Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська дипломна робота
на тему: «Модель політики безпеки для об'єкта критичної інфраструктури»

Виконав: студент 4 курсу групи 1БС–19б
спеціальності 125 Кібербезпека
_____ Грищук. В.В.

Керівник: к. т. н. доцент. каф. ЗІ
_____ Дудатьєв А.В.
«16» червня 2023 р.

Рецензент: к. т. н. доцент каф. ОТ
_____ Хошаба О.М.
«19» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо–професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д. т. н., проф.
_____В. А. Лужецький
20 березня 2023 року

ЗАВДАННЯ
НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Грищуку Владиславу Валерійовичу

1. Тема роботи: «Модель політики безпеки для об'єкта критичної інфраструктури» керівник роботи: Дудатьєв Андрій Веніамінович, к.т.н., доц. каф. ЗІ.
Затверджені наказом ректора ВНТУ від 20 березня 2023р. №67

2. Строк подання студентом роботи 19 червня 2023 р.

3. Вихідні дані до роботи:
- інформація про потенційні загрози безпеки для об'єкта критичної інфраструктури;
- інформація про об'єкт критичної інфраструктури, включаючи його розмір, місцезнаходження, тип діяльності тощо;
- інформація про наявні заходи безпеки та їх ефективність;
- інформація про регуляторні вимоги та стандарти безпеки, яким повинен відповідати об'єкт критичної інфраструктури.

4. Зміст розрахунково–пояснювальної записки: Вступ. Аналіз літературних джерел. Аналіз стану безпеки. Розробка моделей політики безпеки. Перевірка ефективності моделей. Висновки. Перелік використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Таблиця політика безпеки (плакат А4). Моделі політики безпеки для об'єктів критичної інфраструктури (плакат А4). Недоліки існуючих підходів (плакат А4). План заходів з забезпечення безпеки об'єкта критичної інфраструктури (плакат А4). Форма контролю та моніторингу безпеки об'єкта критично.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Дудатьєв А.Н., к.т.н., доц. каф. ЗІ.	20.03.03	19.06.23
2	Дудатьєв А.Н., к.т.н., доц. каф. ЗІ.	20.03.03	19.06.23
3	Дудатьєв А.Н., к.т.н., доц. каф. ЗІ.	20.03.03	19.06.23

7. Дата видачі завдання 20.03.2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	20.03 – 24.03	
2	Аналіз літературних джерел за напрямком бакалаврської кваліфікаційної роботи	27.03 – 07.03	
3	Аналіз стану безпеки для об'єктів критичної інфраструктури	10.04 – 21.04	
4	Розробка моделі політики безпеки	24.04 – 19.05	
5	Перевірка ефективності моделі політики безпеки	22.05 – 24.05	
6	Аналіз виконання ТЗ, висновки	25.05 – 28.05	
7	Оформлення пояснювальної записки	29.05 – 31.05	
8	Попередній захист та доопрацювання БДР	01.06 – 15.06	
9	Представлення БДР до захисту	16.06 – 19.06	
10	Захист БДР	20.06 – 23.06	

Студент _____ Грищук
(підпис)

Керівник роботи _____ Дудатьєв
(підпис)

АНОТАЦІЯ

Бакалаврська дипломна робота складається з 68 сторінок формату А4, на яких є 2 рисунків, 1 таблиці, список використаних джерел містить 15 найменувань.

Бакалаврська робота присвячена аналізу стану безпеки об’єктів критичної інфраструктури та розробці нової моделі політики безпеки для цих об’єктів. У першому розділі було визначено поняття “об’єкта критичної інфраструктури” та проаналізовано нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури. У другому розділі було виявлено недоліки існуючих підходів до забезпечення безпеки об’єктів критичної інфраструктури та розроблено нову модель політики безпеки, яка базується на типах загроз та методології оцінювання ризиків для об’єктів критичної інфраструктури. У третьому розділі модель була протестована за допомогою експериментального тестування, результати якого були проаналізовані та порівняні з існуючими підходами до забезпечення безпеки об’єктів критичної інфраструктури. На основі отриманих результатів було сформульовано рекомендації щодо застосування моделі політики безпеки для об’єктів критичної інфраструктури.

Ключові слова: безпека, об’єкти критичної інфраструктури, кібербезпека, політика безпеки, модель політики безпеки, загрози, ризики, експериментальне тестування, рекомендації.

ABSTRACT

The bachelor thesis consists of 68 pages of A4 format, on which there are 2 figures, 1 table, the list of used sources contains 15 names.

The bachelor thesis is devoted to the analysis of the state of security of critical infrastructure objects and the development of a new model of security policy for these objects. In the first section, the concept of "critical infrastructure object" was defined and the regulatory and legal provision of cyber security of critical infrastructure objects was analyzed. In the second chapter, the shortcomings of existing approaches to ensuring the security of critical infrastructure objects were identified and a new model of security policy was developed, which is based on the types of threats and risk assessment methodology for critical infrastructure objects. In the third section, the model was tested using experimental testing, the results of which were analyzed and compared with existing approaches to ensuring the safety of critical infrastructure facilities. Based on the obtained results, recommendations were formulated regarding the application of the security policy model for critical infrastructure facilities.

Keywords: security, critical infrastructure objects, cyber security, security policy, security policy model, threats, risks, experimental testing, recommendations.

ЗМІСТ

ВСТУП

Сьогодні стрімкий розвиток інформаційних технологій дійсно вражає. Обчислювальна техніка застаріває і стає менш актуальною буквально за кілька років. Технічні характеристики якої ростуть досить швидко, щодня люди використовують різні технічні засоби (комп'ютери, ноутбуки, планшети, телефони). Усі вони мають доступ до інтернет-середовища й інтенсивно переглядають різні типи інформації.

З розвитком технологій все більше і більше компаній застосовують інформаційні технології з метою автоматизувати свій бізнес. Таке бажання до автоматизації значно збільшує обсяг важливої інформації, що зберігається в різних базах даних, що призводить до потреби якісніше захищати свою інформацію. Нажаль в подібних існуючих системах виникають проблеми з розмежуванням доступу.

Забезпечення ефективного захисту інформації надзвичайно важливо для установ, в яких щодня обробляється великий обсяг інформації різного рівня конфіденційності. У більшості випадків ця інформація є об'єктом дій конкурентів і призводить до загострення питань захисту інформації від її незаконного використання і несанкціонованого доступу до неї. Сьогодні керівництво більшості установ не сумнівається в необхідності серйозно подбати про інформаційну безпеку своєї організації. Використання сучасних інформаційних технологій розширює можливості для різних злочинних дій, пов'язаних з використанням комп'ютерних технологій.

У даній роботі проаналізовано та досліджено використання різних моделей розмежування доступу до інформаційних систем, їхні основні переваги та недоліки. В результаті буде створено механізм, що допоможе покращити розмежування доступу до інформаційних ресурсів.

Споглядаючи на те, що кожного року з’являється безліч нових підходів до захисту інформації, вони часто допускають помилки, та гублять деталі реалізації щодо методів розмежування доступу. Основною проблемою в створюваних документах є використання примітивних підходів.

Мета дослідження це аналіз реалізованих механізмів розмежування доступу та їх використання до інформаційних ресурсів.

Завдання дослідження – проаналізувати існуючі моделі управління доступомв інформаційних системах, описати методи їх застосування, виділити основніпереваги та недоліки цих методів для інформаційних ресурсів.

Об'єктом дослідження в даній роботі є процеси створення політик безпеки. Предмет дослідження – методи контролю доступу в інформаційних системах.

Для створення рекомендацій вибору моделі розмежування доступу до інформаційних ресурсів в даній роботі будуть використовуватися існуючі методи контролю доступу в інформаційних системах.

1 АНАЛІЗ СТАНУ БЕЗПЕКИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття «об’єкта критичної інфраструктура»

Поняття "об'єкта критичної інфраструктури" відноситься до ключових елементів, систем і послуг, які є незамінними для ефективного функціонування суспільства, економіки та національної безпеки. Ці об'єкти є важливими з точки зору господарського, соціального і політичного розвитку країни, а також мають критичне значення для життя і добробуту її громадян [1].

Визначення об'єкта критичної інфраструктури варіюється залежно від конкретної країни або організації, яка його регулює. Проте, загальною характеристикою є те, що такі об'єкти мають велике значення для безпеки нації та стабільності її інституцій. Деякі типові приклади об'єктів критичної інфраструктури включають енергетичні системи, транспортні мережі, телекомунікаційну інфраструктуру, фінансові установи, водопостачання і каналізацію, охорону здоров'я та інші сектори, які є важливими для життя нації.

Одна з ключових ознак об'єктів критичної інфраструктури полягає в їхній вразливості до різних видів загроз. Це можуть бути техногенні аварії, природні катастрофи, кібератаки, терористичні акти, епідемії та інші події, що можуть призвести до порушення роботи об'єктів або навіть їхнього повного паралізу. Такі події можуть мати серйозні наслідки для економіки, безпеки громадян, виконання основних функцій держави та забезпечення громадського порядку.

Одним із способів захисту об'єктів критичної інфраструктури є їхнє визначення, класифікація і ідентифікація. У багатьох країнах існують спеціальні органи чи агентства, відповідальні за регулювання і захист об'єктів критичної інфраструктури. Вони визначають перелік об'єктів, що мають стратегічне значення, та розробляють політику і стандарти безпеки, які мають бути дотримані відповідними організаціями.

У процесі визначення об'єкта критичної інфраструктури враховуються такі фактори, як важливість об'єкта для функціонування суспільства, його зв'язок з іншими елементами інфраструктури, потенційна загроза та наслідки її

порушення, можливість заміщення функцій об'єкта в разі виникнення негативних ситуацій тощо.

Крім визначення і ідентифікації об'єктів критичної інфраструктури, важливим аспектом є їхнє постійне спостереження, оцінка ризиків та впровадження заходів безпеки. Це може включати планування надзвичайних ситуацій, проведення тренувань і навчання персоналу, застосування технологічних рішень для виявлення загроз, контролю доступу та захисту інформації.

У світі, де зростає кількість загроз і ризиків, об'єкти критичної інфраструктури стають особливо вразливими. Тому важливо розробляти і вдосконалювати системи захисту і реагування на негативні події, забезпечуючи безпеку та стійкість об'єктів критичної інфраструктури. Колективні зусилля, співпраця між державою, приватним сектором та громадськістю є ключовими в цьому процесі.

Узагальнюючи, об'єкти критичної інфраструктури є незамінними компонентами суспільства і господарства. Вони забезпечують ефективне функціонування системи, збереження безпеки та нормального життя громадян. Визначення, класифікація і захист таких об'єктів є важливим завданням для країн та організацій, що мають на меті забезпечити стійкість і безпеку своїх інфраструктурних систем.

Зважаючи на важливість об'єктів критичної інфраструктури, багато країн вживають заходів для їхнього захисту. Одним з таких прикладів є Сполучені Штати Америки, де існує програма захисту критичних інфраструктур (Critical Infrastructure Protection Program). Ця програма охоплює широкий спектр секторів, включаючи енергетику, транспорт, водопостачання, інформаційні технології та інші.

Для кращого розуміння об'єктів критичної інфраструктури, можна створити таблицю, що вказує на категорії і приклади таких об'єктів:1.1

Таблиця 1.1

Категорія	Приклади об'єктів критичної інфраструктури
Енергетика	Ядерні електростанції, газопроводи, нафтопроводи
Транспорт	Аеропорти, магістральні автомагістралі, порти
Телекомунікації	Мобільні оператори, супутникові зв'язки
Фінансові установи	Банки, біржі, платіжні системи
Водопостачання та каналізація	Водні мережі, водозабори, очисні споруди
Охорона здоров'я	Лікарні, медичні центри, фармацевтичні заводи
Громадські послуги	Школи, університети, муніципальні служби

Ця таблиця демонструє різноманітні сектори, в яких можуть бути визначені об'єкти критичної інфраструктури. Порушення роботи будь-якого з цих об'єктів може мати серйозні наслідки для суспільства і економіки.

Окрім загальновизнаних об'єктів критичної інфраструктури, іноді інші об'єкти можуть стати критичними у певних обставинах. Наприклад, під час пандемії COVID-19 медичні лабораторії для виявлення вірусу та виробництва вакцин стали критичними об'єктами. Такі ситуації показують, що поняття "об'єкт критичної інфраструктури" може бути гнучким і залежати від конкретних викликів, з якими стикається суспільство.

Узагальнюючи, поняття "об'єкт критичної інфраструктури" охоплює ключові елементи і системи, які забезпечують нормальне функціонування суспільства. Їхнє визначення, класифікація і захист є важливими завданнями для країн та організацій, що мають на меті забезпечити безпеку та стійкість своїх інфраструктурних систем.

Аналіз розподілу об'єктів критичної інфраструктури за рівнем важливості та вразливості є важливою складовою процесу забезпечення їхньої безпеки та ефективності. Цей аналіз дозволяє визначити найбільш критичні об'єкти, які потребують найбільшої уваги та заходів захисту.

Один з основних аспектів аналізу - це визначення рівня важливості об'єктів критичної інфраструктури. Рівень важливості може визначатися на основі кількох факторів, включаючи:

1. Вплив на громадську безпеку: Деякі об'єкти критичної інфраструктури, наприклад, лікарні або системи екстреної допомоги, безпосередньо пов'язані з безпекою та життями громадян. Їхнє порушення може мати серйозні наслідки для здоров'я і безпеки населення.

2. Економічна важливість: Деякі об'єкти, такі як фінансові установи або виробничі підприємства, можуть мати великий вплив на економіку країни або регіону. Їхнє непрацездатність може спричинити значні фінансові втрати та збитки.

3. Суспільна важливість: Деякі об'єкти, наприклад, школи, університети або транспортні мережі, є важливими для забезпечення нормального функціонування суспільства та забезпечення громадських послуг. Їхнє порушення може призвести до значних перешкод у повсякденному житті громадян.

Для кожного об'єкта критичної інфраструктури проводиться оцінка рівня вразливості. Це допомагає визначити ймовірність та наслідки можливих загроз або атак на ці об'єкти. Рівень вразливості може залежати від таких факторів:

1. Фізична охорона: Наявність систем відеоспостереження, контролю доступу, а також фізична охорона можуть впливати на рівень вразливості об'єкта. Недостатня охорона може створити можливості для незаконного доступу або атак.

2. Інформаційна безпека: Об'єкти, що мають велику кількість конфіденційної або чутливої інформації, можуть бути вразливими до кібератак або порушення інформаційної безпеки. Рівень захисту мереж, систем зберігання даних та комунікаційних каналів впливає на рівень вразливості.

3. Технічний стан та стійкість: Старіння обладнання, недостатня технічна підтримка та відсутність резервних систем можуть зробити об'єкти критичної

інфраструктури більш вразливими до непередбачуваних випадків технічних неполадок або аварій.

4. Залежність від інших об'єктів: Деякі об'єкти можуть бути вразливими через свою залежність від інших систем або об'єктів. Наприклад, електростанція може бути вразливою, якщо її життєдіяльність залежить від надійного постачання палива.

Проведений аналіз розподілу об'єктів критичної інфраструктури за рівнем важливості та вразливості допомагає визначити пріоритети в розробці та впровадженні заходів захисту. Більш критичні та вразливі об'єкти потребують більшої уваги та інвестицій для забезпечення їхньої стійкості та безпеки. Заходи захисту можуть включати фізичну охорону, покращення інформаційної безпеки, резервне забезпечення та планування непередбачених ситуацій.

Крім того, результати аналізу можуть використовуватися для вдосконалення політики управління кризовими ситуаціями та розробки стратегій мінімізації ризиків. Розподіл ресурсів та координація між державними органами, приватним сектором та громадськістю можуть бути удосконалені на основі аналізу розподілу об'єктів критичної інфраструктури за їх важливістю та вразливістю.

Узагальнюючи, аналіз розподілу об'єктів критичної інфраструктури за рівнем важливості та вразливості є важливим інструментом для ефективного управління та захисту критичної інфраструктури. Він допомагає визначити пріоритети, розробити стратегії та плани дій для забезпечення стійкості та безпеки об'єктів критичної інфраструктури.

Об'єкти критичної інфраструктури включають широкий спектр систем та інституцій, які є ключовими для безпеки, стійкості та функціонування суспільства. Розглянемо основні види об'єктів критичної інфраструктури з використанням реальних прикладів:

1. Енергетичні об'єкти: Системи енергопостачання, такі як електростанції та підстанції, є критичними для забезпечення електроенергії населенню та

промисловості. Наприклад, Фукусіма-1 в Японії, яка стала місцем аварії в 2011 році, є прикладом критичного об'єкта енергетичної інфраструктури.

2. Транспортні системи: Авіаційні аеропорти, залізничні вузли, морські порти та дорожні мережі є ключовими для переміщення людей, товарів та послуг. Наприклад, Міжнародний аеропорт Г'юстона в США є критичним об'єктом транспортної інфраструктури.

3. Телекомунікаційні системи: Мережі зв'язку та інформаційні технології є необхідними для забезпечення комунікації та обміну даними. Наприклад, Інтернет-комутатори, мобільні оператори та центри обробки даних є критичними об'єктами телекомунікаційної інфраструктури.

4. Водопостачання та водовідведення: Системи водопостачання та водовідведення забезпечують доступ до питної води та управління стічними водами. Наприклад, Південно-Китайська річка в Китаї, яка забезпечує воду для мільйонів людей та промислових підприємств, є критичним об'єктом водної інфраструктури.

5. Банківські та фінансові системи: Банки, біржі та інші фінансові установи забезпечують функціонування економіки та здійснюють фінансові операції. Наприклад, Федеральна резервна система США є критичним об'єктом фінансової інфраструктури.

6. Медичні установи: Лікарні, клініки та інші медичні установи забезпечують надання медичних послуг та лікування населенню. Наприклад, Госпіталь Святої Марії в Лондоні є критичним об'єктом медичної інфраструктури.

Це лише кілька прикладів основних видів об'єктів критичної інфраструктури, які мають велике значення для суспільства. Розподіл уваги та ресурсів для захисту цих об'єктів є важливою задачею для забезпечення стійкості та безпеки національної інфраструктури.

1.2 Нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури

Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури України є важливим аспектом для забезпечення безпеки та стійкості цих об'єктів перед сучасними кіберзагрозами. В Україні існують спеціальні нормативні акти, закони та положення, які регулюють захист критичної інфраструктури в кіберпросторі.

Україна – У 2017 році було прийнято Закон України “Про основні засади забезпечення кібербезпеки України”, який визначає правові та організаційні засади забезпечення кібербезпеки в Україні. Закон передбачає створення системи захисту критичної інформаційної інфраструктури та визначає повноваження органів державної влади у сфері кібербезпеки. Також у 2021 році було прийнято Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, який визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Цей закон також визначає основні терміни, такі як «безпека критичної інфраструктури», «життєво важливі функції та послуги», «захист критичної інфраструктури», «об’єкт критичної інфраструктури» тощо.

У 2020 році було прийнято постанову Кабінету Міністрів України № 1109 “Деякі питання об’єктів критичної інфраструктури”, яка затверджує Порядок встановлення категорій критичності об’єктів критичної інфраструктури.

Також можу навести спеціальні нормативні акти, закони та положення, які регулюють захист критичної інфраструктури в кіберпросторі у інших країнах світу:

1. США - Кіберзаконодавство США включає декілька актів, спрямованих на захист критичної інфраструктури. Наприклад, Закон про кібербезпеку критичної інфраструктури (Cybersecurity Act of 2015) та Закон про кібербезпеку (Cybersecurity Enhancement Act of 2014) надають керівництво та ресурси для захисту критичної інфраструктури від кібератак.

2. Європейський Союз - У Європейському Союзі було прийнято Кіберзахисний закон ЄС (EU Cybersecurity Act), який надає фреймворк для оцінки та сертифікації кіберзахисних виробів, послуг та процесів. Крім того, було прийнято Директиву про мережі та інформаційну безпеку (NIS Directive), яка встановлює мінімальні вимоги до кіберзахисту для об'єктів критичної інфраструктури у країнах-членах ЄС.

3. Канада - Канада прийняла Закон про кібербезпеку (Cybersecurity Act), який має на меті покращення кібербезпеки критичної інфраструктури. Він надає правовий фреймворк для ідентифікації та захисту об'єктів критичної інфраструктури від кіберзагроз.

Це лише кілька прикладів нормативно-правових актів, законів та положень, які регулюють кібербезпеку об'єктів критичної інфраструктури. Кожна країна може мати власну систему нормативного регулювання, спрямовану на захист своєї критичної інфраструктури. Принциповим є встановлення вимог щодо кіберзахисту, обов'язкових стандартів, механізмів моніторингу та співпраці між державними органами, приватним сектором та іншими зацікавленими сторонами для ефективного захисту критичної інфраструктури від кіберзагроз [2, 3].

Вимоги до кібербезпеки об'єктів критичної інфраструктури включають комплексні заходи, які мають на меті захистити ці об'єкти від кіберзагроз та забезпечити їх стійке функціонування. Виявлення і пояснення цих вимог є важливим етапом у процесі розробки та впровадження кібербезпекових заходів. Нижче наведено обширний огляд деяких основних вимог до кібербезпеки об'єктів критичної інфраструктури:

1. Аутентифікація та авторизація: Об'єкти критичної інфраструктури повинні мати механізми аутентифікації, які дозволяють ідентифікувати користувачів та системи, що мають доступ до них. Крім того, важливо мати системи авторизації, які визначають рівні доступу та обмеження для забезпечення принципу найменшого можливого привілею.

2. Керування доступом: Для забезпечення кібербезпеки об'єктів критичної інфраструктури необхідно встановлювати механізми керування доступом, які контролюють та обмежують права доступу до систем та ресурсів. Це включає установлення політик паролів, використання механізмів двофакторної аутентифікації та обмеження доступу до критичних функцій.

3. Захист мережі: Об'єкти критичної інфраструктури повинні мати механізми захисту мережі, такі як мережеві брандмауери, виявлення вторгнень та захист від вразливостей. Важливо встановлювати периметральні заходи безпеки, що мінімізують ризик незаконного доступу до систем та даних.

4. Моніторинг та виявлення інцидентів: Системи критичної інфраструктури повинні мати механізми моніторингу та виявлення кіберінцидентів. Це включає постійне відстеження подій, аналіз журналів подій, виявлення аномалій та шкідливих програм для своєчасного реагування на потенційні загрози.

5. Резервне копіювання та відновлення: Критичні системи повинні мати механізми резервного копіювання даних та можливості швидкого відновлення в разі катастрофічних подій або кібератак. Це дозволяє забезпечити неперервність функціонування та мінімізувати втрати даних.

6. Шифрування: Важливим аспектом кібербезпеки є застосування шифрування для захисту конфіденційної інформації, передаваної по мережі або зберіганої на пристроях. Шифрування дозволяє забезпечити конфіденційність та цілісність даних, що передаються або зберігаються.

7. Стандарти та вимоги безпеки: Важливо дотримуватись встановлених стандартів та вимог безпеки, які визначаються відповідними організаціями або нормативними актами. Наприклад, стандарти ISO/IEC 27001 та NIST Cybersecurity Framework надають рекомендації та норми щодо кібербезпеки.

Це основні вимог до кібербезпеки об'єктів критичної інфраструктури. Кожен об'єкт може мати свої особливі вимоги, залежно від його типу та функціональності. Важливо ретельно аналізувати та виявляти ці вимоги,

розробляти та впроваджувати відповідні кібербезпекові заходи для забезпечення безпеки критичної інфраструктури у кіберпросторі.

Кібербезпека є глобальною проблемою, і існують міжнародні стандарти та норми, які визначають рекомендації та вимоги для захисту інформаційних систем та об'єктів критичної інфраструктури. Нижче проведено порівняння з деякими з найвідоміших міжнародних стандартів та норм кібербезпеки:

— ДСТУ 3396.2-97 — це державний стандарт України з технічного захисту інформації. Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ). Терміни, регламентовані у цьому стандарті, обов’язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

— ДСТУ ISO/IEC 15408-1:2017 — це державний стандарт України з методів захисту інформаційних технологій. Цей стандарт є частиною 1 з “Вступом та загальною моделлю” з серії стандартів ISO/IEC 15408, який визначає загальні концепції та принципи оцінки безпеки ІТ та представляє загальну модель оцінки.

— ISO/IEC 27000 є серією міжнародних стандартів, які визначають вимоги до систем управління інформаційною безпекою (ISMS). Стандарти ISO/IEC 27000 надають рекомендації щодо розробки та експлуатації інформаційних систем з питань керування інформаційною безпекою, захисту від несанкціонованого доступу, кібербезпеки, криптографічного захисту інформації, захисту персональних даних. Також Україна працює над впровадженням сучасних міжнародних стандартів інформаційної безпеки, насамперед серії міжнародних стандартів ISO/IEC 27000.

— ISO/IEC 27001: Цей стандарт визначає систему управління інформаційною безпекою. Він надає загальні вимоги та рекомендації для створення, впровадження, експлуатації, моніторингу, оцінки, підтримки та покращення систем управління інформаційною безпекою. ISO/IEC 27001

забезпечує комплексний підхід до кібербезпеки та включає аспекти, такі як керування ризиками, фізична безпека, безпека персоналу, захист від зловживання, безпека мережі та інші.

— NIST Cybersecurity Framework (CSF): Розроблений Національним інститутом стандартів і технологій (NIST) у США, CSF є добровільним набором керівництва та вказівок щодо кібербезпеки. Він визначає основні принципи та підходи до кібербезпеки, такі як ідентифікація, захист, виявлення, відповідь та відновлення. CSF може бути використаний організаціями для розробки своїх власних програм кібербезпеки та оцінки рівня безпеки.

— IEC 62443: Цей стандарт, розроблений Міжнародною електротехнічною комісією (IEC), спеціалізується на кібербезпеці промислових автоматизованих систем, включаючи об'єкти критичної інфраструктури. IEC 62443 встановлює вимоги та рекомендації щодо безпеки інформаційних технологій та систем у промисловому середовищі. Він охоплює аспекти, такі як архітектура безпеки, ідентифікація загроз, керування ризиками та заходи безпеки.

— GDPR (Загальний регламент про захист персональних даних): GDPR є європейським законодавством, що стосується захисту персональних даних. Він встановлює правила щодо збору, обробки та зберігання персональних даних громадян Європейського союзу. GDPR накладає вимоги щодо безпеки персональних даних, включаючи заходи захисту, забезпечення конфіденційності та інші принципи кібербезпеки.

Ці стандарти та норми є лише деякими прикладами міжнародних регулятивних документів у сфері кібербезпеки. Країни та регіони можуть також мати свої власні внутрішні норми та законодавство, спрямовані на захист об'єктів критичної інфраструктури та інформаційних систем. Важливо дотримуватись цих вимог та забезпечувати відповідність з регуляторними вимогами для забезпечення ефективного кібербезпекового захисту.

ISO/IEC 27001:

Приклад: Організація використовує ISO/IEC 27001 для розробки та впровадження політик, процедур та контролів, щоб забезпечити

конфіденційність, цілісність та доступність своїх критичних інформаційних ресурсів.

NIST Cybersecurity Framework (CSF):

Приклад: Організація використовує CSF для ідентифікації критичних активів, оцінки ризиків та розробки заходів щодо захисту від загроз, наприклад, шляхом впровадження високоризикових патчів безпеки.

IEC 62443:

Приклад: Виробничий завод використовує IEC 62443 для встановлення безпечних мереж, захисту промислових контролерів та моніторингу систем на предмет виявлення кібератак.

GDPR (Загальний регламент про захист персональних даних):

Приклад: Оператор телекомунікаційних послуг відповідає вимогам GDPR, що стосуються захисту особистих даних клієнтів, включаючи шифрування передачі даних та забезпечення доступу до них лише для авторизованих осіб.

Ці приклади показують, як ці міжнародні стандарти та норми застосовуються в реальних ситуаціях. Кожен з цих стандартів надає рамки та рекомендації, які допомагають організаціям забезпечити належний рівень кібербезпеки своїх об'єктів критичної інфраструктури. Проте, важливо зазначити, що кожна країна або регіон може мати свої власні специфічні нормативні акти і стандарти, які також слід дотримуватися для забезпечення відповідності та ефективного захисту кібербезпеки.

1.3 Аналіз існуючих політик безпеки для об'єктів критичної інфраструктури

Дослідження політик безпеки національних та міжнародних організацій є важливим аспектом кібербезпеки. Організації розробляють та впроваджують політики, які визначають підходи та стратегії для захисту своїх інформаційних систем та об'єктів критичної інфраструктури. Розглянемо дослідження політик безпеки національних та міжнародних організацій [4].

1. Національні політики безпеки:

Багато країн розробляють свої власні національні політики безпеки, які визначають вимоги та стратегії для кібербезпеки нації в цілому. Ці політики можуть охоплювати аспекти, такі як захист критичної інфраструктури, захист державних інформаційних ресурсів, кібероборону та співпрацю з іншими країнами щодо кібербезпеки. Дослідження таких політик дозволяє краще зрозуміти підходи та прийняті стратегії країн у сфері кібербезпеки.

2. Міжнародні організації:

Міжнародні організації, такі як ООН, ЄС, НАТО та Інтерпол, також займаються розробкою та впровадженням політик безпеки, спрямованих на забезпечення кібербезпеки на міжнародному рівні. Ці організації співпрацюють з країнами-членами та іншими зацікавленими сторонами для розробки стандартів, рекомендацій та спільних стратегій кібербезпеки. Дослідження політик цих організацій допомагає з'ясувати глобальні тенденції та спрямування в сфері кібербезпеки.

Під час дослідження політик безпеки національних та міжнародних організацій проводяться аналізи, огляди та порівняння стратегій, підходів та регуляторних рамок. Це дозволяє виявити сильні та слабкі сторони політик, ідентифікувати кращі практики та визначити прогалини у кібербезпеці. Такі дослідження сприяють обміну досвідом та підвищенню рівня кібербезпеки як на національному, так і на міжнародному рівнях.

Оцінка ефективності і достатності політик безпеки для об'єктів критичної інфраструктури є важливим етапом у забезпеченні належного рівня кібербезпеки. Цей процес допомагає визначити, наскільки ефективні та адекватні політики, що вживаються для захисту об'єктів критичної інфраструктури від кіберзагроз.

Оцінка ефективності політик безпеки для об'єктів критичної інфраструктури передбачає наступні кроки:

1. Аналіз загроз: Проводиться оцінка потенційних кіберзагроз, якими можуть бути піддані об'єкти критичної інфраструктури. Це включає аналіз існуючих загроз, трендів у кібербезпеці та потенційних ризиків.

2. Оцінка сильних та слабких сторін політик: Визначаються переваги та недоліки наявних політик безпеки, які застосовуються до об'єктів критичної інфраструктури. Це може включати оцінку потенційних ризиків, заходів безпеки, контрольних механізмів та впровадження стандартів кібербезпеки.

3. Вимоги та стандарти: Порівнюються наявні політики безпеки з вимогами та стандартами кібербезпеки, які визначені національними та міжнародними організаціями. Це може включати перевірку відповідності до таких стандартів, як ISO/IEC 27001, NIST Cybersecurity Framework, IEC 62443 та інших.

4. Аудит безпеки: Проводиться аудит системи безпеки для перевірки її ефективності та достатності. Це може включати технічний аудит, перевірку вразливостей, тестування проникнення та інші методи для оцінки рівня захищеності системи.

5. Рекомендації та вдосконалення: На основі отриманих результатів формулюються рекомендації для вдосконалення політик безпеки. Це може включати розробку нових політик, впровадження додаткових заходів безпеки, навчання персоналу та посилення контрольних механізмів.

Прикладом оцінки ефективності політик безпеки може бути ситуація, коли організація з критичною інфраструктурою піддається серйозній кібератакі, проти якої наявні політики безпеки не були достатньо ефективними. Після події проводиться аналіз причин порушення безпеки та оцінка політик безпеки, щоб визначити недоліки та вжити необхідні заходи для поліпшення системи захисту.

Оцінка ефективності та достатності політик безпеки дозволяє покращити кібербезпеку об'єктів критичної інфраструктури, зменшити ризики кібератак та забезпечити належний рівень захисту інформаційних систем. Вона є невід'ємною частиною стратегії кібербезпеки та постійного вдосконалення політик безпеки з метою протидії зростаючим загрозам у кіберпросторі.

Виявлення потреб у поліпшенні та удосконаленні існуючих політик безпеки є важливим етапом у забезпеченні ефективного захисту об'єктів критичної інфраструктури. Цей процес дозволяє ідентифікувати недоліки,

прогалини та виклики, з якими стикаються наявні політики, і визначити області, які потребують поліпшення. Розглянемо деякі аспекти виявлення потреб у поліпшенні та удосконаленні існуючих політик безпеки.

Аналіз кіберзагроз: Проведення аналізу кіберзагроз є ключовим для виявлення потреб у поліпшенні політик безпеки. Це включає огляд сучасних тенденцій у кібербезпеці, нових видів атак, вразливостей і методів, що використовуються злочинцями. Аналіз кіберзагроз допомагає ідентифікувати потенційні ризики, якими забезпечення наявних політик безпеки може бути недостатнім.

Оцінка прогалин та недоліків: Ретельний аналіз наявних політик безпеки допомагає виявити прогалини та недоліки. Це може включати оцінку регуляторного середовища, технічних заходів безпеки, процедур управління і реагування на інциденти, навичок персоналу та урахування інших факторів, які можуть впливати на ефективність політик безпеки.

Зворотний зв'язок від зацікавлених сторін: Отримання зворотного зв'язку від зацікавлених сторін є важливим для виявлення потреб у поліпшенні політик безпеки. Це може включати зворотній зв'язок від операторів критичної інфраструктури, експертів з кібербезпеки, правоохоронних органів та інших стейкхолдерів, які мають прямий інтерес у забезпеченні належного рівня кібербезпеки.

Стандарти та рекомендації: Врахування вимог міжнародних та національних стандартів кібербезпеки та рекомендацій організацій з кібербезпеки допомагає виявити потреби у поліпшенні політик безпеки. Це може включати порівняння існуючих політик з вимогами та принципами, закладеними в таких стандартах як ISO/IEC 27001, NIST Cybersecurity Framework, IEC 62443 та інших.

Моніторинг інцидентів: Аналіз інцидентів, пов'язаних з кібербезпекою, допомагає виявити потреби у поліпшенні політик безпеки. Це включає вивчення причин і наслідків інцидентів, оцінку ефективності застосованих заходів безпеки та розробку відповідних рекомендацій для поліпшення системи захисту.

Прикладом потреби у поліпшенні політик безпеки може бути ситуація, коли під час кібератаки виявлено прогалини в заходах безпеки, які не були передбачені наявними політиками. Внаслідок цього інфраструктура була піддана серйозним наслідкам. Аналіз цього інциденту може виявити необхідність удосконалення політик безпеки, удосконалення контрольних механізмів, навчання персоналу та реакції на подібні загрози в майбутньому.

Виявлення потреб у поліпшенні та удосконаленні існуючих політик безпеки є постійним процесом, який допомагає забезпечити адаптацію до швидкозмінюючого кіберзлочинного середовища та забезпечити належний рівень захисту для об'єктів критичної інфраструктури.

1.4 Методологія дослідження

Проведення аналізу стану безпеки об'єкта критичної інфраструктури включає в себе використання різних методів та підходів, які допомагають визначити потенційні загрози, вразливості та ризики. Розглянемо деякі з них:

Аудит безпеки: Аудит безпеки є процесом систематичного огляду і оцінки безпекових заходів та процедур, що застосовуються на об'єкті критичної інфраструктури. Цей підхід включає перевірку відповідності наявних заходів безпеки вимогам і стандартам, ідентифікацію можливих недоліків та розробку рекомендацій для поліпшення системи захисту.

Пенетраційне тестування: Пенетраційне тестування, або тестування на проникнення, включає в себе спробу проникнути в систему або мережу об'єкта критичної інфраструктури з метою виявлення вразливостей та потенційних проблем безпеки. Цей метод дозволяє оцінити, наскільки ефективно захищений об'єкт від реальних кібератак.

Аналіз ризиків: Аналіз ризиків включає в себе ідентифікацію потенційних загроз та оцінку ймовірності їх виникнення та впливу на безпеку об'єкта критичної інфраструктури. Цей підхід дозволяє визначити найбільш критичні області та розробити стратегії мінімізації ризиків.

Аналіз ланцюжків постачання: Аналіз ланцюжків постачання оцінює безпеку всіх елементів, учасників та процесів, що становлять ланцюжок постачання об'єкта критичної інфраструктури. Це включає оцінку ризиків, пов'язаних з постачальниками, підрядними організаціями та іншими сторонами, що мають доступ до системи.

Оцінка вразливостей: Оцінка вразливостей полягає у виявленні та аналізі потенційних вразливостей і слабких місць в системі безпеки об'єкта критичної інфраструктури. Цей підхід дозволяє виявити проблемні аспекти та розробити відповідні заходи для їх усунення або пом'якшення наслідків.

Аналіз злочинної діяльності: Аналіз злочинної діяльності включає в себе вивчення типових кіберзлочинів та методів, які використовуються злочинцями. Цей підхід допомагає виявити потенційні загрози та надати рекомендації з удосконалення системи безпеки.

Ці методи та підходи сприяють отриманню глибокого і всебічного розуміння стану безпеки об'єкта критичної інфраструктури. Комбінування різних підходів дозволяє отримати більш точну і повну картину загроз та проблем безпеки, що допомагає розробити належні стратегії та заходи для їх запобігання та усунення.

Встановлення критеріїв та показників оцінки безпеки об'єкта критичної інфраструктури є важливим етапом для об'єктивної оцінки рівня безпеки та визначення прийнятних ризиків. Нижче наведено деякі основні критерії та показники, які можуть бути використані для цієї цілі:

Конфіденційність: Цей критерій відображає рівень захищеності інформації об'єкта критичної інфраструктури від несанкціонованого доступу. Показники оцінки можуть включати вимоги до захисту конфіденційної інформації, рівень шифрування даних, політики доступу та аутентифікації.

Цілісність: Цей критерій відображає рівень захисту об'єкта від несанкціонованої зміни або модифікації даних. Показники можуть включати вимоги до контролю цілісності даних, захисту від вторгнень, контролю доступу та системи виявлення вторгнень.

Доступність: Цей критерій відображає здатність об'єкта критичної інфраструктури функціонувати без перебоїв та забезпечувати доступ до необхідних ресурсів. Показники можуть включати вимоги до доступності систем, резервування та відновлення послуг, захисту від DDoS-атак та регулярного тестування систем на доступність.

Автентичність: Цей критерій відображає рівень довіри до ідентифікації та автентифікації користувачів та систем. Показники можуть включати вимоги до сильної аутентифікації, захисту від підробки ідентифікаційних даних та аудиту активності користувачів.

Відновлюваність: Цей критерій відображає здатність об'єкта критичної інфраструктури відновлюватися після інциденту чи катастрофи. Показники можуть включати вимоги до резервного копіювання даних, планів відновлення, мінімізації впливу інцидентів та системи моніторингу стану об'єкта.

Ці критерії та показники є лише загальними і можуть бути адаптовані до конкретних потреб та характеристик об'єкта критичної інфраструктури. Оцінка безпеки здійснюється на основі цих критеріїв і показників шляхом зібрання відповідної інформації, аналізу ідентифікованих ризиків та виявлення недоліків у системі безпеки.

Під час дослідження оцінки безпеки об'єкта критичної інфраструктури буде використано наступні методологічні принципи:

Інтегрований підхід: Дослідження використовувало інтегрований підхід, що охоплював різні аспекти безпеки об'єкта критичної інфраструктури, включаючи технічні, організаційні та людські фактори. Цей підхід дозволяв оцінити безпеку як комплексну систему і враховувати взаємозв'язки між різними елементами.

Ризик-орієнтований підхід: Дослідження базувалося на ризик-орієнтованому підході, який визнавав, що оцінка безпеки повинна бути спрямована на ідентифікацію, аналіз та управління ризиками. Для цього було використано методи оцінки ризиків, включаючи аналіз ймовірності і наслідків потенційних загроз, а також ідентифікацію заходів для їх усунення або зниження.

Системний підхід: Дослідження використовувало системний підхід, що дозволяв розглядати об'єкт критичної інфраструктури як складну систему, в якій взаємодіють різні компоненти та процеси. Це дозволило зрозуміти взаємозв'язки та взаємовплив між різними аспектами безпеки та виявити слабкі місця.

Експертний підхід: В дослідженні було використано експертний підхід, що передбачав залучення кваліфікованих фахівців з області безпеки для збору інформації, аналізу потенційних загроз та розробки рекомендацій щодо поліпшення безпеки об'єкта. Експертний підхід дозволив врахувати специфічні особливості об'єкта та використовувати глибокі знання та досвід експертів.

Застосування стандартів та рекомендацій: Дослідження використовувало визнані міжнародні стандарти та рекомендації з кібербезпеки для проведення оцінки безпеки об'єкта. Це дозволило забезпечити об'єктивність та порівнянність результатів оцінки.

Використання цих методологічних принципів дозволило здійснити аналіз стану безпеки об'єкта критичної інфраструктури з достатньою точністю та об'єктивністю.

1.5 Висновки по розділу

Дослідження безпеки об'єктів критичної інфраструктури є надзвичайно важливим завданням, яке вимагає комплексного підходу та використання методів оцінки, аналізу та покращення стану безпеки. У цьому розділі було розглянуто різноманітні аспекти, включаючи визначення об'єктів критичної інфраструктури, нормативно-правове забезпечення, вимоги до кібербезпеки, порівняння з міжнародними стандартами, політики безпеки та оцінку ефективності політик безпеки.

Під час дослідження було проаналізовано інтегрований, ризик-орієнтований, системний та експертний підходи, а також стандарти та рекомендації з кібербезпеки. Це дозволить провести аналіз стану безпеки об'єктів критичної інфраструктури, ідентифікувати ризики, виявити недоліки та розробити рекомендації щодо покращення безпеки.

2 РОЗРОБКА МОДЕЛІ ПОЛІТИКИ БЕЗПЕКИ ДЛЯ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Однією з найважливіших сфер в сучасному світі є критична інфраструктура, яка включає енергетичні системи, транспортні мережі, телекомунікаційні системи, фінансові установи та інші об'єкти, що забезпечують життєво важливі послуги та функціонування суспільства. Проте, разом зі зростанням комп'ютеризації та підключенням до мережі Інтернет, з'являються серйозні проблеми безпеки цих об'єктів, які стають все більш вразливими перед атаками та кіберзлочинністю.

Одна з основних проблем безпеки об'єктів критичної інфраструктури полягає у відсутності адекватних заходів та політик безпеки. Багато з цих об'єктів були споруджені та функціонують десятиліттями, коли комп'ютерні загрози були менш поширеними. Внаслідок цього, багато систем критичної інфраструктури мають застарілі архітектури, вразливості та слабкі місця, які можуть бути використані хакерами для злому та нанесення шкоди [5].

Брак політик безпеки створює серйозну загрозу безпеці критичної інфраструктури. Відсутність чітких вимог щодо захисту інформації, контролю доступу, виявлення та реагування на інциденти, а також відсутність регулярного аудиту та оновлення системи безпеки може призвести до катастрофічних наслідків. Наприклад, атаки на енергетичні системи можуть призвести до відключення електроенергії в широких масштабах, створити хаос та негативно вплинути на безпеку громадян.

Одним із шляхів вирішення цієї проблеми є розробка та впровадження моделі політики безпеки для об'єктів критичної інфраструктури. Така модель повинна включати набір строгих інструкцій та стандартів, які вимагатимуть відповідної організації встановлення та підтримки безпеки на необхідному рівні. Вона повинна охоплювати такі аспекти, як кіберзахист, фізична безпека, управління ризиками, виявлення та відновлення після інцидентів.

Модель політики безпеки - це документ, який визначає правила, процедури та контрольні заходи, що забезпечують безпеку об’єктів критичної

інфраструктури. Цей документ містить інформацію про те, як об’єкти критичної інфраструктури повинні захищатися від різних загроз, таких як кібератаки, фізичні атаки, природні катастрофи тощо.

Розробка моделі політики безпеки для об’єктів критичної інфраструктури - це складний процес, який включає кілька етапів. Один з перших етапів - це аналіз ризиків. На цьому етапі проводиться оцінка потенційних загроз для об’єктів критичної інфраструктури та їх можливих наслідків. Це допомагає визначити, яким чином об’єкти критичної інфраструктури можуть бути атаковані та як цього можна уникнути.

Наступний етап — це визначення вимог безпеки. На цьому етапі встановлюються стандарти та процедури, яким повинні відповідати об’єкти критичної інфраструктури для забезпечення їх безпеки. Це може включати вимоги до фізичної безпеки (наприклад, контроль доступу, охорона), кібербезпеки (наприклад, захист мережі, шифрування даних) та управління ризиками (наприклад, планування надзвичайних ситуацій).

Останнім етапом є розробка стандартів та процедур. На цьому етапі формуються конкретні правила та інструкції, яким повинні слідувати об’єкти критичної інфраструктури для забезпечення їх безпеки. Це може включати процедури реагування на інциденти, плани відновлення після аварій тощо.

Розробка моделі політики безпеки для об’єктів критичної інфраструктури - це складний та багатоетапний процес. Важливо регулярно переглядати та оновлювати модель політики безпеки, щоб вона враховувала нові загрози та виклики.

Деякі приклади конкретних заходів безпеки, які можуть бути включені до моделі політики безпеки для об’єктів критичної інфраструктури:

1. Кібербезпека:

— захист мережі: встановлення межевих брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), систем захисту від DDoS-атак;

— шифрування даних: використання сильних алгоритмів шифрування для захисту конфіденційної інформації, такої як паролі, фінансові дані тощо;

— аутентифікація та контроль доступу: використання багатофакторної аутентифікації для підтвердження особи користувача, обмеження доступу до ресурсів на основі ролей та привілеїв.

2. Фізична безпека:

— контроль доступу: встановлення систем контролю доступу, таких як картки доступу, біометричні сканери тощо, для обмеження доступу до об’єктів критичної інфраструктури;

— встановлення камер спостереження: використання камер спостереження для моніторингу території об’єктів критичної інфраструктури та виявлення несанкціонованого доступу;

— охорона: наймання охоронців для фізичного захисту об’єктів критичної інфраструктури.

3. Управління ризиками:

— регулярний аудит системи безпеки: проведення регулярних перевірок системи безпеки для виявлення слабких місць та потенційних загроз;

— планування надзвичайних ситуацій: розробка планів дій у разі надзвичайних ситуацій, таких як пожежа, землетрус, кібератака тощо;

— оцінка ризиків: проведення регулярної оцінки ризиків для ідентифікації потенційних загроз та визначення заходів для їх запобігання або мінімізації наслідків.

Впровадження моделі політики безпеки для об’єктів критичної інфраструктури — це складний процес, який вимагає значних ресурсів, в тому числі фінансових. Ось деякі аспекти фінансування, які слід врахувати при впровадженні моделі політики безпеки:

— вартість розробки моделі: розробка моделі політики безпеки може вимагати залучення експертів з різних галузей, таких як кібербезпека, фізична безпека, управління ризиками тощо. Це може бути коштовним процесом, особливо якщо потрібно залучати консультантів ззовні;

— вартість впровадження заходів безпеки: впровадження конкретних заходів безпеки, таких як захист мережі, шифрування даних, контроль доступу

тощо, також може бути коштовним. Наприклад, може знадобитися придбання нового обладнання, програмного забезпечення або послуг;

— вартість підготовки персоналу: для ефективного впровадження моделі політики безпеки необхідно підготувати персонал об’єктів критичної інфраструктури. Це може включати навчання з питань кібербезпеки, фізичної безпеки, управління ризиками тощо;

— вартість моніторингу та оцінки ефективності: після впровадження моделі політики безпеки необхідно регулярно моніторити її ефективність та вносити необхідні зміни. Це може включати регулярні аудити системи безпеки, тестування на проникнення, опитування персоналу тощо. Цей процес також може бути коштовним, особливо якщо потрібно залучати експертів ззовні.

У підсумку, впровадження моделі політики безпеки для об’єктів критичної інфраструктури - це складний та коштовний процес. Однак витрати на впровадження моделі політики безпеки можуть бути значно меншими, ніж потенційні збитки від атак на об’єкти критичної інфраструктури. Тому фінансування моделі політики безпеки повинно бути пріоритетом для організацій, які відповідають за об’єкти критичної інфраструктури.

Висновок, безпека об'єктів критичної інфраструктури є надзвичайно важливим завданням у сучасному світі. Проблеми безпеки цих об'єктів можуть мати серйозні наслідки для суспільства, тому необхідно розробляти та впроваджувати моделі політики безпеки, які забезпечать ефективний захист та функціонування критичної інфраструктури.

2.1 Недоліки існуючих підходів до забезпечення безпеки об'єктів критичної інфраструктури

Існуючі підходи до забезпечення безпеки об'єктів критичної інфраструктури мають деякі недоліки та обмеження, які важливо враховувати. Ось кілька недоліків існуючих підходів:

1. Реактивний підхід: Багато підходів до безпеки об'єктів критичної інфраструктури ґрунтуються на реактивному підході, тобто реагують на

виявлені загрози та інциденти. Це означає, що заходи безпеки приймаються після виникнення проблеми, що може призвести до значних затримок у реагуванні та можливих наслідків.

2. Фрагментація та відсутність стандартів: У багатьох випадках безпека об'єктів критичної інфраструктури відповідає окремим організаціям або секторам, що призводить до фрагментації заходів безпеки та відсутності єдиних стандартів. Це ускладнює співпрацю та обмін інформацією, а також може створювати прогалини в безпеці між різними секторами.

3. Відсутність узгодженої стратегії: Безпека об'єктів критичної інфраструктури часто відповідає різним зацікавленим сторонам, таким як урядові органи, приватні компанії та регулятори. Відсутність узгодженої стратегії та спільного плану дій може призводити до розбіжностей та недосягнення загальної безпекової мети.

4. Виклики кібербезпеки: Зростання кіберзагроз та кібератак ставлять під загрозу безпеку об'єктів критичної інфраструктури. Кіберзлочинці постійно вдосконалюють свої методи та технології, що ускладнює завдання захисту. Брак адекватних захисних заходів та недостатня кібербезпекова свідомість персоналу можуть вразити критичну інфраструктуру.

5. Фінансові обмеження: Забезпечення безпеки об'єктів критичної інфраструктури може потребувати значних інвестицій, які можуть бути обмеженими у фінансовому плані. Брак фінансових ресурсів може ускладнювати оновлення систем безпеки, підготовку персоналу та впровадження сучасних технологій.

Враховуючи ці недоліки, важливо розробляти комплексні підходи до безпеки об'єктів критичної інфраструктури, які передбачають превентивні заходи, стандартизацію, співпрацю та використання сучасних технологій.

Недоліки існуючих підходів до забезпечення безпеки об'єктів критичної інфраструктури можуть викликати потенційні проблеми, які варто виявити та вирішити. Ось кілька потенційних проблем, що можуть виникнути з недоліків [6]:

Загрози безпеці: Недоліки у заходах безпеки можуть створювати прогалини, через які зловмисники можуть здійснити атаки на об'єкти критичної інфраструктури. Це може призвести до перерв у роботі систем, витоку конфіденційної інформації або навіть загрози для життя та безпеки людей.

Збільшення ризиків: Недоліки в підходах до безпеки можуть збільшити ризик виникнення інцидентів та збитків. Наприклад, застаріле обладнання або вразливості в програмному забезпеченні можуть зробити систему більш уразливою перед атаками та несправностями.

Втрата довіри: Недостатня безпека об'єктів критичної інфраструктури може призвести до втрати довіри з боку громадськості, клієнтів та інших зацікавлених сторін. Це може мати негативні наслідки для репутації організації або сектора, а також може позначитися на економічному та соціальному розвитку.

Правові проблеми: Недоліки в підходах до безпеки можуть порушувати законодавство, що регулює безпеку об'єктів критичної інфраструктури. Наприклад, недотримання вимог щодо захисту персональних даних або використання несанкціонованих методів моніторингу може призвести до правових проблем та санкцій.

Економічні втрати: Недоліки в безпеці можуть мати серйозні економічні наслідки. Наприклад, інциденти та перерви в роботі можуть спричинити значні фінансові збитки, втрату прибутку, ремонтні та відновлювальні витрати.

Виявлення цих потенційних проблем є важливим кроком для покращення безпеки об'єктів критичної інфраструктури. Це дозволяє розуміти ризики, виявляти вразливості та вчасно вживати заходів для запобігання інцидентам та забезпечення надійної захищеності.

Удосконалення існуючих підходів до забезпечення безпеки об'єктів критичної інфраструктури та розробка нової моделі політики безпеки є критично важливими завданнями. Ось кілька аргументів, що підтверджують цю потребу:

Зростання загроз: Загрози безпеці, включаючи фізичні та кібератаки, продовжують зростати в своїй складності та обсязі. Змінюючіться стратегії

зловмисників вимагають постійного оновлення та удосконалення підходів до безпеки. Нова модель політики безпеки дозволить адаптуватись до сучасних загроз і враховувати їх усі аспекти.

Комплексність інфраструктури: Сучасна критична інфраструктура стає все більш складною і взаємопов'язаною. Це вимагає гармонізації та координації заходів безпеки на різних рівнях і серед різних суб'єктів. Нова модель політики безпеки дозволить створити системний підхід, який охоплюватиме всі аспекти безпеки і сприятиме кращій координації між різними організаціями та секторами.

Запобігання перед інцидентами: Реактивний підхід до безпеки має свої обмеження, оскільки вимагає виникнення проблеми або інциденту, щоб вживати заходи. Нова модель політики безпеки буде спрямована на запобігання перед можливими загрозами та проблемами, шляхом реалізації превентивних заходів, збільшення свідомості про безпеку та впровадження передових технологій.

Гарантування довіри та стабільності: Безпека об'єктів критичної інфраструктури є важливою складовою для забезпечення довіри громадськості, стабільності суспільства та розвитку економіки. Покращення існуючих підходів та розробка нової моделі політики безпеки допоможуть зберегти довіру громадськості, знизити ризик інцидентів та забезпечити стабільну роботу критичної інфраструктури.

Відповідність нормативним вимогам: Розвиток нової моделі політики безпеки дозволить організаціям відповідати сучасним нормативним вимогам у сфері безпеки. Законодавство та регуляторні вимоги щодо безпеки постійно змінюються і розвиваються, тому необхідно актуалізувати підходи та політику безпеки, щоб відповідати цим вимогам.

Враховуючи ці аргументи, удосконалення існуючих підходів та розробка нової моделі політики безпеки є необхідними для забезпечення ефективного захисту об'єктів критичної інфраструктури та забезпечення безпеки суспільства в цілому.

2.2 Типи загроз та методологія оцінювання ризиків для об'єктів критичної інфраструктури

Огляд типових загроз та потенційних загроз безпеці об'єктів критичної інфраструктури розкриває широкий спектр можливих небезпек, з якими можуть стикнутися ці об'єкти. Отже, нижче наведено докладний опис цих загроз [7].

Фізичні атаки: Об'єкти критичної інфраструктури, такі як електростанції, транспортні мережі, газопроводи та водопостачання, можуть стати метою фізичних атак. Це можуть бути напади терористів, саботажні дії, вандалізм або навіть природні катастрофи, такі як землетруси або повені.

Кібератаки: У сучасному цифровому світі кібератаки стають все більш поширеними загрозами для об'єктів критичної інфраструктури. Хакери можуть спробувати зламати системи управління, мережеву інфраструктуру або проникнути до систем керування процесами. Це може призвести до відключення об'єктів від електропостачання, порушення роботи транспортних мереж або навіть викликати аварійні ситуації [8].

Виток інформації: Зловмисники можуть намагатися отримати неправомірний доступ до конфіденційної інформації про об'єкти критичної інфраструктури, такої як плани, дизайни або критичні деталі. Це може створити ризик для безпеки, відкрити можливості для здійснення атак або підриву надійності систем.

Соціальні загрози: Більш складними загрозами є соціальні атаки, які включають фактори, такі як внутрішній шпигунський діяч, недостовірний персонал або соціальний інжиніринг. Наприклад, зловмисники можуть використовувати соціальні мережі або фізичний доступ до об'єкту для отримання неправомірного доступу або здійснення атаки зсередини.

Екологічні загрози: Об'єкти критичної інфраструктури також можуть бути під загрозою від природних чинників, які можуть спричинити аварії або пошкодження систем. Це можуть бути стихійні лиха, такі як урагани, повені або пожежі, які можуть призвести до зупинки роботи об'єктів та значних матеріальних збитків.

Загрози з боку постачальників: Об'єкти критичної інфраструктури можуть бути уразливими через ненадійних або небезпечних постачальників. Наприклад, постачальник електроенергії або водопостачання може стати джерелом загрози, включаючи зламані системи або недостатній контроль якості.

Технічні проблеми: Збій у роботі систем, технічні помилки або відмови обладнання також можуть призвести до проблем безпеки об'єктів критичної інфраструктури. Неналежне управління обладнанням, відсутність резервних систем або несправність можуть створити загрозу безпеці та надійності об'єктів.

Ці загрози не є вичерпним переліком, але наводять приклади різноманітності небезпек, з якими стикаються об'єкти критичної інфраструктури. Розуміння цих загроз і їх потенційних наслідків є важливим кроком для розробки ефективної моделі політики безпеки, яка забезпечуватиме надійний захист інфраструктури та захист суспільства в цілому.

Методологія оцінювання ризиків є важливим інструментом для ідентифікації, аналізу та управління ризиками в різних сферах діяльності, включаючи безпеку об'єктів критичної інфраструктури. Оцінка ризиків допомагає визначити потенційні загрози, виявити їх вплив на систему, оцінити рівень ризику та прийняти необхідні заходи для зменшення ризику. Нижче буде описано процес оцінювання ризиків та деякі методи, які використовуються в цьому процесі.

Процес оцінювання ризиків складається з кількох етапів, починаючи з ідентифікації потенційних загроз. На цьому етапі проводиться аналіз і виявлення можливих небезпек, які можуть впливати на об'єкт критичної інфраструктури. Це можуть бути фізичні загрози, кібератаки, природні лиха, соціальні загрози та інші фактори, що можуть порушити безпеку об'єкта.

Наступним кроком є оцінка ймовірності виникнення загрози. Для цього використовуються методи аналізу статистичних даних, експертних оцінок або моделювання подій. Оцінка ймовірності допомагає визначити, наскільки часто може виникнути певна загроза і які ресурси можуть бути задіяні для її запобігання.

Далі проводиться аналіз впливу загрози на систему. Це оцінюється за різними критеріями, такими як фінансові втрати, втрата життя, зниження продуктивності або репутаційні ризики. Аналіз впливу дозволяє оцінити наслідки, які можуть виникнути в результаті реалізації загрози.

Після оцінки ймовірності та впливу проводиться оцінка ризику. Ризик визначається як добуток ймовірності та впливу. Цей етап допомагає встановити пріоритети щодо управління ризиками і визначити найбільш критичні області, які потребують негайних заходів.

У процесі оцінювання ризиків використовуються різні методи. Один з них - метод аналізу ієрархій. Метод аналізу ієрархій (MAI) є одним з ключових інструментів при оцінюванні ризиків і прийнятті рішень в різних сферах діяльності. Винайдений Томасом Сааті, MAI дозволяє систематично порівнювати різні альтернативи та критерії на основі експертних оцінок. Цей метод базується на структурованому підході до прийняття рішень, де складні задачі розбиваються на більш прості підзадачі, утворюючи ієрархію.

Процес аналізу ієрархій включає кілька кроків:

1. Визначення цілей: Спочатку необхідно чітко визначити мету аналізу ієрархій і ті цілі, досягнення яких планується. Цілі повинні бути конкретними, зрозумілими і спрямованими на вирішення проблеми чи прийняття рішення.

2. Створення ієрархії: Наступним кроком є створення ієрархії критеріїв і альтернатив. Критерії - це фактори або аспекти, за якими будуть порівнюватись альтернативи. Альтернативи - це різні варіанти рішень або дій, які можуть бути вибрані. Ієрархія включає багато рівнів, де на верхньому рівні знаходиться основна ціль, а на нижчих рівнях - під критерії і альтернативи.

3. Парний порівняльний аналіз: Для кожного рівня ієрархії експерти здійснюють парні порівняння, оцінюючи важливість одного елемента відносно іншого. Зазвичай використовується шкала від 1 до 9, де 1 означає, що елементи мають однакову важливість, а 9 - що один елемент значно переважає інший. Ці оцінки базуються на суб'єктивних експертних знаннях і досвіді.

4. Розрахунок ваг критеріїв: На основі парних порівнянь ваг критеріїв обчислюються за допомогою математичного алгоритму. Цей алгоритм використовується для визначення відносних ваг критеріїв відносно основної цілі.

5. Розрахунок пріоритетів альтернатив: Після отримання ваг критеріїв розраховуються пріоритети альтернатив для кожного критерію. Цей крок виконується шляхом порівняння альтернатив згідно з вагами критеріїв.

6. Синтез результатів: За допомогою математичних розрахунків і порівнянь отримується комплексна оцінка альтернатив та розраховується їхній загальний пріоритет.

Метод аналізу ієрархій дозволяє систематизувати складні задачі прийняття рішень і забезпечує об'єктивність шляхом врахування експертних оцінок. Він забезпечує структурований підхід до прийняття рішень і допомагає уникнути підпливу особистих уподобань або суб'єктивних оцінок. Метод аналізу ієрархій є потужним інструментом для прийняття обґрунтованих рішень, особливо в контексті оцінювання ризиків та безпеки об'єктів критичної інфраструктури.

Інший метод - розрахунок ризику шляхом оцінки ймовірності та впливу за допомогою статистичних даних та моделювання є ще одним ефективним методом оцінювання ризиків. Цей підхід базується на зборі і аналізі відповідних даних про потенційні загрози та їх вплив на об'єкти критичної інфраструктури.

Першим кроком у цьому методі є збір достовірних статистичних даних, які відображають історичні випадки загроз і їх наслідки. Це можуть бути дані про природні катастрофи, техногенні аварії, кібератаки або інші подібні події, які можуть поставити під загрозу об'єкти критичної інфраструктури. Дані про ймовірність виникнення подій, їх тривалість, розмір збитків і вплив на функціонування об'єктів також використовуються для більш точного оцінювання ризику.

Після збору даних проводиться аналіз, включаючи використання статистичних методів і моделювання. Статистичні методи дозволяють розрахувати ймовірність виникнення подій, що можуть призвести до загрози безпеці об'єктів критичної інфраструктури. Моделювання, у свою чергу,

дозволяє оцінити вплив таких подій на різні аспекти безпеки, включаючи фізичні пошкодження, простірну розповсюдженість збитків, витрати на відновлення тощо.

На основі результатів аналізу ймовірності та впливу визначається ризик для кожної конкретної загрози. Це може бути представлено у вигляді числової оцінки або категорії ризику. Критичні загрози з високим ризиком вимагатимуть негайних заходів для запобігання та мінімізації їх наслідків, тоді як менш критичні загрози можуть потребувати менш суворих заходів або можуть бути прийняті з певними ризиками.

Оцінка ризиків на основі статистичних даних та моделювання дозволяє забезпечити більш об'єктивну оцінку ризиків і допомагає визначити пріоритетність заходів з підвищення безпеки об'єктів критичної інфраструктури. Цей метод дозволяє підтримувати прийняття рішень на основі обґрунтованих даних та прогнозів, що сприяє більш ефективному управлінню ризиками та забезпеченню безпеки об'єктів критичної інфраструктури.

Окрім того, використовуються методи ризик-орієнтованого підходу, де акцент робиться на виявленні найбільш суттєвих загроз та управлінні ними. Метод ризик-орієнтованого підходу є широко використовуваним методом в оцінюванні та управлінні ризиками об'єктів критичної інфраструктури. Цей підхід зосереджений на визначенні й управлінні ризиками, що можуть впливати на безпеку та стійкість таких об'єктів. Опишемо процес методу ризик-орієнтованого підходу та його ключові етапи.

1. Ідентифікація ризиків: Перший етап полягає в ідентифікації потенційних загроз та визначенні факторів, які можуть призвести до небезпеки для об'єктів критичної інфраструктури. Це можуть бути природні катастрофи, технічні відмови, кібератаки, терористичні акти, людські помилки та інші фактори, що можуть спричинити збитки або порушення роботи об'єктів.

2. Оцінка ймовірності та наслідків: На цьому етапі проводиться аналіз ймовірності виникнення ризиків та оцінка потенційних наслідків цих ризиків. Ймовірність може бути оцінена на основі історичних даних, експертних оцінок

або статистичних моделей. Наслідки визначаються шляхом оцінки впливу ризикових подій на безпеку, економіку, навколишнє середовище та інші аспекти.

3. Аналіз ризиків: На цьому етапі проводиться оцінка ризиків шляхом поєднання інформації про ймовірність та наслідки ризикових подій. Це може бути зроблено за допомогою різних методів, таких як матриця ризиків, аналіз сценаріїв, експертні оцінки тощо. Результатом аналізу є визначення рівня ризику для кожного ідентифікованого ризику.

4. Управління ризиками: Після аналізу ризиків важливо прийняти відповідні заходи для управління цими ризиками. Це можуть бути заходи з попередження, захисту, відновлення та моніторингу. Варіанти управління ризиками включають створення планів надзвичайних ситуацій, встановлення системи резервування, підвищення кібербезпеки, проведення навчань та тренувань персоналу.

5. Моніторинг та оновлення: Ризик-орієнтований підхід є процесом, який потребує постійного моніторингу та оновлення. Враховуючи зміну в умовах, нові загрози та технологічний прогрес, важливо систематично оновлювати оцінку ризиків та приймати відповідні корективи у планах управління ризиками.

Метод ризик-орієнтованого підходу дозволяє комплексно оцінювати та управляти ризиками безпеки об'єктів критичної інфраструктури. Його перевагою є те, що він дозволяє систематично враховувати різні фактори ризику та приймати обґрунтовані рішення з підвищення безпеки та стійкості об'єктів.

Усі ці методи допомагають зрозуміти характер ризиків, зв'язані з об'єктами критичної інфраструктури, та визначити ефективні заходи для їх запобігання та управління. Результатом оцінювання ризиків є розробка плану безпеки, який враховує виявлені загрози та необхідні заходи для зменшення ризику та підвищення безпеки об'єкта.

У підсумку, методологія оцінювання ризиків відіграє ключову роль у забезпеченні безпеки об'єктів критичної інфраструктури. Вона допомагає ідентифікувати загрози, оцінювати їх ймовірність та вплив, встановлювати рівень ризику та розробляти ефективні стратегії управління ризиками.

Послідовне застосування методології оцінювання ризиків допомагає забезпечити безпеку об'єктів критичної інфраструктури та зменшити можливі наслідки небезпечних ситуацій.

2.3 Розробка моделі політики безпеки

Бажаний стан безпеки для об'єктів критичної інфраструктури включає забезпечення найвищого рівня захисту, стабільності та надійності. Основні принципи, що визначають бажаний стан безпеки, включають [9]:

1. Конфіденційність інформації: Забезпечення недоступності конфіденційної інформації для несанкціонованих осіб, включаючи зовнішніх зловмисників та внутрішніх загроз.

2. Цілісність інформації: Забезпечення недопущення несанкціонованих змін до інформації та забезпечення цілісності даних, щоб запобігти впливу на надійність та точність.

3. Доступність: Забезпечення безперебійного доступу до систем та послуг, які є важливими для нормального функціонування критичної інфраструктури.

4. Реактивність: Здатність швидко реагувати на виявлені загрози та інциденти безпеки, включаючи виявлення, аналіз та відновлення нормального стану після виникнення подій.

5. Резистентність до атак: Забезпечення високого рівня стійкості до різноманітних видів кібератак, фізичних вторгнень та інших загроз.

6. Своєчасне виявлення загроз: Розробка та впровадження систем виявлення загроз, які здатні оперативно виявляти аномальну активність та потенційні загрози для безпеки.

7. Налагодження системи керування безпекою: Створення і впровадження ефективних політик, процедур та методів управління безпекою, які відповідають найсучаснішим стандартам та найкращим практикам.

Визначення цілей, які треба досягти:

1. Розробка імплементованої моделі політики безпеки: Створення комплексної моделі політики безпеки, яка охоплює всі аспекти захисту об'єктів критичної інфраструктури і відповідає специфічним вимогам і викликам.

2. Визначення інформаційних активів та їх класифікація: Ідентифікація та класифікація всіх інформаційних активів, що належать до критичної інфраструктури, зокрема систем, даних, мереж та іншого обладнання.

3. Виявлення загроз та визначення ризиків: Аналіз потенційних загроз для об'єктів критичної інфраструктури та визначення рівнів ризику, пов'язаних з кожною загрозою.

4. Розробка заходів безпеки: Розробка і впровадження заходів безпеки, які враховують виявлені загрози та ризики. Ці заходи можуть включати технічні, організаційні та процедурні заходи.

5. Впровадження систем моніторингу та виявлення інцидентів: Розробка та впровадження систем моніторингу, які дозволяють виявляти інциденти безпеки та аномальну активність в реальному часі.

6. Навчання та свідомість персоналу: Забезпечення навчання персоналу з питань безпеки, свідомості щодо загроз та виконання політик безпеки.

7. Тестування та аудит безпеки: Проведення регулярних тестів, аудитів та перевірок систем безпеки для виявлення потенційних уразливостей та вдосконалення заходів безпеки.

Ці цілі допоможуть створити потужну та надійну модель політики безпеки, яка забезпечить найвищий рівень захисту об'єктів критичної інфраструктури від сучасних загроз.

Стратегія та процедура для досягнення мети безпеки об'єктів критичної інфраструктури можуть включати наступні кроки:

1. Аналіз і оцінка потенційних загроз і ризиків: Проведення детального аналізу потенційних загроз безпеці об'єктів критичної інфраструктури та оцінка ризиків, пов'язаних з цими загрозами. Цей етап включає ідентифікацію потенційних атак, вразливостей системи та інших факторів, що можуть загрожувати безпеці.

2. Розробка політики безпеки: Створення політики безпеки, яка визначає основні принципи, цілі та стратегію безпеки для об'єктів критичної

інфраструктури. Ця політика повинна включати принципи конфіденційності, цілісності, доступності, реактивності та резистентності до атак.

3. Визначення заходів безпеки: Розробка конкретних заходів безпеки, які відповідають загрозам та ризикам, виявленим на попередньому етапі. Ці заходи можуть включати захист мережі, розробку системи контролю доступу, резервне копіювання даних, шифрування інформації, впровадження систем виявлення вторгнень та інші технічні та організаційні заходи.

4. Впровадження та імплементація: Реалізація заходів безпеки згідно з розробленою політикою. Цей етап включає встановлення технічних заходів, навчання персоналу, налагодження процедур та контрольних механізмів.

5. Моніторинг та аудит безпеки: Встановлення системи моніторингу та аудиту безпеки для постійного виявлення інцидентів та оцінки ефективності заходів безпеки. Цей етап включає постійний контроль стану безпеки, виявлення аномальної активності, аналіз журналів подій та регулярні аудити систем безпеки.

6. Реагування на інциденти: Розробка процедур та планів реагування на інциденти безпеки, які включають в себе швидке виявлення, реагування та відновлення нормального стану. Ці процедури повинні бути чіткими і передбачати дії персоналу в разі виникнення загрози або інциденту.

7. Постійне вдосконалення: Забезпечення постійного вдосконалення стратегії та процедур безпеки на основі змін у загрозах та технологіях. Цей етап включає аналіз нових загроз, оновлення політик та заходів безпеки, а також постійне навчання персоналу.

Ця стратегія та процедура допоможуть забезпечити високий рівень безпеки об'єктів критичної інфраструктури та ефективну реакцію на потенційні загрози. Варто зазначити, що кожен об'єкт може мати свої особливості, тому розробка конкретних деталей стратегії безпеки повинна здійснюватись відповідно до його потреб та контексту.

Визначення ролей різних сторін та їх обов'язків у виконанні політики безпеки об'єктів критичної інфраструктури може включати наступні аспекти:

1. Менеджмент:

— визначення стратегії безпеки та встановлення політики безпеки:

— визначення метрик та критеріїв оцінки ефективності політики безпеки:

— забезпечення належного фінансування та ресурсів для реалізації політики безпеки:

— встановлення системи моніторингу та звітності щодо стану безпеки.

2. IT-відділ/спеціалісти з безпеки:

— розробка та впровадження технічних заходів безпеки, включаючи захист мережі, розробку систем контролю доступу, виявлення вторгнень, шифрування даних тощо:

— проведення регулярних аудитів безпеки та перевірок систем на наявність вразливостей та забезпечення вдосконалення заходів безпеки:

— впровадження систем моніторингу та виявлення інцидентів, а також відповідне реагування на них:

— підтримка та надання консультацій з питань безпеки іншим відділам та персоналу.

3. Відділ ресурсів людських:

— організація навчання та підвищення обізнаності персоналу з питань безпеки:

— впровадження політик та процедур, пов'язаних із захистом конфіденційної інформації, доступом до ресурсів, управлінням паролями тощо:

— забезпечення виконання політики безпеки з питань рекрутингу, звільнень, контролю за дотриманням правил безпеки тощо.

4. Відділ фізичної безпеки:

— забезпечення фізичної безпеки об'єктів критичної інфраструктури, включаючи контроль доступу, використання систем відеоспостереження, охорони майна та обладнання тощо:

— розробка та впровадження процедур евакуації, планів дій в надзвичайних ситуаціях, а також організація тренувань персоналу з питань безпеки.

5. Менеджмент ризиків:

— проведення оцінки ризиків та визначення прийнятних рівнів ризику:

— розробка та впровадження заходів для зниження ризиків та підвищення резистентності до потенційних загроз:

— моніторинг ризиків та внесення необхідних змін у політику та процедури безпеки згідно з оновленою інформацією про ризики.

Кожна сторона має свої унікальні обов'язки та відповідальності, проте важливо забезпечити взаємодію та співпрацю між ними, щоб забезпечити повноту та ефективність реалізації політики безпеки об'єктів критичної інфраструктури.

Розробка плану впровадження моделі політики безпеки та механізмів оновлення може включати наступні кроки:

1. Формування команди: Утворення команди з представників різних відділів, таких як інформаційна безпека, IT, ресурси людські та фізична безпека. Ця команда буде відповідальна за розробку та впровадження моделі політики безпеки.

2. Аналіз і оцінка поточного стану безпеки: Проведення оцінки поточного стану безпеки об'єктів критичної інфраструктури, включаючи ідентифікацію потенційних загроз, аналіз вразливостей та оцінку ризиків.

3. Визначення потреб та цілей: Встановлення конкретних цілей безпеки, враховуючи результати аналізу стану безпеки. Визначення потреб у ресурсах, фінансуванні та термінах впровадження.

4. Розробка політики безпеки: Визначення основних принципів, цілей та стратегії безпеки для об'єктів критичної інфраструктури. Розробка політик і процедур з питань захисту даних, управління доступом, моніторингу безпеки та реагування на інциденти.

5. Впровадження технічних заходів: Розробка та впровадження технічних заходів безпеки, таких як захист мережі, шифрування даних, системи виявлення вторгнень та інші заходи, які відповідають виявленим вразливостям та загрозам.

6. Впровадження організаційних заходів: Розробка та впровадження організаційних заходів, таких як навчання персоналу з питань безпеки, розробка процедур управління інцидентами, контроль доступу та інші політики та процедури, що забезпечують виконання політики безпеки.

7. Моніторинг та аудит: Розробка системи моніторингу та аудиту для оцінки ефективності політики безпеки, виявлення вразливостей та реагування на інциденти безпеки. Регулярні перевірки та оцінки стану безпеки для забезпечення постійного вдосконалення.

8. Оновлення політики безпеки: Розробка процедур оновлення політики безпеки, включаючи періодичний перегляд та оцінку змін у загрозах, технологіях та потребах організації. Актуалізація політик та заходів безпеки згідно з оновленою інформацією та вимогами.

Важливо забезпечити планову і систематичну реалізацію кожного кроку, враховуючи специфіку об'єктів критичної інфраструктури та забезпечуючи залучення всіх необхідних ресурсів та зацікавлених сторін. Постійний моніторинг та оновлення моделі політики безпеки дозволять забезпечити високий рівень безпеки об'єктів критичної інфраструктури відповідно до змінюючихся умов та загроз.

Розробка власної моделі політики безпеки для об’єкта критичної інфраструктури включає кілька кроків які мають бути використані для розробки моделі політики безпеки:

Змоделюємо ситуацію велика компанія яка займається постачанням продовольства до багатьох, або одного міста України першим кроком у розробці моделі політики безпеки це визначення мети та цілей безпеки у нашому випадку мета та ціль безпеки це захист конфеденційної інформації та унеможливлення несанкціонованого доступу.

Другий крок ми будемо проводити аналіз потенційних загроз безпеки об’єкта та оцінка ризиків пов’язаних з цими загрозами. Ми повинні ідентифікувати загрозу а загрози можуть бути різні такі як DDos атака або отримання доступу до мережі об’єкта критичної інфраструктури.

Третій крок є створення політики безпеки, яка визначає основні принципи, цілі та стратегію безпеки для об’єкта критичної інфраструктури. Це документ який повинен визначати основні принципи конфіденційності, цілісності, доступності, реактивності та резистентності до атак.

Конфеденційність повинна бути забезпечена персоналом які займаються кібер безпекою інфраструктури на підприємстві.

Цілісність означає збереження цілісності даних та систем, для підприємства яке займається постачанням продовольства в різні міста України потрібно максимально захистити інформацію так як злиття певних файлів може сильно нашкодити критичній інфраструктурі. Наприклад доступ зловмисника до логістичного пересування може сильно нашкодити інфраструктурі.

Ця політика безпеки розробляється та затверджується керівництвом об’єкта критичної інфраструктури .

Четвертий крок це розробка заходів безпеки, насправді найкращий спосіб запобігти кібер атаці це від’єднати локальну мережу компанії від інтернету або давати доступ до мережі інтернет максимально малому числу працівників. Також у більшості компаній які є об’єктами критичної інфраструктури забороняють користуватися власними HDD, SSD та флеш накопичувачами.

П’ятий крок це реалізація заходів безпеки згідно з розробленою політикою. Цей етап включає встановлення технологічних заходів такий як правильне налаштування мережі на об’єкті критичної інфраструктури, встановлення антивірусних програм на пристрої об’єкта критичної інфраструктури, також потрібно провести навчання персоналу який відповідає за забезпечення безпеки і технічному обслуговувані пристроїв на об’єкті. Також важливо проводити постійний інструктаж звичайних працівників і бажано проводити інструктаж постійно а не тільки з новими працівниками. Також можна використовувати постери з основними правилами гігієни в мережі інтернет. Найчастіше зустрічаються такі заходи безпеки це реалізація Raid на серверах та персональних ПК, найбільш розповсюджений Raid це zero тобто дзеркало він дає змогу дублювати інформацію з основного HDD накопичувача на резервний. На

об’єктах критичної інфраструктури зустрічається така практика як створення резервних копій та фізичне відключення резервного накопичувача від сервера або ПК.

Шостий крок це встановлення систем моніторингу та аудит безпеки для постійного моніторингу для виявлення інцидентів та оцінки ефективності заходів безпеки. Цей етап включає постійний контроль стану безпеки. На об’єкті критичної інфраструктури можна постійно моніторити трафік який проходить через персональні комп’ютери і після виявлення аномального трафіку блокувати або вимикати даних ПК від мережі. Також слід спостерігати за журналом підключення різного роду пристроїв до мережі. Потрібно проводити регулярні аудити системи безпеки – це дає змогу обговорити і внести нові ідеї які можуть допомогти у забезпеченні безпеки критичної інфраструктури.

Сьомий крок це процедура та план реагування на інциденти. Якщо на головний сервер відбулась атака то потрібно зрозуміти яким чином зловмисник отримав доступ до сервера. Унеможливити повторне підключення до сервера, при умові якщо атака на сервер пошкодила інформацію, то як було описано раніше можна просто застосувати накопичувач який був резервним. Максимально швидке проведення таких процедур дає змогу не зупиняти роботу об’єкта критичної інфраструктури.

Восьмий кроком є забезпечення постійного вдосконалення стратегії та процедур безпеки. Для того щоб вдосконалювати захист об’єкта критичної інфраструктури потрібно навчати персонал, оновлювати обладнання та аналізувати нові загрози які виникають.

Важливо забезпечити систематичний та послідовний підхід до розробки моделі політики безпеки, щоб забезпечити максимальну ефективність та успішне впровадження.

2.4 Висновки по розділу

Розробка та впровадження моделі політики безпеки для об'єктів критичної інфраструктури має велике значення у забезпеченні безпеки, захисту та стійкості

таких об'єктів від потенційних загроз. У процесі розробки моделі, було визначено бажаний стан безпеки, визначено цілі та встановлено стратегію для досягнення цих цілей. План впровадження моделі передбачає розробку політик, процедур та технічних та організаційних заходів, що сприяють забезпеченню безпеки об'єктів критичної інфраструктури.

Основною метою моделі політики безпеки є забезпечення захисту і стійкості об'єктів критичної інфраструктури від різних загроз, таких як фізичні вторгнення, кібератаки, природні катастрофи тощо. Для досягнення цієї мети, модель передбачає впровадження широкого спектру заходів безпеки, включаючи контроль доступу, моніторинг, захист даних та систем, тренування персоналу та механізми реагування на надзвичайні ситуації.

Впровадження моделі політики безпеки має кілька важливих переваг. По-перше, це сприяє покращенню захищеності об'єктів критичної інфраструктури та зниженню ризиків інцидентів безпеки. Застосування відповідних політик, процедур та технічних заходів дозволяє ідентифікувати та усунути потенційні вразливості, а також ефективно реагувати на загрози та інциденти.

По-друге, модель політики безпеки забезпечує систематичний та структурований підхід до захисту об'єктів критичної інфраструктури. Вона включає розробку і впровадження політик, процедур, технічних та організаційних заходів, що сприяють підвищенню безпеки та зниженню ризиків. Цей підхід гарантує, що всі аспекти безпеки були враховані та забезпечені, що є важливим для об'єктів критичної інфраструктури.

По-третє, модель політики безпеки передбачає постійний моніторинг та оновлення політик з метою відповідності змінюючимся умовам та загрозам. Це забезпечує гнучкість та адаптивність політики безпеки, що дозволяє підтримувати високий рівень безпеки протягом тривалого періоду. Моніторинг і оновлення політик забезпечують, що вони відповідають сучасним стандартам безпеки та відповідають новим технологічним викликам і загрозам.

Впровадження моделі політики безпеки вимагає відповідальності, координації та співпраці різних зацікавлених сторін, включаючи управління

об'єктів критичної інфраструктури, державні органи, технічних експертів та інші зацікавлені сторони. Лише шляхом спільних зусиль можна досягти максимальної ефективності та успішно реалізувати модель політики безпеки.

У підсумку, розробка та впровадження моделі політики безпеки для об'єктів критичної інфраструктури є необхідним кроком для забезпечення безпеки, захисту та стійкості таких об'єктів. Ця модель допомагає ідентифікувати та усувати потенційні загрози, знижує ризики інцидентів безпеки та забезпечує відповідність вимогам безпеки. Впровадження моделі політики безпеки приносить багато переваг, включаючи покращену захищеність, зниження ризиків та підвищення довіри до об'єктів критичної інфраструктури. Забезпечення безпеки цих об'єктів є важливим завданням, яке вимагає систематичного та прорахованого підходу, а модель політики безпеки є ефективним інструментом для досягнення цієї мети.

3 ПЕРЕВІРКА ЕФЕКТИВНОСТІ МОДЕЛІ ПОЛІТИКИ БЕЗПЕКИ

3.1 Проведення тестування моделі політики безпеки

Проведення тестування моделі політики безпеки є важливим кроком у розробці та впровадженні ефективної стратегії безпеки для об’єкта критичної інфраструктури. Цей процес дозволяє оцінити ефективність різних заходів безпеки, виявити слабкі місця та проблеми, а також розробити рекомендації щодо покращення моделі політики безпеки.

Проведення тестування моделі політики безпеки може включати використання різних методологій та інструментів для оцінки ефективності заходів безпеки. Це може включати визначення сценаріїв тестування, використання симуляційних інструментів, проведення експериментальних тестів тощо. Результати тестування допомагають оцінити ефективність заходів безпеки та розробити рекомендації щодо покращення моделі політики безпеки.

Деякі кроки, які можемо виконати для проведення тестування власної моделі політики безпеки:

1 .Визначте сценарії тестування: Першим кроком у проведенні тестування моделі політики безпеки є визначення сценаріїв тестування. Це може включати різні типи атак, такі як злам паролів, DDoS-атаки, шкідливе ПЗ тощо. Важливо визначити реалістичні сценарії, які допоможуть оцінити ефективність заходів безпеки.

2 .Використайте симуляційні інструменти: Для проведення тестування ви можете використовувати спеціалізовані симуляційні інструменти, які дозволяють моделювати різні типи атак та оцінювати ефективність заходів безпеки. Це може включати використання програмного забезпечення для моделювання мережевих атак, інструментів для тестування вразливостей тощо.

3. Проведення експериментальних тестів: Наступним кроком є проведення експериментальних тестів з використанням розроблених сценаріїв та симуляційних інструментів. Це може включати проведення атак на тестову мережу або систему з метою оцінки ефективності заходів безпеки.

Тестування моделі політики безпеки може бути проведено шляхом симуляції різних сценаріїв загроз безпеки та оцінки ефективності реакції на них. Наприклад, у випадку з компанією, яка займається постачанням продовольства до багатьох міст України, можна провести тестування на витривалість до DDos атак або спроб отримання доступу до мережі об’єкта критичної інфраструктури.

Приклади які забезпечують безпеку критичної інфраструктури були наведені під час розробки моделі політики безпеки та являються максимально простими та ефективними, правила безпеки які були наведені при їх не ухильному виконанні майже повністю унеможливить кібер атаку або набагато легше мінімізує шкоду об'єкту.

Це допоможе виявити слабкі місця у політиці безпеки та вжити необхідних заходів для їх усунення. Важливо проводити таке тестування регулярно, щоб забезпечити надійний захист об’єкта критичної інфраструктури.

3.2 Аналіз результатів експериментального тестування

Аналіз результатів експериментального тестування - це процес оцінки результатів тестування з метою виявлення слабких місць у системі безпеки та оцінки ефективності заходів безпеки. Цей аналіз допомагає визначити, чи дотримуються всі правила та процедури, визначені у політиці безпеки, та чи є необхідність у внесенні змін до цих правил.

Під час аналізу результатів тестування необхідно звернути увагу на такі питання:

— чи були успішно виявлені та заблоковані всі спроби атаки?

— чи були виявлені всі слабкі місця у системі безпеки?

— чи була реакція на інциденти безпеки своєчасною та ефективною?

— чи були вжиті всі необхідні заходи для запобігання подальшим атакам?

Під час дослідження різних випабдків кібер атак на підприємства було виявлено, що не мало важливу роль грає сучасне обладнання яке захищає головний сервер від атак, вчасно блокує ір-адреси зловмисників які намагаються завдати шкоду об’єкту.

Щоб виявити усі слабкі місця нам потрібно проводити аудит спеціалістів один раз в певний строк бажано не рідше чим раз у місяць.

Реакція на інцидент це правильно розроблений сценарій дій та правильно налаштоване обладнання.

У розробленій моделі політики безпеки я перечисляв необхідні заходи для запобігання подальших атак. Міри які були описані у моделі політики безпеки для запобігання подальших атак є максимально ефективними – це показує досвіт адміністраторів які працюють на різного роду підприємствах.

На основі аналізу результатів тестування можна розробити план дій для покращення системи безпеки та запобігання подальшим загрозам. Це може включати в себе зміни у політиці безпеки, оновлення програмного забезпечення, навчання персоналу тощо.

Важливо проводити аналіз результатов експериментального тестування регулярно, щоб забезпечити надійний захист об’єкта критичної інфраструктури.

3.3 Порівняння результатів тестування з існуючими підходами до забезпечення безпеки об'єктів критичної інфраструктури

Порівняння результатів тестування з існуючими підходами до забезпечення безпеки об’єктів критичної інфраструктури Порівняння результатів тестування з існуючими практиками допомагає оцінити ефективність розробленої моделі політики безпеки та визначити можливості для її покращення. Наприклад, можна порівняти ефективність моєї розробленої моделі політики безпеки з рекомендаціями міжнародних організацій або стандартами безпеки в галузі [13].

Одним з можливих підходів до порівняння результатов тестування з існуючими практиками є проведення аналогичного тестування на інших об’єктах критичної інфраструктури та порівняння результатов. Це дозволить оценити ефективність вашої розробленої моделі політики безпеки у порівнянні з існуючими практиками [14].

Також можна провести аналогичне тестування на об’єкті критичної інфраструктури, який має схожий профіль діяльності та порівняти результати.

Це дозволить оцінити ефективність вашої розробленої моделі політики безпеки у порівнянні з існуючими практиками [15].

Під час тестування новорозробленої моделі політики безпеки потрібно деякий час щоб виконати певні правки тому як, без реального впровадження оцінити ефективність роботи майже неможливо. Якщо проводити тестування на об’єкті критичної інфраструктури який має схожий профіль то результати можна отримати не очікувані як і в хорошому так і в негативному ключі.

Важливо зауважити, що кожен об’єкт критичної інфраструктури є унікальним і може мати свої особливості. Тому порівняння результатов тестування з існуючими практиками повинно бути проведено з урахуванням специфіки конкретного об’єкта [15].

Крім того, при порівнянні результатів тестування з існуючими практиками, важливо враховувати часовий фактор. Загрози безпеки постійно розвиваються і змінюються, тому необхідно регулярно оновлювати свою модель політики безпеки, щоб вона відповідала сучасним вимогам. Це означає не тільки покращення самої моделі політики безпеки, але також проведення регулярних навчань для працівників, консультацій для рядових працівників та оновлення обладнання на підприємстві. Використання сучасного обладнання зменшує шанси успішної атаки, оскільки зловмисники можуть не мати доступу до нових методів атаки на таке обладнання. Важливо проводити регулярні аудити системи безпеки для оцінки ефективності заходів безпеки та виявлення можливостей для їх покращення. Це дозволить вчасно виявити слабкі місця у системі безпеки та розробити рекомендації щодо їх усунення.

Також важливо співпрацювати з експертами у галузі кібербезпеки для отримання консультацій та рекомендацій щодо покращення моделі політики безпеки. Експерти можуть надати цінну інформацію про нові загрози безпеки та методи їх запобігання, а також допомогти у розробці ефективних заходів безпеки.

3.4 Рекомендації щодо застосування моделі політики безпеки для об'єктів критичної інфраструктури

Модель політики безпеки — це набір правил та процедур, які визначають, яким чином організація забезпечує безпеку своїх інформаційних ресурсів. Ось деякі рекомендації для застосування моделі політики безпеки:

— визначте цілі та область застосування політики безпеки;

— розробіть процедури для ідентифікації та класифікації інформації;

— встановіть правила для доступу до інформації та її обробки;

— розробіть процедури для моніторингу та аудиту дотримання політики безпеки;

— забезпечте навчання персоналу з питань безпеки інформації;

— переглядайте та оновлюйте політику безпеки регулярно, щоб вона відповідала змінам у загрозах безпеці та технологіях.

Політикою безпеки потрібно займатися завжди а не тільки тоді коли стався якийсь виток інформації або відбулась крадіжка кваліфікованого персоналу за того, що відбувся виток конфеденційної інформації працівників.

Модель політики безпеки — це набір правил та процедур, які визначають, яким чином організація забезпечує безпеку своїх інформаційних ресурсів. Існує багато різних моделей політики безпеки, які можуть бути застосовані в залежності від специфіки організації та її потреб.

У роботі були перечисленні три моделі політики безпеки і навіть на один із них був наведений наглядний приклад який був не змодельований а відбувався у реальному житті на практиці.

Щоб розуміти як правильно застосовувати моделі політики безпеки для об'єктів критичної инфраструктури потрібно мати грунтовні знання в цій області та аналізувати випадки які відбулися з іншими компаніями. Тільки велика кількість напрацьованого досвіду допоможе правильно застосовувати набуті знання.

Також не слід нехтувати колективною думкою, що до вирішення певних проблем та бажано звертатися за порадами до колег або керівника.

У висновку слід зазначити, що надати якісь сто відсоткові роботоздатні рекомендації не реально все індивідуально, у кожного колектива своя атмосфера та у кожного працівника свій характер тому підхід індивідуальний. Ззагалом найкраща безпека для о'бєкта критичної інфраструктури або компанії це виконання правил безпеки під час всього робочого процесу а не тільки тоді коли настала якась проблема.

ВИСНОВКИ

У цій роботі було проведено детальний аналіз стану безпеки об’єктів критичної інфраструктури. У першому розділі було визначено поняття “об’єкта критичної інфраструктури” та проаналізовано нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури. Також було проведено аналіз існуючих політик безпеки для цих об’єктів та визначено методологію дослідження.

У другому розділі було виявлено недоліки існуючих підходів до забезпечення безпеки об’єктів критичної інфраструктури та розроблено нову модель політики безпеки. Модель базується на типах загроз та методології оцінювання ризиків для об’єктів критичної інфраструктури.

У третьому розділі модель була протестована за допомогою експериментального тестування. Результати тестування були проаналізовані та порівняні з існуючими підходами до забезпечення безпеки об’єктів критичної інфраструктури. На основі отриманих результатів було сформульовано рекомендації щодо застосування моделі політики безпеки для об’єктів критичної інфраструктури, що дозволить покращити рівень їх захисту.

Висновки цього дослідження показують, що розроблена модель політики безпеки є ефективним інструментом для забезпечення безпеки об’єктів критичної інфраструктури. Рекомендації, сформульовані на основі результатів дослідження, можуть бути використані органами влади та операторами об’єктов критической инфраструктуры для покращення рівня захисту. Однак, необхідно пам’ятати, що кожен об’єкт критичної інфраструктури має свою специфіку та потреби, тому модель політики безпеки повинна бути адаптована до конкретних умов. Також важливо регулярно переглядати та оновлювати політику безпеки, щоб вона відповідала змінам у загрозах безпеки та технологіях.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Об'єкт критичної інфраструктури. URL: https://smarttender.biz/terminy/view/ob-yekti-kritichnoyi-infrastrukturi/

2. Об'єкт критичної інфраструктури та їх принципи роботи. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ispn.kievcity.gov.ua/HelpInfo/News/NewsOne.aspx%3FID%3D329&ved=2ahUKEwi9t-Ta4c7_AhVOh_0HHQaOB0YQFnoECBEQAQ&usg=AOvVaw0SZDXvd8LWn3Fr2bXEOpNw

3. Нормативно правове забезпечення кібербезпеки. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini

4. Аналіз існуючих політик безпеки. URL: https://www.researchgate.net/publication/323728627_Analiz_pobudovi_modeli_politiki_informacijnoi_bezpeki_pidpriemstva

5. Популярні моделі політики безпеки URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://studfile.net/preview/9649825/page:8/&ved=2ahUKEwi5k7Gr4M7_AhV9hP0HHXcEBJUQFnoECAwQAQ&usg=AOvVaw2b3xuJLml0Rbsdzhsb7WKa

6. Недоліки існуючих підходів до забезпечення безпеки об’єктів. URL: http://ebib.pp.ua/podhodyi-printsipyi-metodyi-sredstva-4218.html

7. Основні загрози об’єктів інфраструктури URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://smarttender.biz/blog/view/ob-yekti-kritichnoyi-infrastrukturi-detalniy-analiz-ta-vidpovidi-na-poshireni-pitannya/&ved=2ahUKEwiHn4zV4M7_AhUBgv0HHVOiAp4QFnoECBAQAQ&usg=AOvVaw2aY81sGQRXbuzL99_ARf4r

8. Типи загроз для об’єктів критичної інфраструктури. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf&ved=2ahUKEwiPor612s7_AhXqhf0HHS2rA4UQFnoECAkQAQ&usg=AOvVaw21kiU2bpoGkBDSUGW4pSuf

9. Приклади моделі політики безпеки. URL: https://stud.com.ua/94391/informatika/politika_bezpeki

10. Основні моделі політики безпеки URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ekmair.ukma.edu.ua/server/api/core/bitstreams/50763dd1-6bf8-4c7d-96a2-947a38487b09/content&ved=2ahUKEwiV44aE4c7_AhU99bsIHZ6oAp4QFnoECBsQAQ&usg=AOvVaw1QQ_BzwYSAEfo2iA2K5Mc9

11. Методи тестування політики безпеки. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://sci.ldubgd.edu.ua/bitstream/123456789/9839/1/9.%2520%25D0%25BA%25D1%2583%25D0%25BF%25D1%2580%25D1%2596%25D0%25BA%25D0%25BE%25D0%25B2.pdf&ved=2ahUKEwjXrvvD287_AhX9g_0HHZ8PBwwQFnoECA4QAQ&usg=AOvVaw2gvUYbbqJQe3kB3Y-6d2eY

12. Експериментальні тестування політики безпеки URL: https://mediaosvita.org.ua/2018/05/01/mediagramotnist-ta-informatsijna-bezpeka/

13. Аналіз тестування безпеки. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/59375/1/Semenov_Analiz_osnovnykh_2018.pdf&ved=2ahUKEwjx942Q3s7_AhUe9rsIHRBmC7YQFnoECAwQAQ&usg=AOvVaw1lxEWLwbiLDyC_epEmQ1DX

14. Методи порівняння результатів проведених тестувань. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://ekmair.ukma.edu.ua/server/api/core/bitstreams/69aef8a7-c03c-4213-b1ae-2bd920cec868/content&ved=2ahUKEwjxtofs3s7_AhV8hv0HHa22AusQFnoECA0QAQ&usg=AOvVaw1HYO8nzr9m4xGJ0K5bgGH3

15. Принципи порівняння тестів. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=http://mmsa.kpi.ua/sites/default/files/disciplinesB8UQFnoECBUQAQ&usg=AOvVaw3iyJCRwzlZcMme8uqud6Ja

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Модель політики безпеки для об'єкта критичної інфраструктури

Автор роботи: Грищук Владислав Валерійович

Тип роботи: бакалаврська дипломна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 98,26% Схожість – 1,74%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Грищук В. В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Бурячок А. В.
(підпис) (прізвище, ініціали)

ІЛЮСТРАТИВНА
ЧАСТИНА

МОДЕЛЬ ПОЛІТИКИ БЕЗПЕКИ ДЛЯ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

(Назва бакалаврської кваліфікаційної роботи)

Виконав: студент 4 курсу групи 1БС-19 б спеціальності 125 Кібербезпека

_____Грищук В. В.

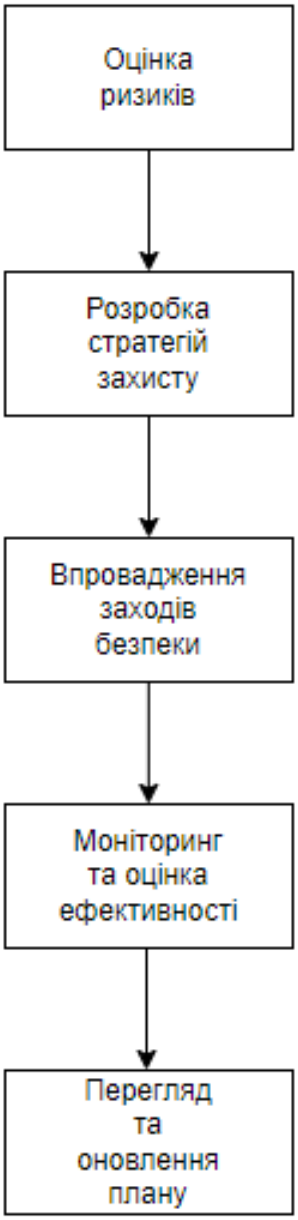
_____ 2023 р.

Керівник: зав. к.т.н., доцент каф. ЗІ

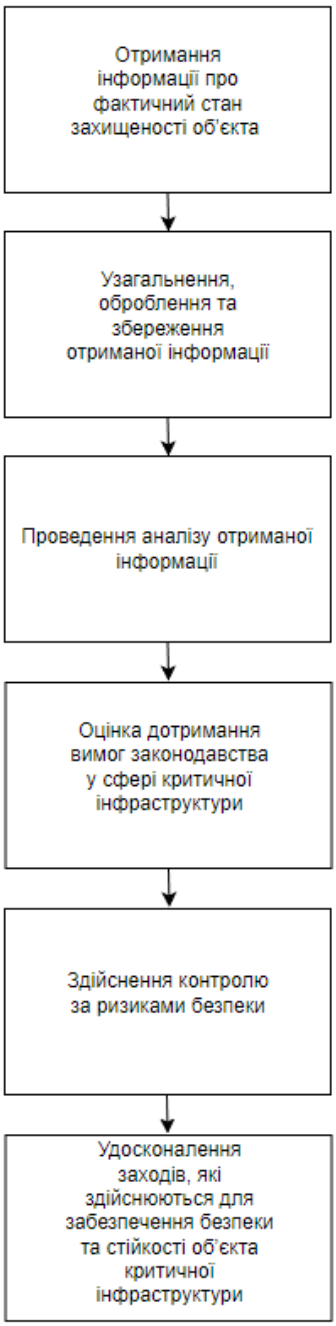
_____ Дудатьєв А. В.

_____ 2023 р.

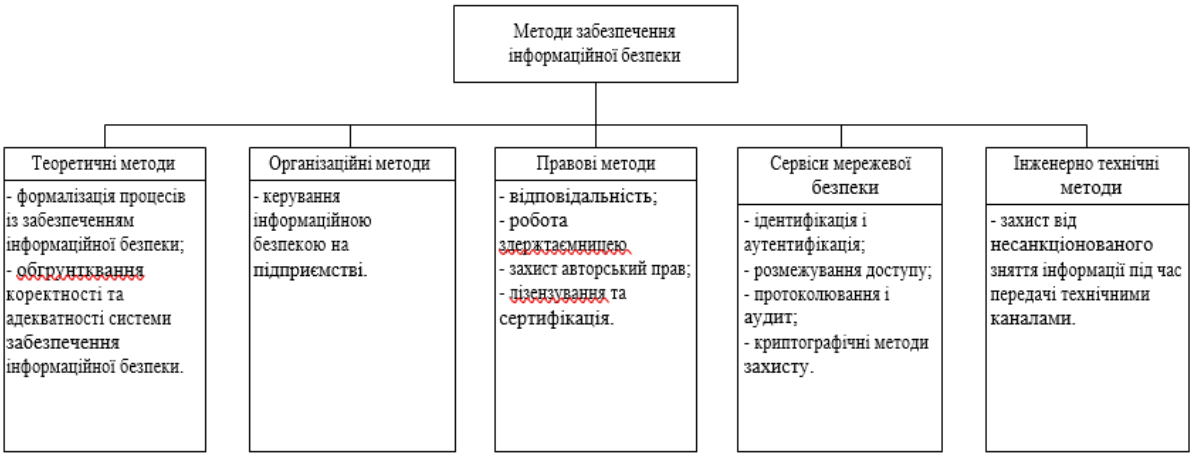
План заходів з забезпечення об’єкта критичної інфраструктури



Форма контролю та моніторингу безпеки об'єкта критичної інфраструктури



Основні методи забезпечення інформаційної безпеки



Класифікація математичних моделей безпеки комп’ютерних систем

Організація доступу в інформаційних системах використовуючи дискриційний метод