реагування на ризики* – передбачає окреслення очікувань щодо того, як різні типи ризиків повинні розглядатися та управлятися в організації. Це може включати стратегії пом'якшення ризиків у сферах з високим рівнем ризику, передачу певних ризиків через страхування або контракти, або прийняття та моніторинг ризиків у межах прийнятних порогових значень.

2. *Прийняття ризиків* – рівень прийнятності ризиків також передбачає визначення того, до якої міри організація готова приймати певні ризики для досягнення своїх цілей. Це може включати оцінку потенційних можливостей та їх порівняння з пов'язаними з ними ризиками, щоб визначити, чи виправдовує потенційна винагорода рівень ризику.

3. *Межі та порогові значення* – чітке визначення меж та порогових значень прийнятних ризиків має важливе значення для забезпечення того, щоб рівень ризику залишався в межах керованості. Ці межі можуть включати максимально прийнятні рівні фінансових втрат, операційних збоїв, шкоди репутації або невідповідності нормативним вимогам. Встановлюючи ці порогові значення, керівництво може проактивно виявляти та вирішувати ситуації, в яких рівень ризику перевищує прийнятні межі (табл.2.1) [21].

Встановивши чітко визначену систему прийняття ризиків, керівництво може забезпечити ясність і вказівки працівникам і зацікавленим сторонам щодо

прийнятних рівнів ризику в організації. Це дозволяє приймати більш обґрунтовані рішення, сприяє ефективному управлінню ризиками і, зрештою, сприяє досягненню бізнес-цілей, захищаючи при цьому інтереси організації.

Таблиця 2.1

Рівень допустимості ризиків

Рівень ризику	Опис рівня допустимості
Низький	Ризики, віднесені до категорії низьких, можуть бути прийняті, якщо немає можливості легко та економічно ефективно впровадити негайні стратегії лікування. Періодичний моніторинг необхідний для того, щоб забезпечити виявлення будь-яких змін в обставинах та належне реагування на них.
Середній	Ризики, класифіковані як середні, являють собою рівень ризику, з яким можна погодитися, якщо не можна легко та економічно ефективно впровадити негайні стратегії лікування. Необхідний регулярний моніторинг, щоб забезпечити виявлення будь-яких змін в обставинах та вжиття відповідних заходів.
Середньо-Високий	Ризики, що належать до категорії середньо-високих, вимагають негайної уваги. Стратегії лікування, спрямовані на зниження рівня ризику, вимагають дещо більшого часу. Хоча ці ризики не такі серйозні, як сценарії з високим рівнем ризику, вони все одно становлять значну загрозу для організації, і їх необхідно негайно усунути, щоб запобігти несприятливим наслідкам.
Високий	Ризики, віднесені до категорії високих, вважаються неприйнятними. Стратегії реагування, спрямовані на зменшення їхнього впливу, повинні бути розроблені та впроваджені протягом відносно короткого періоду часу. Ці стратегії можуть включати проактивні заходи для пом'якшення або мінімізації впливу ризиків, такі як впровадження додаткових протоколів безпеки або перерозподіл ресурсів для усунення вразливостей.
Дуже високий	Ризики, класифіковані як дуже високі, означають неминучу загрозу серйозного впливу. Необхідно вжити негайних заходів, щоб або припинити відповідну діяльність, або невідкладно впровадити стратегії пом'якшення чи передачі ризиків. Якщо ці ризики не будуть вчасно усунуті, це може призвести до значної шкоди цілям, активам або зацікавленим сторонам організації.

Оцінка ризиків полягає у виявленні ризиків, характерних для навколишнього середовища, та визначенні рівня виявлених ризиків. Основними етапами оцінки ризиків є ідентифікація ризиків, аналіз ризиків та оцінка ризиків (рис.2.1).

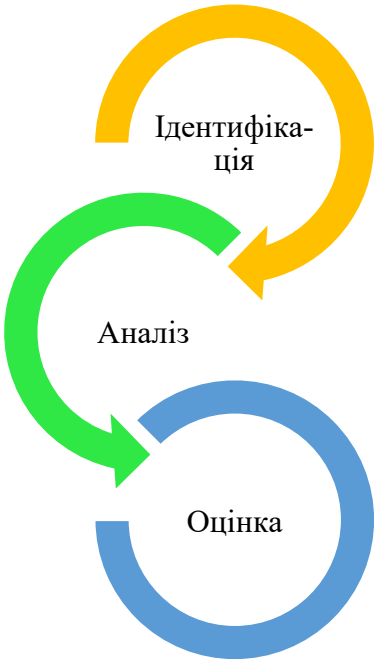

Рис. 2.1 Процес оцінки ризиків

Перший етап оцінки ризиків – ідентифікація ризиків, який включає кілька важливих завдань, спрямованих на розуміння та каталогізацію активів у системі, виявлення потенційних загроз та побудову реалістичних сценаріїв ризиків [22].

Перше завдання, ідентифікація активів, фокусується на створенні всеосяжної інвентаризації всіх фізичних і логічних активів, що входять до сфери оцінки ризиків. Ця інвентаризація включає всі критичні активи, які мають важливе значення для досягнення бізнес-цілей і є основними цілями для зловмисників. Сюди також входять ресурси, які зловмисники можуть використати для проникнення в різні сегменти мережі, щоб дістатися до активів. Після завершення інвентаризації активів необхідно створити діаграму мережевої архітектури. Ця діаграма візуально відображає взаємозв'язок і шляхи комунікації між активами, визначаючи всі точки входу в систему, або вектори атаки, а також місця розташування елементів системи. Таке візуальне представлення має вирішальне значення для наступного кроку ідентифікації загроз.

Друге завдання, моделювання загроз, передбачає використання інвентаризаційного списку активів і діаграми мережевої архітектури для визначення потенційних загрозливих подій, які можуть використати вразливості

кожного активу. Моделювання загроз - це структурований процес, який допомагає організаціям ідентифікувати відповідні події загроз і будувати цілеспрямований захист. Цей процес починається з визначення сфери застосування та декомпозиції системи, які були розпочаті під час виконання завдання з ідентифікації активів [23]. Далі організації повинні систематично виявляти можливі події, в яких зловмисники можуть скомпрометувати активи. Після ідентифікації загроз моделювання атак пов'язує ці події в потенційні послідовності атак, описуючи, як зловмисник може підійти до вторгнення. Це допомагає організаціям визначити необхідні засоби контролю для захисту системи та визначити пріоритетність їх впровадження.

Останнє завдання, "Побудова сценаріїв ризиків", передбачає створення сценаріїв "що може піти не так", які забезпечують реалістичне і достовірне уявлення про ризики на основі бізнес-контексту, системного середовища і відповідних загроз. Добре розроблені сценарії ризиків полегшують комунікацію із зацікавленими сторонами і дозволяють проводити структурований аналіз на наступних етапах. Кожен сценарій ризику повинен чітко формулювати чотири ключові елементи: актив, який є об'єктом цінності, визначеним у першому завданні; подія загрози, яка є подією атаки, визначеною в завданні моделювання загроз; вразливість, яка є слабким місцем в активі або допоміжних процесах, що може бути використана подією загрози; і наслідок, який є прямим результатом події загрози.

Крок 2 процесу оцінки ризиків - це аналіз ризиків, який передбачає вивчення елементів кожного сценарію ризику для визначення ймовірності реалізації сценарію та потенційного впливу в разі його реалізації [24].

Аналіз ризиків починається з визначення ймовірності кожного сценарію ризику. Фактори, які слід враховувати, включають можливість виявлення, яка вимірює, наскільки легко противник може знайти вразливість, на що впливає доступність інформації та вразливість активу; можливість експлуатації, яка оцінює, наскільки легко вразливість може бути використана, враховуючи права доступу, складність інструментів і необхідні технічні навички; і відтворюваність,

яка оцінює, наскільки легко атака може бути повторена, залежно від складності атаки і умов навколишнього середовища.

Наступним завданням аналізу ризиків є визначення впливу кожного ризикового сценарію. Реалізація ризикового сценарію може поставити під загрозу конфіденційність, цілісність та доступність активів.

Оцінювання ризику – 3-ій крок. Цей етап передбачає визначення та розуміння значущості кожного рівня ризику. Процес включає визначення та встановлення пріоритетності ризиків, а також їх документування для ефективної комунікації та управління ними [25].

Визначення та пріоритизація ризиків. Оцінка ризиків починається з визначення та встановлення пріоритетності виявлених ризиків. Як описано в попередніх розділах, ризик - це функція ймовірності того, що певна подія загрози використає потенційну вразливість активу і спричинить відповідні наслідки. Цей взаємозв'язок можна візуалізувати за допомогою матриці ризиків, наприклад, матриці 5 на 5, яка класифікує рівні ризиків на основі добутку оцінок "Ймовірність" і "Вплив", визначених на етапі аналізу ризиків. Для кожного сценарію ризику порівняйте отриманий рівень ризику з визначеним рівнем толерантності до ризику, встановленим організацією. Сценарії ризиків, рівні яких перевищують поріг толерантності, повинні бути пріоритетними для обробки з метою приведення їх у прийнятні межі (рис. 2.2). При визначенні пріоритетності ризиків також важливо встановити очікувану тривалість впровадження заходів щодо їх зниження.

Рис. 2.2 Матриця ризиків

Документування ризиків. Ефективне управління ризиками вимагає ретельного документування. Результати ідентифікації, аналізу та оцінки ризиків повинні бути чітко зафіксовані в Реєстрі ризиків, який слугує важливим інструментом комунікації для зацікавлених сторін. Реєстр ризиків - це динамічний документ, який слід регулярно переглядати та оновлювати, щоб забезпечити точний та актуальний огляд ризиків кібербезпеки організації. Він повинен містити наступну інформацію:

– сценарій ризику – детальний опис того, як подія загрози може використати потенційну вразливість активу для спричинення негативних наслідків.

– дата ідентифікації – дата, коли було виявлено сценарій ризику.

– існуючі заходи – поточні засоби контролю та заходи, що застосовуються для реагування на сценарій ризику.

– поточний ризик – оцінений рівень ризику, враховуючи існуючі заходи (невід'ємний ризик із застосованими поточними засобами контролю).

– план лікування – заплановані заходи та терміни для зниження ризику до прийнятного рівня в межах толерантності організації до ризику.

– статус виконання – поточний стан виконання плану лікування.

– залишковий ризик – оцінений рівень ризику після впровадження плану лікування (поточний ризик із застосуванням додаткових заходів).

– власник ризику – особа або група осіб, відповідальна за те, щоб залишкові ризики залишалися в межах прийнятого в організації рівня толерантності.

2.2 Методи реагування на ризики кібербезпеки

Існує чотири основні варіанти реагування на ризики, які організації можуть розглянути: прийняти, уникнути, передати та пом'якшити. Кожен варіант передбачає різний підхід до управління виявленими ризиками.

Прийняття ризику передбачає визнання та прийняття ризику без вжиття додаткових заходів для його зменшення. Цей варіант підходить, коли ризик не виходить за межі толерантності організації. Прийняття означає, що організація готова мати справу з потенційними наслідками ризику, оскільки витрати або зусилля, необхідні для його зменшення, можуть бути не виправдані очікуваними вигодами. По суті, це означає зважене рішення про те, що потенційний вплив ризику є керованим в рамках існуючої операційної структури, а будь-які подальші зусилля зі зниження ризику будуть непропорційними отриманим вигодам [26].

Уникнення ризику, з іншого боку, тягне за собою припинення будь-яких дій або видів діяльності, які наражають організацію на ідентифікований ризик. Хоча такий підхід може здатися екстремальним, він може бути найрозумнішим, якщо потенційний ризик значно переважає переваги. Уникаючи ризику повністю, організація гарантує, що ймовірність настання несприятливої події відсутня. Наприклад, організація може відмовитися від проведення платіжних операцій в Інтернеті, щоб повністю уникнути ризику перехоплення цих операцій зловмисниками для шахрайських цілей. Це означає відмову від певних видів діяльності задля підтримки безпеки та стабільності.

Передача ризику передбачає розподіл тягаря ризику з іншою стороною, що зменшує потенційний вплив на організацію. Це можна зробити шляхом придбання страховки або передачі певних операцій на аутсорсинг. Передаючи ризик, організація перекладає частину потенційних наслідків на зовнішню структуру, яка краще підготовлена до їх подолання. Наприклад, придбання кіберстрахування перекладає фінансові наслідки потенційних кіберінцидентів на страхову компанію, тоді як аутсорсинг IT-послуг може передати операційні ризики сторонньому експерту.

Пом'якшення ризиків фокусується на зниженні рівня ризику за допомогою різних заходів, таких як розгортання засобів контролю безпеки та впровадження найкращих практик. Цей підхід має на меті зменшити або ймовірність настання ризику, або його вплив, якщо він все ж таки відбудеться. Наприклад,

впровадження брандмауера може значно зменшити ризик несанкціонованого доступу шляхом обмеження мережевого трафіку. Шляхом пом'якшення організація активно працює над тим, щоб знизити ризик до прийнятного рівня, забезпечуючи його відповідність своїй стратегії толерантності до ризиків та управління ними [27].

Вибір відповідних заходів реагування на ризики має вирішальне значення для ефективного управління ризиками. Багато організацій за замовчуванням намагаються зменшити ризики, інвестуючи в дорогі засоби контролю безпеки та технічні рішення. Однак важливо також розглядати уникнення та передачу ризиків як потенційно більш економічно ефективні альтернативи. Наприклад, щоб зменшити ризик компрометації системи, коли співробітники отримують доступ до шкідливих веб-сайтів, організація може повністю вимкнути можливості інтернет-серфінгу замість того, щоб розгортати дорогі профілактичні рішення для кінцевих точок. Такий підхід дозволяє ефективно уникнути ризику, а не намагатися контролювати його за допомогою дорогих технологій.

Коли організації вирішують боротися з ризиками шляхом їх зменшення, вкрай важливо, щоб засоби контролю безпеки були релевантними та відповідними до конкретних ризиків, яким вони протидіють. Ефективне зниження ризиків означає, що обрані засоби контролю повинні або зменшити ймовірність виникнення ризику, або зменшити потенційний вплив, якщо ризик все ж таки матеріалізується. Наприклад, впровадження брандмауера для обмеження несанкціонованого доступу до мережі безпосередньо впливає на ризик, зменшуючи ймовірність того, що несанкціоновані особи можуть зламати систему. Аналогічно, шифрування даних зменшує вплив витоку даних, гарантуючи, що викрадені дані залишаються нечитабельними без ключа розшифровки.

Організації повинні критично оцінювати характер ризиків, з якими вони стикаються, і розглядати весь спектр варіантів реагування на ризики. Уникнення та передача даних іноді можуть бути більш ефективними та економічно

вигідними, ніж пом'якшення наслідків. Уникнення ризику може передбачати припинення певних видів діяльності, які несуть ризик, таким чином усуваючи можливість його виникнення. Передача ризику, з іншого боку, передбачає перенесення ризику на іншу сторону, наприклад, шляхом придбання страховки або передачі певних функцій на аутсорсинг. Обидві стратегії можуть бути високоефективними в управлінні ризиками без потреби в розгалуженому і дорогому внутрішньому контролі [28].

Зрештою, рішення про те, які заходи реагування на ризики слід вжити, має бути узгоджене із загальною толерантністю організації до ризиків та її стратегічними цілями. Вище керівництво має бути залучено до процесу прийняття рішень, щоб гарантувати, що всі дії з реагування на ризики будуть належним чином оцінені та санкціоновані. Розглядаючи всі доступні варіанти реагування на ризики - уникнення, передача та пом'якшення - організації можуть розробити збалансований та економічно ефективний підхід до управління ризиками, гарантуючи, що ресурси розподіляються ефективно і що організація залишається стійкою до потенційних загроз.

2.3 Процес розробки системи моніторингу та аналізу подій в кібербезпеці

Моніторинг кібербезпеки як процес складається з чотирьох ключових етапів: ідентифікація, підготовка, виконання та аналіз. Цей комплексний підхід передбачає визначення цілей моніторингу, вибір відповідних інструментів, розробку відповідної політики, розгортання необхідної інфраструктури моніторингу, підготовку персоналу та аналіз прогресу у виявленні загроз (рис. 2.3.).

Визначення цілей безпеки для конкретних ризиків має важливе значення для розробки надійної стратегії кібербезпеки. Хоча деякі організації схильні застосувати швидкі рішення, більш структурований і комплексний підхід часто виявляється більш вигідним у довгостроковій перспективі.

Рис. 2.3. Кроки впровадження системи моніторингу

Потреби організації в безпеці можуть сильно відрізнятися залежно від характеру її активів з високим рівнем ризику та конкретних пріоритетів безпеки. Саме тут встановлення цілей безпеки, орієнтованих на ризики, набуває вирішального значення [29].

Першим кроком у визначенні цих цілей є ретельна оцінка поточного ландшафту загроз. Це означає визначення типів загроз, з якими стикається організація, розуміння методів і тактик, що застосовуються потенційними зловмисниками, а також розпізнавання вразливостей в існуючих системах і процесах організації. Отримавши детальне розуміння середовища загроз, організація може краще підготуватися до потенційних інцидентів безпеки та реагувати на них.

Далі важливо узгодити цілі безпеки з загальними стратегічними задачами організації. Заходи безпеки повинні підтримувати загальну місію та стратегічні цілі підприємства, а не діяти ізольовано. Таке узгодження гарантує, що ініціативи з безпеки сприятимуть успіху організації, а ресурси ефективно розподілятимуться на найбільш пріоритетні напрямки [30].

Ще одним важливим елементом є сприяння співпраці між різними зацікавленими сторонами. Кібербезпека - це не лише відповідальність IT-відділу; вона вимагає внеску і співпраці з боку різних підрозділів організації, в тому числі

керівництва, юридичного та операційного відділів. Залучаючи різні точки зору, організація може розробити більш комплексну та ефективну стратегію безпеки.

Оцінка ризиків є важливою практикою в цьому процесі. Оцінюючи ризики за ступенем їхньої критичності, організація може визначити пріоритети у своїх зусиллях з безпеки. Це передбачає оцінку потенційного впливу різних ризиків та ймовірності їх виникнення, що дозволяє організації зосередитися на зменшенні найбільш значущих загроз у першу чергу [31].

Крім того, життєво важливим є встановлення цілей безпеки, які можна виміряти. Ці цілі повинні бути конкретними, досяжними і кількісно вимірюваними, забезпечуючи чіткі орієнтири для досягнення успіху. Встановивши конкретні цілі, організація може відстежувати свій прогрес у часі і за необхідності коригувати свої стратегії для забезпечення постійного вдосконалення.

Вибір і перевірка правильних інструментів є важливим кроком у зміцненні зусиль з моніторингу кібербезпеки. Існує безліч інструментів для підтримки цих зусиль, включаючи засоби управління інформацією та подіями безпеки (SIEM), системи виявлення вторгнень (IDS), інструменти для аналізу мережевого трафіку та системи виявлення кінцевих точок. Вибір відповідних інструментів вимагає глибокого розуміння конкретних потреб вашої організації та основних ризиків, з якими ви стикаєтеся [32].

Щоб забезпечити сумісність з конкретними потребами організації, необхідно ретельно оцінити особливості та функціональні можливості кожного інструменту. Важливо, щоб обрані інструменти ефективно протидіяли виявленим ризикам і надавали можливості, необхідні для моніторингу та захисту ваших критично важливих активів. Слід врахувати конкретні виклики, з якими стикається організація, наприклад, тип даних, з якими вона працює, складність мережі та регуляторні вимоги, яким вона повинна відповідати.

Міркування щодо бюджету також мають вирішальне значення. Слід розрахувати реальну ефективність інвестицій, порівнюючи вартість інструментів з потенційною економією від запобігання інцидентам безпеки.

Інтеграція з іншими внутрішніми інструментами кібербезпеки є ще одним ключовим фактором. Щоб забезпечити швидке налаштування та розгортання, варто шукати рішення, які можна легко інтегрувати з існуючими системами. Така сумісність життєво важлива для створення цілісної та ефективної системи кібербезпеки, в якій різні інструменти можуть працювати разом для забезпечення комплексного захисту [33].

Ще одним важливим фактором є зручність використання. Необхідно перевірити зручність навігації та користувацького інтерфейсу інструментів, щоб переконатися, що ваша команда може ефективно використовувати їх без тривалого навчання. Інтуїтивно зрозумілі інструменти не лише підвищують продуктивність, але й зменшують ймовірність помилок користувачів, які можуть поставити під загрозу безпеку.

Зрештою, варто звернути увагу на ринкову репутацію постачальників. Щоб оцінити надійність та ефективність інструментів, слід ознайомитися з оглядами та відгуками інших користувачів. Сильна ринкова репутація може бути показником продуктивності інструменту та відданості постачальника підтримці клієнтів.

Визначення політики та процедур моніторингу кібербезпеки має вирішальне значення для встановлення чіткого та ефективного стратегічного напрямку. Комплексна політика моніторингу кібербезпеки діє як стратегічний компас, що спрямовує дії та рішення команди. Вона повинна включати мету та сферу застосування політики, чітко визначаючи її цілі та масштаби її застосування. Цілі моніторингу повинні бути сформульовані таким чином, щоб вони відповідали загальним цілям організації у сфері безпеки, і щоб усі заходи сприяли досягненню цих цілей [34].

Політика повинна детально описувати конкретні методики та засоби, які будуть використовуватися в процесі моніторингу. Сюди входить опис типів моніторингу, які необхідно проводити, засобів та технологій, які необхідно застосовувати, а також процесів збору та аналізу даних. Ролі та обов'язки мають бути чітко визначені, щоб забезпечити підзвітність і ясність серед членів

команди. Обов'язки та рівні повноважень кожної особи мають бути визначені, що допоможе впорядкувати роботу та зменшити кількість двозначностей.

Визначення політики та процедур моніторингу кібербезпеки має вирішальне значення для встановлення чіткого та ефективного стратегічного напрямку. Комплексна політика моніторингу кібербезпеки діє як стратегічний компас, що спрямовує дії та рішення команди. Вона повинна включати мету та сферу застосування політики, чітко визначаючи її цілі та масштаби її застосування. Цілі моніторингу повинні бути сформульовані таким чином, щоб вони відповідали загальним цілям організації у сфері безпеки, і щоб усі заходи сприяли досягненню цих цілей [35].

Політика повинна детально описувати конкретні методики та засоби, які будуть використовуватися в процесі моніторингу. Сюди входить опис типів моніторингу, які необхідно проводити, засобів та технологій, які необхідно застосовувати, а також процесів збору та аналізу даних. Ролі та обов'язки мають бути чітко визначені, щоб забезпечити підзвітність і ясність серед членів команди. Обов'язки та рівні повноважень кожної особи мають бути визначені, що допоможе впорядкувати роботу та зменшити кількість двозначностей.

Навчання є критично важливим компонентом, який гарантує, що всі члени команди будуть належним чином підготовлені до впровадження та дотримання політики моніторингу. Слід запланувати регулярні тренінги, щоб команда була в курсі нових інструментів, процедур і загроз, що з'являються. Політика також має передбачати заходи примусу та наслідки порушень для підтримання дисципліни та забезпечення дотримання вимог [36].

Комунікаційний план має важливе значення для ефективного поширення політики. Цей план повинен детально описувати, як політика буде доведена до відома всіх зацікавлених сторін, а також включати механізми звітування та розгляду будь-яких винятків. Для надання всебічної підтримки та забезпечення послідовності у впровадженні слід додати допоміжну документацію, таку як інструкції, посібники та довідкові матеріали.

Розгортання інфраструктури моніторингу є наступним кроком на етапі підготовки. Це передбачає налаштування параметрів підключення до серверів, створення конфігурацій і створення механізмів резервного копіювання для забезпечення безперебійної роботи інструментів моніторингу кібербезпеки. Інфраструктура повинна підтримувати всі зусилля з впровадження і бути достатньо надійною, щоб впоратися з робочим навантаженням моніторингу. Періодичне тестування та оновлення необхідні для підтримки ефективності інфраструктури та адаптації до будь-яких змін у безпековому ландшафті.

Регулярний аналіз та адаптація мають вирішальне значення для підтримання та посилення захисту кібербезпеки. Досвід реагування на інциденти дає цінні відомості, які можуть покращити майбутні стратегії безпеки. Зворотний зв'язок від зацікавлених сторін, включаючи співробітників, керівництво та зовнішніх партнерів, може висвітлити сфери, що потребують вдосконалення, і допомогти точно налаштувати заходи безпеки. Спостереження команд спостереження дають практичну інформацію про те, наскільки добре працюють політики та процедури безпеки в режимі реального часу [37].

Також важливо враховувати галузеві тенденції та нові моделі загроз при перегляді та оновленні практик безпеки. Кіберзагрози постійно розвиваються, і щоб залишатися на крок попереду, потрібен динамічний підхід. Документування цих знань і висновків у вигляді всеосяжного звіту є надійним джерелом інформації для організації, гарантуючи, що найкращі практики будуть зафіксовані і легко доступні для використання в майбутньому.

2.4 Модель управління ризиками кібербезпеки критичної інфраструктури

Будь-яка модель управління ризиками кібербезпеки (рис.2.4)повинна включати входи, залежності, які обробляють ці входи, та виходи або результати. Створення моделі управління ризиками кібербезпеки об’єктів критичної

інфраструктури починається з визначення вхідних даних, які включають параметри, що впливають на ризики.

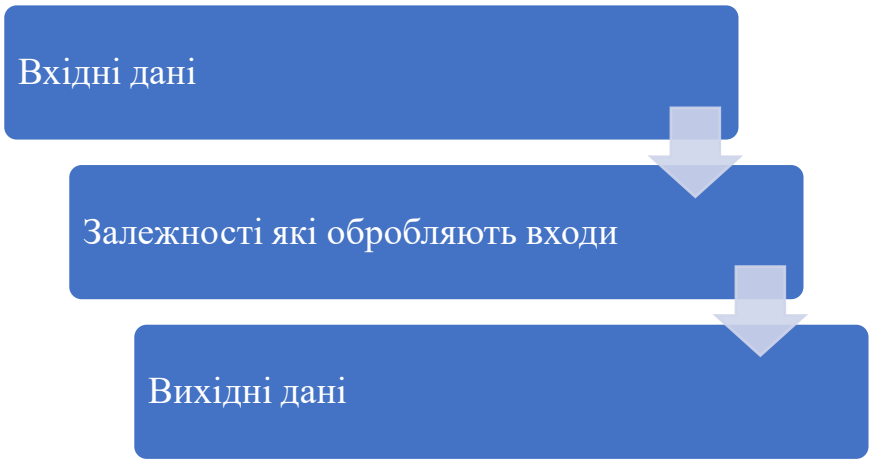

Рис. 2.4. Структура моделі

Далі необхідно визначити залежності, тобто взаємозв'язки між цими входами, що дозволяють обробляти інформацію та здійснювати точні розрахунки. Залежності визначають, як різні параметри впливають один на одного та на загальний рівень ризику. Нарешті, модель повинна мати виходи, які є результатами, що включають оцінки рівня ризику та рекомендації щодо його зменшення. Такі результати дозволяють зробити висновки про ефективність поточних заходів безпеки та розробити стратегії для покращення кібербезпеки критичної інфраструктури.

Вхідні дані (Inputs)

1. **Активи**:
   - Вартість активів
   - Критичність активів (пропозиція – від 0 до 1)
2. **Загрози**:
   - Типи загроз (наприклад, DDoS, фішинг, вразливості ПЗ)
   - Ймовірність виникнення загроз
3. **Уразливості**:
   - Кількість вразливостей
   - Стан системи оновлень та патчів

4. **Контрзаходи**:
   - Наявність систем виявлення вторгнень (IDS)
   - Наявність систем запобігання вторгнень (IPS)
   - Політики безпеки
5. **Фактори впливу (Impact)**:
   - Потенційні фінансові збитки
   - Вплив на репутацію
   - Вплив на операційні процеси
6. **Інциденти**:
   - Історичні дані про інциденти
   - Час реагування на інциденти

Залежності (Dependencies)

1. **Ймовірність атаки (Probability of Attack)**:
   - Залежить від типів загроз та їхньої ймовірності.
   - Впливає на ймовірність виникнення інцидентів.

$$P_A = 1 - \prod_{i=1}^{n}(1 - P_{T_i}) \quad , \tag{1}$$

де $\boldsymbol{P}_{\text{A}}$ – ймовірність атаки (безрозмірна величина, від 0 до 1);
$\boldsymbol{P}_{\text{Ti}}$ – ймовірність окремої загрози (безрозмірна величина, від 0 до 1)

2. **Вразливість системи (System Vulnerability)**:

$$V = \frac{Critical\ Vulnerabilities}{Total\ Vulnerabilities} \quad , \tag{2}$$

де V - вразливість системи (безрозмірна величина, від 0 до 1);
Critical Vulnerabilities - кількість критичних уразливостей (шт.);
Total Vulnerabilities - загальна кількість уразливостей (шт.)

3. **Ефективність контрзаходів (Effectiveness of Countermeasures)**:

$$E = \frac{Detected\ Incident}{Total\ Incidents} \quad , \tag{3}$$

де E - ефективність контрзаходів (безрозмірна величина, від 0 до 1);

Detected Incidents - кількість виявлених інцидентів (шт.);
Total Incidents - загальна кількість інцидентів (шт.).

4. **Вплив інциденту (Impact of Incident)**:

$$I = Asset\ Criticality \times Financial\ Impact\ , \qquad (4)$$

де I - вплив інциденту (USD);
Asset CriticalityAsset Criticality - критичність активів (безрозмірна величина, від 0 до 1);
Financial ImpactFinancial Impact - фінансовий вплив (USD)

Виходи (Outputs)

1. **Рівень ризику (Risk Level)**:
   - Визначається як функція ймовірності атаки та впливу інциденту за формулою

$$R = P_{attack} \times V \times I, \qquad (5)$$

де R - рівень ризику (USD)
Pattack - ймовірність атаки (безрозмірна величина, від 0 до 1)
V - вразливість системи (безрозмірна величина, від 0 до 1)
I - вплив інциденту (USD)

Рівень ризику розраховується для кожного активу та для системи в цілому.

2. **Рекомендації щодо зменшення ризиків (Risk Mitigation Recommendations)**:
   - пропозиції щодо покращення контрзаходів;
   - пропозиції щодо зменшення вразливостей.
3. **План реагування на інциденти (Incident Response Plan)**:
   - дії для швидкого реагування на інциденти;
   - протоколи для зменшення впливу інцидентів.
4. **Оцінка ефективності безпеки (Security Effectiveness Assessment)**:

- оцінка поточного стану кібербезпеки.
- визначення областей, що потребують покращення

Тепер розглянемо на практиці сценарій моделювання

Вхідні дані (Inputs)

1. **Активи:**
   - вартість активів: $2,000,000
   - критичність активів: 0.9 (де 1 - найвища критичність)
2. **Загрози:**
   - типи загроз: Ransomware, SQL Injection
   - ймовірність виникнення загроз:
     - Ransomware: 25%
     - SQL Injection: 10%
3. **Уразливості:**
   - кількість уразливостей: 8
   - стан системи оновлень та патчів: Встановлення патчів раз на місяць
4. **Контрзаходи:**
   - наявність систем виявлення вторгнень (IDS): Так
   - наявність систем запобігання вторгнень (IPS): Так
   - політики безпеки: Оновлення політик щомісяця
5. **Фактори впливу (Impact):**
   - потенційні фінансові збитки: $500,000
   - вплив на репутацію: Високий
   - вплив на операційні процеси: Середній
6. **Інциденти:**
   - історичні дані про інциденти: 5 інцидентів на рік
   - час реагування на інциденти: 3 години

Залежності (Dependencies)

1. **Ймовірність атаки (Probability of Attack):**

$$P_{attack} = 1 - (1 - 0.25) \times (1 - 0.10) = 1 - 0.75 \times 0.90 = 1 - 0{,}675 = 0.325$$

2. **Вразливість системи (System Vulnerability)**:

$$V = \frac{4}{8} = 0.5$$

3. **Ефективність контрзаходів (Effectiveness of Countermeasures)**:

$$E = \frac{4}{5} = 0.8$$

Таким чином, ефективність контрзаходів становить 0.8 або 80%.

4. **Вплив інциденту (Impact of Incident)**:

$$I = 0.9 \times 500000 = 450000$$

Виходи (Outputs)

5. **Рівень ризику (Risk Level)**:

$$R = 0.325 \times 0.5 \times 450000 = 73125$$

Висновки до розділу 2

Розділ присвячений розробленню моделі управління ризиками кібербезпеки, яка охоплює три ключові аспекти: аналіз та оцінку ризиків кібербезпеки, методи реагування на ці ризики, а також процес розробки системи моніторингу та аналізу подій в кібербезпеці.

Детально розглянуто методи та інструменти для аналізу і оцінки ризиків кібербезпеки. Розглядаються різні підходи до ідентифікації вразливостей інформаційних систем та оцінки потенційних загроз. Визначається значимість кожного ризику на основі ймовірності його виникнення та потенційного впливу на організацію. Це включає використання кількісних і якісних методів аналізу,

таких як моделі загроз, методи оцінки ризиків на основі даних про попередні інциденти, а також експертні оцінки.

Зосереджено увагу на розробці і впровадженні методів реагування на ризики кібербезпеки. Описуються різні стратегії управління ризиками, такі як уникнення, зменшення, передача та прийняття ризиків. Розглядаються сучасні технології та підходи до захисту інформаційних систем, включаючи засоби виявлення та запобігання вторгненням, системи управління інцидентами, а також механізми відновлення після інцидентів. Особлива увага приділяється автоматизації процесів реагування та використанню машинного навчання для покращення ефективності цих процесів.

Описано процес розробки системи моніторингу та аналізу подій в кібербезпеці. Визначаються ключові компоненти таких систем, зокрема, засоби збору, обробки та зберігання даних про події, а також аналітичні інструменти для виявлення аномалій та кореляції подій. Наголошується на важливості інтеграції систем моніторингу з іншими компонентами інформаційної безпеки та їх здатності до масштабування для обробки великих обсягів даних. Описуються кращі практики та стандарти для розробки ефективних систем моніторингу, а також методи оцінки їх продуктивності та надійності.

Узагальнюються основні підходи до управління ризиками кібербезпеки, пропонуються методології для оцінки та мінімізації цих ризиків, а також окреслюються процеси розробки та впровадження систем моніторингу, що є ключовими для забезпечення комплексного захисту інформаційних систем організацій.

Розділ 3 ВПРОВАДЖЕННЯ ТА ВДОСКОНАЛЕННЯ МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

3.1 Впровадження моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури

Управління ризиками кібербезпеки є центральним елементом захисту об’єктів критичної інфраструктури. Впровадження ефективної моделі управління ризиками дозволяє ідентифікувати потенційні загрози, оцінювати їхній вплив, розробляти та впроваджувати відповідні заходи захисту. Ця модель має бути динамічною та адаптивною, щоб відповідати постійно змінюваному ландшафту кіберзагроз.

Розглянемо цей процес на основі системи управління ризиками, що сгрупований в таблиці 3.1.:

Таблиця 3.1

Запропонована система управління ризиками

№	Тип ризиків	Ризики
1	Інформаційні	• Витік даних або шахрайські дії • Порушення доступу до критично важливих інформаційних систем • Проблеми захисту, що виникають внаслідок критичних інцидентів з боку третіх осіб, які впливають на діяльність підприємства
2	Ризики невідповідності	• Обробка персональної інформації невідповідно до правил конфіденційності даних • Дотримання вимог щодо реалізації та просування послуг, включаючи дотримання законодавства
3	Операційні	• Порушення обміну інформацією між організацією, постачальниками та споживачами • Порушення безперервності або стійкості діяльності • Проблеми з отриманням необхідних матеріалів та робочої сили
4	Стратегічні	• Втрата інтелектуальної власності та комерційної таємниці • Пошкодження репутації та втрата суспільної довіри • Довгострокові фінансові втрати через неефективні інвестиції в кібербезпеку

Метою впровадження є інтеграція заходів контролю в плани безпеки та конфіденційності для системи та організації. Це включає реалізацію необхідних заходів захисту, що забезпечують відповідність системи вимогам безпеки та конфіденційності. Ключовим аспектом цього процесу є детальне документування всіх аспектів впровадження заходів контролю в базовій конфігурації. Документування охоплює конкретні деталі реалізації, налаштування та взаємодії засобів контролю з іншими компонентами системи. Це забезпечує прозорість процесів, можливість подальшого аудиту та адміністрування, а також підвищує загальний рівень кібербезпеки організації [38].

Основними завданнями впровадження є контроль за процесом (Завдання 1) та оновлення інформації про реалізацію засобів (Завдання 2). Це включає моніторинг ефективності впроваджених заходів і своєчасне внесення коректівів у разі виявлення недоліків. Крім того, важливим є забезпечення постійного вдосконалення засобів контролю відповідно до нових загроз та змін у кіберпросторі.

Завданням 1 є впровадження засобів контролю, передбачених планами безпеки та конфіденційності, із застосуванням сучасних методологій інженерії безпеки та конфіденційності систем. Цей процес вимагає ретельного підходу, що охоплює всі етапи життєвого циклу розробки системи, починаючи від нової розробки або придбання, і закінчуючи впровадженням та оцінкою ефективності заходів. Основною метою є створення комплексного і надійного захисту, який відповідатиме вимогам безпеки та конфіденційності інформаційних систем і забезпечить їхню стійкість до можливих кіберзагроз [39].

Очікуваним результатом цього завдання є задокументування впроваджених засобів контролю у базовій конфігурації системи. Документування охоплює детальне описання всіх реалізованих заходів, їхніх параметрів, налаштувань та інтеграції з іншими компонентами системи. Це забезпечує не лише прозорість процесів, але й можливість подальшого аудиту та перевірки ефективності впроваджених рішень. Належна документація сприяє

кращому розумінню системи з боку всіх залучених фахівців та полегшує подальше адміністрування.

Основна відповідальність за виконання цього завдання покладається на власника системи та загального постачальника засобів контролю. Власник системи відповідає за загальне керівництво процесом та забезпечення відповідності заходів контролю вимогам організації. Загальний постачальник засобів контролю, в свою чергу, несе відповідальність за технічну реалізацію заходів безпеки та їхнє інтегрування в систему.

У реалізації завдання 1 також беруть участь допоміжні ролі, які забезпечують всебічний підхід до впровадження засобів контролю. Серед них власник інформації, архітектор безпеки, архітектор конфіденційності, інженер з безпеки систем та інженер з конфіденційності. Кожна з цих ролей має свої специфічні обов’язки, що включають аналіз ризиків, розробку та впровадження відповідних заходів захисту, а також забезпечення їхньої відповідності нормативним вимогам та стандартам [40].

Процес впровадження засобів контролю починається на етапі нової розробки або придбання системи. На цьому етапі визначаються вимоги до безпеки та конфіденційності, проводиться аналіз потенційних ризиків та загроз, а також розробляються плани захисту. Далі відбувається етап впровадження та оцінки, де засоби контролю інтегруються в систему, проводяться тести їхньої ефективності, і вносяться необхідні корективи для оптимізації захисту.

Впровадження засобів контролю вимагає використання передових методологій інженерії безпеки та конфіденційності. Це передбачає застосування системного підходу до проектування та реалізації заходів захисту, використання сучасних технологій та інструментів, а також дотримання найкращих практик у сфері кібербезпеки. Завдяки цьому забезпечується високий рівень захисту інформаційних систем, їхня відповідність нормативним вимогам та стійкість до кіберзагроз.

Таким чином, завдання 1 є ключовим елементом у забезпеченні кібербезпеки та конфіденційності інформаційних систем організації. Реалізація

цього завдання сприяє створенню надійного захисного середовища, яке здатне ефективно протистояти сучасним кіберзагрозам і забезпечувати збереження конфіденційності та цілісності інформаційних ресурсів. Успішне впровадження засобів контролю потребує координації зусиль усіх залучених фахівців, використання передових технологій та методологій, а також постійного моніторингу та вдосконалення заходів безпеки [41].

Завдання 2 передбачає задокументування змін до запланованого впровадження засобів контролю на основі фактичного стану впровадження. Це є важливим етапом у забезпеченні відповідності системи безпеки та конфіденційності поточним вимогам і стандартам. Оновлені плани безпеки та конфіденційності мають містити детальну інформацію про реалізацію впроваджених засобів контролю, що дозволяє експертам проводити об'єктивну оцінку їх ефективності. Основна відповідальність за виконання цього завдання покладається на власника системи та загального постачальника засобів контролю. Власник системи несе відповідальність за забезпечення того, щоб усі зміни, внесені до плану впровадження, були належним чином задокументовані та відповідали фактичному стану впровадження. Загальний постачальник засобів контролю відповідає за надання необхідних ресурсів та підтримки для успішного виконання цього завдання.

Допоміжні ролі включають ті самі допоміжні ролі, що й у завданні 1. Це означає, що в процесі задокументування змін залучені ті ж фахівці, що й на попередніх етапах, включаючи архітекторів безпеки та конфіденційності, інженерів системної безпеки та конфіденційності, офіцерів безпеки та конфіденційності системи, архітекторів підприємства та системних адміністраторів. Їх участь забезпечує всебічний підхід до документування змін та гарантує, що всі аспекти безпеки та конфіденційності належним чином враховані.

Фаза життєвого циклу розробки системи, до якої застосовується це завдання, охоплює етапи нової розробки та придбання, впровадження та оцінки, а також експлуатації та обслуговування. На етапі нової розробки та придбання

важливо, щоб усі зміни, внесені до плану впровадження, були належним чином задокументовані ще до початку фактичного впровадження. Це дозволяє забезпечити відповідність системи всім вимогам безпеки та конфіденційності ще на ранніх етапах її розробки. На етапі впровадження та оцінки важливо проводити регулярні перевірки та оцінки впроваджених засобів контролю, щоб виявити будь-які відхилення від плану та внести відповідні корективи. Це дозволяє забезпечити ефективне функціонування системи безпеки та конфіденційності у реальних умовах експлуатації. На етапі експлуатації та обслуговування важливо проводити регулярні аудит та моніторинг системи, щоб вчасно виявляти та усувати будь-які потенційні загрози та вразливості. Це дозволяє забезпечити безперервну відповідність системи вимогам безпеки та конфіденційності протягом всього її життєвого циклу [42].

Документування змін до запланованого впровадження засобів контролю є ключовим елементом забезпечення безпеки та конфіденційності інформаційних систем. Це завдання вимагає від організацій системного підходу до управління змінами, що включає детальне документування всіх змін, проведення регулярних оцінок та аудитів, а також залучення кваліфікованих фахівців для забезпечення відповідності системи вимогам безпеки та конфіденційності. Виконання цього завдання дозволяє організаціям забезпечити високий рівень безпеки та конфіденційності інформаційних систем, що є критично важливим у сучасних умовах зростаючих кіберзагроз.

Таким чином, задокументування змін до запланованого впровадження засобів контролю є невід'ємною частиною процесу управління ризиками інформаційної безпеки, що дозволяє забезпечити ефективне функціонування системи безпеки та конфіденційності протягом всього життєвого циклу інформаційної системи. Це завдання вимагає тісної співпраці між різними фахівцями та підрозділами організації, що дозволяє забезпечити всебічний підхід до управління змінами та гарантує відповідність системи всім вимогам безпеки та конфіденційності згідно посадових обов’язків, які визначені в таблиці 3.2.

Таблиця 3.2

Посадові обов'язки за посадами

№	Роль	Основна чи допоміжна роль	Обов'язки
1	Власник системи	Основна	• Визначення активів, які потребують захисту безпеки та конфіденційності • Визначення типів інформації, яку система повинна обробляти, зберігати та передавати • Визначення потреб в захисті та вимог до безпеки і конфіденційності системи
2	Спільний постачальник засобів контролю	Основна	• Забезпечення засобів захисту, призначених для виявлення, звітування та розслідування інцидентів інформаційної безпеки • Надання власнику/розпоряднику інформації оцінки, яка пояснює економічну цінність впроваджених засобів контролю • Впровадження засобів контролю, визначених власником/розпорядником інформації, над визначеними даними
3	Власник або розпорядник інформації	Допоміжна	• Впровадження та перевірка засобів контролю для забезпечення конфіденційності, цілісності та доступності системи; управління ризиками конфіденційності; та забезпечення дотримання застосовних вимог щодо конфіденційності • Забезпечення належного рівня повноважень для впровадження засобів контролю в систему • Перевірка та затвердження доступу до системи на основі потреб • Координація винятків із впроваджених засобів контролю • Документування впровадження засобів контролю для забезпечення відстеження рішень до та після розгортання системи • Координація оцінки засобів контролю паралельно з розробкою, щоб полегшити раннє виявлення слабких або неефективних засобів контролю • Звернення до пакету повноважень для визначення адекватності впроваджених загальних засобів контролю •

Продовження таблиці 3.2

			• - Визначення компенсуючих або додаткових засобів контролю для підвищення рівня захисту, який не забезпечується успадкованими загальними засобами контролю • - Забезпечення захисту системи від несанкціонованого розкриття, модифікації або видалення • - Забезпечення відповідного рівня повноважень для впровадження засобів контролю в систему • - Затвердження доступу, на основі необхідності, до системи • - Координація винятків із впроваджених засобів контролю • - Документування впровадження засобів контролю для забезпечення відстеження рішень до та після розгортання системи • - Надання інформації власникам системи щодо вимог до безпеки та конфіденційності, а також засобів контролю для системи • - Пропонування засобів контролю для успадкування (за необхідності)
4	1. Архітектор безпеки 2. Архітектор конфіденційності	Допоміжна	• Забезпечення зв'язку між архітектором підприємства та інженером з системної безпеки або конфіденційності • Розподіл засобів контролю за погодженням з власниками системи, постачальниками загальних засобів контролю та спеціалістами з системної безпеки або конфіденційності • Консультування вищого керівництва з низки питань безпеки та конфіденційності • Управління аспектами архітектури підприємства, які захищають інформацію та системи від несанкціонованої системної активності або поведінки; які забезпечують дотримання вимог конфіденційності; і які управляють ризиками для приватності осіб, пов'язаними з обробкою інформації, що ідентифікує особу.

Продовження таблиці 3.2

5	1. Інженер з безпеки систем 2. Інженер з конфіденційності	Допоміжна	• Забезпечення конфіденційності, цілісності та доступності системи шляхом розробки та впровадження захищеної системи • Забезпечення відповідності системи вимогам конфіденційності та управління ризиками для приватного життя осіб, пов'язаними з обробкою PII • Впровадження безпечних мережевих та обчислювальних середовищ, що сприяють підвищенню рівня конфіденційності • Забезпечення планування безпеки та конфіденційності для підтримки системи • Впровадження вимог безпеки та конфіденційності для належної обробки даних в системі • Рекомендації щодо рішень на рівні системи для вирішення вимог безпеки та конфіденційності • Координація найбільш ефективного способу впровадження загальних засобів контролю в організаційних системах
6	1. Відповідальний за безпеку системи 2. Відповідальний за конфіденційність системи	Допоміжна	• Надання допомоги у визначенні відповідного рівня безпеки, що відповідає рівню впливу • Консультування власника системи щодо вимог безпеки та конфіденційності
7	Архітектор підприємства	Допоміжна	• Впровадження стратегії архітектури підприємства, яка сприяє ефективним рішенням у сфері безпеки та конфіденційності • Співпраця з власниками систем та посадовими особами, які надають повноваження, для полегшення визначення меж повноважень • Координація з архітекторами безпеки та конфіденційності з питань безпеки та конфіденційності • Визначення місця системи в архітектурі підприємства
8	Системний адміністратор	Допоміжна	• Впровадження засобів контролю в планах безпеки та конфіденційності • Документація змін до запланованих заходів контролю на основі стану засобів контролю "як реалізовано".

Організації впроваджують засоби контролю відповідно до своєї корпоративної архітектури та найкращих практик, зокрема оцінки ризиків, щоб приймати обґрунтовані рішення. Цей процес передбачає використання системних методологій забезпечення безпеки та конфіденційності, концепцій і принципів. Оцінка ризиків є ключовим елементом цього підходу, оскільки вона допомагає організаціям зважувати витрати, вигоди та ризики, пов'язані з використанням різних технологій або політик для впровадження засобів контролю. Крім того, організації повинні забезпечувати встановлення та реалізацію обов'язкових конфігураційних налаштувань для елементів системи відповідно до федеральних та організаційних політик [43].

У випадках, коли організації не можуть безпосередньо контролювати певні елементи системи, наприклад, комерційні продукти, що закуповуються, вони можуть використовувати сторонні перевірені продукти, які були протестовані, оцінені або сертифіковані незалежними акредитованими лабораторіями. Такі перевірки, оцінки та сертифікації враховують продукти у специфічних конфігураціях та в ізоляції; впровадження засобів контролю враховує, як продукт інтегрується в систему, зберігаючи при цьому функціональність та надійність безпеки.

Вимоги до забезпечення впевненості є ще одним важливим аспектом цього процесу, оскільки вони спрямовані на підвищення рівня впевненості у тому, що засоби контролю впроваджуються правильно, працюють як передбачено і досягають бажаного результату щодо дотримання вимог безпеки та конфіденційності системи. Ці вимоги охоплюють якість дизайну, розробки та впровадження засобів контролю. У процесі впровадження загальних засобів контролю, які успадковуються системою, інженери системної безпеки та конфіденційності, спільно з офіцерами безпеки та конфіденційності системи, координуються з постачальниками загальних засобів контролю для визначення найкращих способів їх реалізації.

У випадках, коли під час впровадження виявляється, що загальні засоби контролю не відповідають встановленим вимогам безпеки або конфіденційності для системи, яка успадковує ці засоби, організації повинні визначити компенсуючі або додаткові засоби контролю, які можуть бути впроваджені. Системні власники можуть доповнювати загальні засоби контролю системними специфічними або гібридними засобами контролю, щоб досягти необхідного рівня захисту для своїх систем, або можуть прийняти більший ризик з відповідним погодженням та затвердженням організації [44].

Під час впровадження контролів можуть виявитися недоліки, які повинні бути вчасно виявлені та виправлені. Проведення початкових оцінок контролів під час розробки та впровадження системи дозволяє організаціям виявляти ці недоліки на ранніх етапах, що забезпечує економічно ефективний метод ініціювання коригувальних дій. Питання, виявлені під час таких оцінок, можуть бути передані уповноваженим особам для вирішення. Результати початкових оцінок можуть бути використані під час етапу авторизації, щоб уникнути затримок або дорогого повторення оцінок. Результати оцінок, які згодом використовуються на інших етапах життєвого циклу системи, повинні відповідати вимогам щодо повторного використання, встановленим організацією.

Загалом, впровадження засобів контролю відповідно до корпоративної архітектури та найкращих практик, зокрема з використанням оцінки ризиків та забезпечення впевненості, є комплексним процесом, який вимагає тісної координації та залучення різних спеціалістів. Це дозволяє забезпечити надійний та ефективний захист інформаційних систем, враховуючи усі можливі загрози та вразливості, що виникають у сучасному середовищі кібербезпеки.

3.2 Рекомендації щодо покращення моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури

Удосконалення моделі управління ризиками кібербезпеки для об'єктів критичної інфраструктури потребує комплексного підходу, що поєднує технологічні досягнення, стратегічне планування та процеси постійного вдосконалення. Кілька ключових рекомендацій можуть значно покращити стан кібербезпеки об'єктів критичної інфраструктури, тим самим забезпечивши надійний захист від потенційних кіберінцидентів та мінімізувавши їхній вплив.

Одним з найважливіших аспектів цього багатогранного підходу є впровадження передових технологій виявлення та реагування на загрози. Впровадження міжмережевих екранів нового покоління (NGFW), систем виявлення/запобігання вторгненням (IDS/IPS), а також рішень для управління інформацією та подіями безпеки (SIEM) є життєво важливими. Ці технології, які використовують машинне навчання і штучний інтелект, призначені для виявлення і реагування на складні загрози в режимі реального часу. Виявляючи та пом'якшуючи потенційні атаки до того, як вони можуть завдати значної шкоди, ці системи забезпечують проактивний захист від кіберзагроз.

Іншим важливим компонентом є покращення управління активами та сегментація мережі. Проведення всебічної інвентаризації активів та забезпечення належної класифікації критично важливих активів має фундаментальне значення. Надійна сегментація мережі також має вирішальне значення, оскільки вона обмежує латеральне переміщення загроз всередині мережі, ефективно ізолюючи критичні системи від менш захищених частин інфраструктури. Такий підхід мінімізує ризик масштабної шкоди у випадку кібератаки, оскільки потенційні проломи локалізуються в ізольованих сегментах.

Інтеграція розвідки загроз і сприяння співпраці є ще однією важливою рекомендацією. Використання платформ розвідки загроз для збору та аналізу даних про нові загрози дозволяє організаціям випереджати потенційні кіберризики. Заохочення співпраці з іншими операторами критичної

інфраструктури, галузевими партнерами та державними установами для обміну розвідданими про загрози та найкращими практиками посилює загальний стан безпеки. Такий підхід до колективного захисту використовує спільні знання та ресурси, забезпечуючи більш повне розуміння ландшафту загроз та покращуючи здатність до ефективного реагування [45].

Ще однією важливою рекомендацією є впровадження архітектури нульової довіри. Ця модель безпеки працює за принципом «ніколи не довіряй, завжди перевіряй», гарантуючи, що кожен користувач, пристрій і додаток, який намагається отримати доступ до мережі, проходить автентифікацію, авторизацію і постійну перевірку, перш ніж йому буде надано доступ до ресурсів. Такий підхід значно знижує ризик несанкціонованого доступу та потенційних порушень завдяки суворому контролю над усіма точками доступу.

Посилення планів реагування на інциденти та відновлення також має вирішальне значення. Розробка та регулярне оновлення комплексних планів реагування на інциденти, які визначають процедури виявлення, локалізації, ліквідації та відновлення після інцидентів кібербезпеки, є вкрай важливими. Проведення регулярних навчань та симуляцій гарантує, що всі зацікавлені сторони будуть готові ефективно реагувати на реальні сценарії, тим самим мінімізуючи вплив кіберінцидентів.

Ще однією ключовою рекомендацією є вдосконалення програм навчання та підвищення обізнаності співробітників. Проведення постійних тренінгів та інформаційних програм з кібербезпеки для всіх працівників підкреслює важливість розпізнавання та повідомлення про потенційні загрози, дотримання політик безпеки та передових практик захисту даних. Спеціалізовані тренінги для IT-спеціалістів та працівників служби безпеки також необхідні для того, щоб вони були в курсі останніх тенденцій загроз і методів їхнього подолання, а також були добре підготовлені до боротьби з кіберзагрозами, що постійно змінюються.

Регулярні оцінки безпеки та тестування на проникнення є важливими для підтримання надійного захисту від кіберзагроз. Проведення регулярних оцінок безпеки, сканування вразливостей та тестування на проникнення допомагає

виявити та усунути слабкі місця в інфраструктурі. Ці проактивні заходи виявляють вразливості до того, як ними зможуть скористатися зловмисники, тим самим посилюючи загальну безпеку об'єкта.

Ще однією важливою рекомендацією є впровадження надійних механізмів контролю доступу. Впровадження суворих політик контролю доступу, включаючи принцип найменших привілеїв (PoLP), гарантує, що користувачі мають лише ті права доступу, які необхідні для виконання своїх посадових обов'язків. Використання багатофакторної автентифікації (MFA) додає додатковий рівень безпеки для доступу до критично важливих систем, ще більше знижуючи ризик несанкціонованого доступу.

Регулярне оновлення та виправлення систем також є важливим процесом для підтримання достатньої протидії кібербезпеки загрозам. Забезпечення регулярного оновлення та виправлення всього програмного та апаратного забезпечення захищає від відомих вразливостей. Налагодження надійного процесу управління виправленнями гарантує, що оновлення безпеки, випущені постачальниками, будуть оперативно впроваджуватися, що зменшує ризик їх використання.

Впроваджуючи ці комплексні рекомендації, об'єкти критичної інфраструктури можуть значно покращити свої моделі управління ризиками кібербезпеки. Ці заходи забезпечують надійний захист від еволюціонуючих загроз, гарантуючи, що критичні системи залишатимуться безпечними та працездатними. Постійне вдосконалення та адаптація до нових загроз мають важливе значення для підтримання сильної позиції кібербезпеки в умовах постійно мінливого ландшафту загроз.

Висновки до розділу 3

Розділ присвячений впровадженню та вдосконаленню моделі управління ризиками кібербезпеки, зокрема в контексті об'єктів критичної інфраструктури.

Досліджено процес впровадження моделі управління ризиками кібербезпеки для об'єктів критичної інфраструктури. Проаналізовано

особливості застосування такої моделі в контексті різних секторів, визначено ключові складові та етапи впровадження. Розглянуті підходи до адаптації загальних моделей управління ризиками до специфічних вимог критичної інфраструктури, враховуючи особливості їх функціонування та потенційні загрози.

Надано рекомендації щодо покращення моделі управління ризиками кібербезпеки для об'єктів критичної інфраструктури. Це включає вдосконалення методологій аналізу ризиків, впровадження новітніх технологій та підходів до виявлення та запобігання кіберзагрозам, а також оптимізацію процесів реагування на інциденти. Розглядаються можливості використання штучного інтелекту, машинного навчання та аналізу великих обсягів даних для підвищення ефективності систем управління ризиками кібербезпеки в критичних інфраструктурних секторах.

Отже, здійснюється аналіз і практичне впровадження моделі управління ризиками кібербезпеки з фокусом на об'єкти критичної інфраструктури. Надаються конкретні рекомендації щодо оптимізації цієї моделі для підвищення рівня захисту та реагування на потенційні кіберзагрози в цих секторах.

ВИСНОВКИ

У результаті дослідження, яке присвячено розробленню моделі управління ризиками кібербезпеки об'єктів критичної інфраструктури, було зроблено кілька важливих висновків.

У першому розділі за результатами аналізу наукових досліджень, що присвячені кібербезпеці об'єктів критичної інфраструктури, було виявлено важливість нормативно-правового забезпечення в цій сфері. Аналіз тенденцій розвитку кіберзагроз дозволив зрозуміти, що ця область піддається постійним змінам, що вимагає постійного оновлення заходів захисту. Також була виявлена тісна залежність інформаційних об'єктів захисту від типу потенційних загроз, що свідчить про необхідність індивідуального підходу до кожного об'єкту критичної інфраструктури.

У другому розділі, що стосується розроблення моделі управління ризиками кібербезпеки, було з'ясовано, що аналіз та оцінка ризиків кібербезпеки є основою для ефективного управління цими ризиками. Методи реагування на ризики кібербезпеки, виявлені в цьому розділі, забезпечують комплексний підхід до захисту інформаційних систем та побудови моделей управління ризиками кібербезпеки об’єктів критичної інфраструктури конкретних організацій. Розроблена принципова модель, яка складається з взаємопов’язаних компонентів для досягнення підвищення кіберзахисту об’єктів критичної інфраструктури з їх основними залежностями. Математична перевірка моделі встановила її якість. Процес розробки системи моніторингу та аналізу подій в кібербезпеці є ключовим для вчасного виявлення та реагування на потенційні загрози.

У третьому розділі, що описує впровадження та вдосконалення моделі управління ризиками кібербезпеки, було виявлено, що успішна імплементація цієї моделі вимагає врахування специфіки об'єктів критичної інфраструктури. Рекомендації щодо покращення моделі управління ризиками вказують на необхідність постійного оновлення методологій та використання новітніх технологій.

Загалом, розробка моделі управління ризиками кібербезпеки для об'єктів критичної інфраструктури є складним, але вкрай важливим завданням. Вона вимагає поєднання нормативно-правового забезпечення, аналізу тенденцій розвитку кіберзагроз, а також індивідуального підходу до кожного об'єкту захисту. Впровадження цієї моделі вимагає постійного вдосконалення і адаптації до змін у кіберсередовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations / A. Mishra et al. *Computers & Security*. 2022. P. 102820. URL: https://doi.org/10.1016/j.cose.2022.102820

2. 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

3. 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

4. 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

5. 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

6. 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

7. N. Petru-Cristian. A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications. Cluj-Napoca. 2024. URL: https://www.researchgate.net/publication/375062115_A_Comprehensive_Analysis_of_High-Impact_Cybersecurity_Incidents_Case_Studies_and_Implications

8. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021. URL: https://doi.org/10.1016/j.egyr.2021.08.126

9. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804

10. 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

11. 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

12. Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions / A. Rejeb et al. *Internet of Things and Cyber-Physical Systems*. 2023. URL: https://doi.org/10.1016/j.iotcps.2023.06.003

13. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods / T. Mazhar et al. *Future Internet*. 2023. Vol. 15, no. 2. P. 83. URL: https://doi.org/10.3390/fi15020083

14. A. S. Bhadouria. Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. *International Journal of Scientific and Research Publications*. 2022. Vol. 10, Issue 10. URL: https://www.researchgate.net/publication/363792663_Study_of_Impact_of_Malicious_Attacks_and_Data_Breach_on_the_Growth_and_Performance_of_the_Company_and_Few_of_the_World%27s_Biggest_Data_Breaches

15. A deeper look into cybersecurity issues in the wake of Covid-19: a survey / M. Alawida et al. *Journal of King Saud University - Computer and Information Sciences*. 2022. URL: https://doi.org/10.1016/j.jksuci.2022.08.003

16. M. Lehto. Cyber-Attacks Against Critical Infrastructure. *Cyber Security: Critical Infrastructure Protection*. 2022. URL: https://www.researchgate.net/publication/359698069_Cyber-Attacks_Against_Critical_Infrastructure

17. Ma C. Smart city and cyber-security technologies used, leading challenges and future recommendations. *Energy Reports*. 2021. URL: https://doi.org/10.1016/j.egyr.2021.08.124

18. Rehak D., Hromada M., Lovecek T. Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic. *Safety Science*. 2020. Vol. 127. P. 104698. URL: https://doi.org/10.1016/j.ssci.2020.104698

19. Vulnerability Exploitation Risk Assessment Based on Offensive Security Approach / S.-S. Yoon et al. *Applied Sciences*. 2023. Vol. 13, no. 22. P. 12180. URL: https://doi.org/10.3390/app132212180

20. A. Jumratjaroenvanit, Y. Teng-Amnuay. Probability of Attack Based on System Vulnerability Life Cycle. *IEEE Xplore*. 2008. URL: https://www.researchgate.net/publication/4369201_Probability_of_Attack_Based_on_System_Vulnerability_Life_Cycle

21. A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance / A. Javadpour et al. *Computers & Security*. 2024. P. 103792. URL: https://doi.org/10.1016/j.cose.2024.103792

22. 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

23. Asset-Oriented Threat Modeling / N. Messe et al. 2020 *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 29 December 2020 – 1 January 2021. 2020. URL: https://doi.org/10.1109/trustcom50675.2020.00073

24. A review of threat modelling approaches for APT-style attacks / M. Tatam et al. *Heliyon*. 2021. Vol. 7, no. 1. P. e05969. URL: https://doi.org/10.1016/j.heliyon.2021.e05969

25. Alwaheidi M. K. S., Islam S. Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems. *Sensors*. 2022. Vol. 22, no. 15. P. 5726. URL: https://doi.org/10.3390/s22155726

26. Yeboah-Ofori A., Islam S. Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet*. 2019. Vol. 11, no. 3. P. 63. URL: https://doi.org/10.3390/fi11030063

27. A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem / S. Silvestri et al. *Sensors*. 2023. Vol. 23, no. 2. P. 651. URL: https://doi.org/10.3390/s23020651

28. Bhoola V., Hiremath S. B., Mallik D. An Assessment of risk response strategies practiced in software projects. *Australasian Journal of Information Systems*. 2014. Vol. 18, no. 3. URL: https://doi.org/10.3127/ajis.v18i3.923

29. Ahmed R. Risk Mitigation Strategies in Innovative Projects. *Key Issues for Management of Innovative Projects*. 2017. URL: https://doi.org/10.5772/intechopen.69004

30. D. Elegberun. O. Ferguson. Strengthening Cyber Security: A Review of Established Frameworks and Best Practices for Implementation. 2022. URL: https://www.researchgate.net/publication/379022664_Strengthening_Cyber_Security_A_Review_of_Established_Frameworks_and_Best_Practices_for_Implementation

31. Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence / S. Ali et al. *Information Fusion*. 2023. P. 101805. URL: https://doi.org/10.1016/j.inffus.2023.101805

32. Strategic alignment and its impact on decision effectiveness: a comprehensive model / M. A. Ghonim et al. *International Journal of Emerging Markets*. 2020. Ahead-of-print, ahead-of-print. URL: https://doi.org/10.1108/ijoem-04-2020-0364

33. Casaril F., Galletta L. Securing SatCom user segment: a study on cybersecurity challenges in view of IRIS. *Computers & Security*. 2024. P. 103799. URL: https://doi.org/10.1016/j.cose.2024.103799

34. 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

35. 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

36. CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES / Samuel Onimisi Dawodu et al. *Computer Science & IT Research Journal*. 2023. Vol. 4, no. 3. P. 220–243. URL: https://doi.org/10.51594/csitrj.v4i3.659

37. The tensions of cyber-resilience: from sensemaking to practice / B. Dupont et al. *Computers & Security*. 2023. P. 103372. URL: https://doi.org/10.1016/j.cose.2023.103372

38. TVARONAVIČIENĖ M., PLĖTA T., DELLA CASA S. CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE PROTECTION. *International Scientific Conference „Contemporary Issues in Business, Management and Economics Engineering"*, Vilnius Gediminas Technical University, 13–14 May 2021. 2021. URL: https://doi.org/10.3846/cibmee.2021.611

39. 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)

40. Implementation of Cybersecurity Risk Theory and Model in Healthcare / O. S. Folorunsho et al. *Advances in Multidisciplinary and scientific Research Journal Publication*. 2022. Vol. 13, no. 4. P. 65–72. URL: https://doi.org/10.22624/aims/cisdi/v13n4p4

41. Lee I. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*. 2021. Vol. 64, no. 5. P. 659–671. URL: https://doi.org/10.1016/j.bushor.2021.02.022

42. Гончар С., Потенко О. МЕТОДОЛОГІЯ ОЦІНКИ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ

ІНФРАСТРУКТУРИ. Ukrainian Information Security Research Journal. 2023. Vol. 25, no. 3. P. 159–165. URL: https://doi.org/10.18372/2410-7840.25.17941

43. FEDYK V., DENYSENKO H. Theoretical and methodological approaches to the management of cyber security risks at critical infrastructure objects: response to cyber incidents and crisis managemen. *INFORMATION AND LAW*. 2024. No. 1(48). P. 195–202. URL: https://doi.org/10.37750/2616-6798.2024.1(48).300822

44. 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

45. 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