МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “РОЗРОБКА МЕТОДИКИ ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ”

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

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

_____ Михайло ВИДРЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Михайло ВИДРЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: Андрій КОТЕНКО
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти - бакалавр

Спеціальність - 125 Кібербезпека

Освітня програма - Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ

_____Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Видренко Михайлу Олексійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Розробка методики захисту об’єктів критичної інформаційної інфраструктури”,

керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор

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

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. №36.Строк подання кваліфікаційної роботи “20” травня 2024р.

2. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека критичної інфраструктури, методи та засоби захисту критичної інформаційної інфраструктури, міжнародні стандарти, наукова та технічна література.*

3. Перелік питань, які мають бути розроблені:

3.1. Ідентифікація та категоризація об’єктів критичної інфраструктури.

3.2. Оцінка ризиків та вразливостей критичної інфраструктури.

3.3. Розробка стратегії та заходів захисту критичної інфраструктури.

4. Перелік ілюстративного матеріалу: матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	Виконано
2.	Збір та аналіз літератури.	29.03.2024	Виконано
3.	Ідентифікація та категоризація об’єктів критичної інфраструктури.	08.04.2024	Виконано
4.	Оцінка ризиків та вразливостей критичної інфраструктури	22.04.2024	Виконано
5.	Розробка стратегії та заходів захисту критичної інформаційної інфраструктури.	15.04.2024 - 10.05.2024	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	Виконано
7.	Оформлення роботи.	22.05.2024	Виконано
8.	Оформлення презентації.	03.06.2024	Виконано
9.	Отримання рецензії на роботу.	03.06.2024	Виконано
10.	Захист в ЕК.	10.06.2024	Виконано

Здобувач вищої освіти _____ Михайло ВИДРЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Видренко М.О до захисту кваліфікаційної роботи

(прізвище та ініціали)

за спеціальністю 125 Кібербезпека

(код, найменування спеціальності)

освітньої програми Управління інформаційною та кібернетичною безпекою

(назва)

на тему: **“**Розробка методики захисту об’єктів критичної інформаційної інфраструктури ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ВИДРЕНКО Михайло у кваліфікаційній роботі проаналізував особливості розробки методів захисту об'єктів критичної інформаційної інфраструктури, дослідив сучасні технології та підходи до захисту інформації, вивчив методи та інструменти захисту інформаційних систем, розробив методику захисту об'єктів критичної інформаційної інфраструктури.

ВИДРЕНКО Михайло продемонстрував глибоке розуміння проблеми дослідження та вміння застосовувати теоретичні знання для вирішення практичних завдань. Він володіє навичками наукового дослідження, вміє самостійно працювати та приймати рішення. Результати дослідження апробовані на науковій конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ВИДРЕНКА Михайла на оцінку “добре” та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА

(підпис) *(Ім’я,ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

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

Завідувач кафедри управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА

(підпис) (Ім’я, ПРІЗВИЩЕ)

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ВИДРЕНКО Михайло
на тему “ Розробка методики захисту об’єктів критичної інформаційної інфраструктури ”
\

Актуальність. У сучасному світі інформація стає одним з найважливіших ресурсів, а критична інформаційна інфраструктура (КІІ) – це основа для функціонування держави, економіки та суспільства. Забезпечення кібербезпеки критичних інформаційних інфраструктур є одним з пріоритетних завдань державної політики, адже кіберзагрози стають дедалі більш витонченими та небезпечними.

З огляду на зазначене дослідження розробки ефективної методики захисту об’єктів критичної інформаційної інфраструктури є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено методики захисту об’єктів критичної інформаційної інфраструктури, визначено ключові ризики та вразливості, проведено оцінку, сформовано стратегію та заходи захисту.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу, в тому числі англомовні джерела.
4. За результатами дослідження розроблена модель технічних засобів забезпечення інформаційної безпеки критичної інфраструктури.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації оцінки ризиків та вразливостей критичної інформаційної інфраструктури.

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

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

Рецензент: _____ Андрій КОТЕНКО
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці ефективної методики захисту об’єктів критичної інформаційної інфраструктури. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел .. Загальний обсяг роботи становить 45 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка ефективної методики захисту об’єктів критичної інформаційної інфраструктури.

Об’єктом дослідження є захист об’єктів критичної інформаційної інфраструктури.

Предмет дослідження – розробка об’єктів критичної інформаційної інфраструктури.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до розробки критичної інформаційної інфраструктури.

Як результат у роботі проаналізовано особливості розробки ефективної методики захисту критичної інформаційної інфраструктури; досліджено оцінку ризиків та вразливостей критичної інфраструктури; вивчені заходи захисту критичної інформаційної інфраструктури.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації розробки та вдосконалення методів та методик захисту об'єктів критичної інформаційної інфраструктури .

Ключові слова: КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, СТРАТЕГІЯ ІБ, МЕТОДИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

ABSTRACT

The qualification work is devoted to the development of an effective methodology for the protection of critical information infrastructure facilities. The work consists of an introduction, three chapters, conclusions and references. The total volume of the work is 45 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop an effective method of protecting critical information infrastructure objects.

The object of research is the protection of objects of critical information infrastructure.

The subject of the study is the development of objects of critical information infrastructure.

Research methods. To solve the above scientific task, the methods of analysis and synthesis, comparison, classification, expert evaluation, and a systematic approach to the development of critical information infrastructure were used.

As a result, the paper analyses the peculiarities of developing an effective methodology for the protection of critical information infrastructure; investigates the assessment of risks and vulnerabilities of critical infrastructure; and studies measures to protect critical information infrastructure.

Scope of application. The developed approaches can be used in the planning and implementation of the development and improvement of methods and techniques for the protection of critical information infrastructure.

Keywords: CYBERSECURITY, CRITICAL INFRASTRUCTURE, CYBER SECURITY STRATEGY, METHODS OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ОКІ об'єкти критичної інфраструктури. ЄС Європейський Союз.

НАТО Організація Північноатлантичного договору.

КІ критична інфраструктура.

ІТ інформаційні технології.

ПЗ програмне забезпечення. ОВВ органи виконавчої влади.

ОМС органи місцевого самоврядування.

ЗМІ засоби масової інформації.

НПА нормативно-правові акти. ЦЗ цивільний захист.

ЦО цивільна оборона.

ЕБ економічна безпека.

ТЕБ техногенна та екологічна безпека. ПБпожежна безпека.

ОП охорона праці.

ЦЗ цивільний захист.

ЦО цивільна оборона.

ЕБ економічна безпека.

ТЕБ техногенна та екологічна безпека. ПБ пожежна безпека.

ОП охорона праці.

ВСТУП

Актуальність теми. У сучасному світі інформація стає одним з найважливіших ресурсів, а критична інформаційна інфраструктура (КІІ) – це основа для функціонування держави, економіки та суспільства. Забезпечення кібербезпеки КІІ є одним з пріоритетних завдань державної політики, адже кіберзагрози стають дедалі більш витонченими та небезпечними.

Метою роботи є розробка ефективної методики захисту об’єктів критичної інформаційної інфраструктури.

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

1. Дослідити ідентифікацію та категоризацію об'єктів критичної інфраструктури.

2. Оцінити ризикі та вразливості критичної інформаційної інфраструктури.

3. Розробити стратегію та заходи захисту критичної інформаційної інфраструктури.

Об’єктом дослідження є захист об’єктів критичної інформаційної інфраструктури.

Предмет дослідження – розробка об’єктів критичної інформаційної інфраструктури.

Метод дослідження – Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Практична значимість дослідження – полягає в тому, що розроблена методика захисту об'єктів КІІ може бути використана для підвищення рівня кібербезпеки КІІ України.

Розділ 1. ІДЕНТИФІКАЦІЯ ТА КАТЕГОРИЗАЦІЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

Ідентифікація та категоризація об'єктів критичної інфраструктури є важливим початковим кроком у процесі забезпечення їх ефективного захисту. Цей процес передбачає визначення механізму та критеріїв віднесення об'єкта критичної інфраструктури до тієї чи іншої категорії відповідно до його критичності. Для цього використовуються галузеві та міжгалузеві критерії з метою отримання балів для оцінки об'єкта. Ідентифікація об'єктів критичної інфраструктури здійснюється на підставі розробленого та затвердженого керівником уповноваженого органу галузевого переліку таких об'єктів. Класифікація об'єктів здійснюється за трьома окремими категоріями: сектори (підсектори), життєво важливі послуги та категорії критичності. Віднесення об'єктів до відповідних категорій критичності забезпечує належний рівень захисту та управління ризиками. Категоризація об'єктів критичної інфраструктури визначає процедуру віднесення їх до певної категорії критичності. На орган, відповідальний за сектор (підсектор) критичної інфраструктури, покладається завдання з ідентифікації та категоризації об'єктів, що перебувають в його управлінні. Результати категоризації вносяться до Національного переліку об'єктів критичної інфраструктури (у разі його створення) та до уповноваженого органу у сфері захисту.

1.1 Аспекти ідентифікації та категоризації об’єктів критичної інформаційної інфраструктури

В Україні віднесення об'єктів до КІ та визначення їх категорії критичності ґрунтується на Постанові Кабінету Міністрів України № 1109 від 23 грудня 2020 року "Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури".

Цей документ визначає:

- Механізм віднесення об'єктів до КІ:
    - Об'єкти до КІ відносяться за видами економічної діяльності, визначеними Класифікатором видів економічної діяльності (КВЕД) України. о Перелік видів економічної діяльності, що належать до КІ, затверджується Кабінетом Міністрів України. о Об'єкти, які відповідають зазначеним видам економічної діяльності, автоматично відносяться до КІ.
- Критерії віднесення об'єктів КІ до категорій критичності:
    - Виділяється 5 категорій критичності: дуже висока, висока, середня, значна, низька.
    - До кожної категорії критичності встановлюються окремі критерії, що ґрунтуються на:

Впливі порушення функціонування об'єкта на:

- Життя та здоров'я людей
- Національну безпеку
- Економіку та фінанси
- Державне управління
- Навколишнє середовище
- Характеристиках об'єкта, таких як:
- Масштаби діяльності
- Незамінність
- Складність технологічних процесів
- Наявність небезпечних речовин
- Можливість виникнення аварій

Процедура віднесення об'єкта до КІ та визначення його категорії критичності:

1. Власник або керівник об'єкта:

– Заповнює Анкету об'єкта критичної інфраструктури згідно з формою, затвердженою Кабінетом Міністрів України. о Надає Анкету та інші необхідні документи уповноваженому органу в сфері управління КІ.

2. Уповноважений орган:

– Проводить експертизу наданої інформації та аналіз відповідності об'єкта критеріям віднесення до КІ. о Виносить рішення про віднесення об'єкта до КІ та визначення його категорії критичності. о Направляє власнику або керівнику об'єкта витяг з протоколу засідання комісії з питань КІ, де зазначено категорію критичності об'єкта.

Віднесення об'єкта до КІ та визначення його категорії критичності мають важливе значення для:

• Забезпечення підвищеного рівня захисту КІ від різноманітних загроз.

• Визначення пріоритетів у сфері фінансування та ресурсного забезпечення заходів з захисту КІ.

• Застосування відповідних вимог щодо кіберзахисту та фізичного захисту КІ.

• Здійснення державного контролю за діяльністю об'єктів КІ.

1.2 Категорії критичності в секторальному переліку об’єктів критичної інфраструктури

В Україні, згідно з Постановою Кабінету Міністрів № 1109 від 16 січня 2024 року, об'єкти критичної інфраструктури (КІ) поділяються на чотири категорії критичності:

І категорія:

– Об'єкти, що мають високу важливість для держави цілком і здатні суттєво впливати на інші об'єкти КІ.

До цієї категорії належать, зокрема:

– Державні органи та установи, що забезпечують оборону та національну безпеку України;

– Об'єкти атомної енергетики; о Транспортні магістралі; о Об'єкти телекомунікаційних мереж; о Фінансові установи.

II категорія:

– Об'єкти, що є життєво важливими, а припинення чи порушення їх роботи спричинить кризову ситуацію регіонального значення.

– До цієї категорії належать, зокрема:

– Об'єкти нафтогазової промисловості; о Об'єкти енергетики; о Об'єкти водопостачання та водовідведення; о Об'єкти охорони здоров'я; о Об'єкти харчової промисловості.

III категорія:

– Важливі об'єкти, порушення чи припинення роботи яких спричинить кризову ситуацію місцевого значення.

– До цієї категорії належать, зокрема: о Об'єкти машинобудівної промисловості; о Об'єкти хімічної промисловості; о Об'єкти транспортної інфраструктури; о Об'єкти сфери послуг; о Об'єкти наукової та дослідницької діяльності.

IV категорія:

– Необхідні об'єкти, порушення чи припинення роботи яких спричинить кризову ситуацію локального значення.

– До цієї категорії належать, зокрема:

– Об'єкти сфери торгівлі; о Об'єкти сфери освіти; о Об'єкти культури; о Об'єкти спорту; о Житлові комплекси.

До секторального переліку об'єктів КІ входять лише ті об'єкти, які відповідають критеріям, визначеним у Постанові № 1109.

1.3 Національний перелік об'єктів критичної інфраструктури.

Ведення Національного переліку об'єктів критичної інфраструктури є важливим кроком у процесі захисту критичної інфраструктури. Національний перелік об'єктів критичної інфраструктури формується та затверджується Компетентним органом з питань захисту критичної інфраструктури. Ведення Національного переліку об'єктів критичної інфраструктури включає процедури створення та ведення Реєстру об'єктів критичної інфраструктури, включення об'єктів до Реєстру, внесення відомостей про об'єкти критичної інфраструктури та виключення їх з Реєстру. Реєстр ведеться з метою координації дій суб'єктів національної системи захисту критичної інфраструктури на державному рівні. Публічна інформація в Реєстрі містить відомості про галузевий орган, уповноважений орган та дату внесення до Реєстру. Власник об'єкта критичної інфраструктури - юридична особа будь-якої форми власності, яка має у власності об'єкт критичної інфраструктури. Підставою для внесення інформації до Реєстру є повідомлення про об'єкт критичної інфраструктури.

Національний перелік об'єктів КІ - це реєстр, який містить інформацію про всі об'єкти КІ в Україні. Його ведення здійснюється відповідно до Постанови Кабінету Міністрів України № 1109 від 23 грудня 2020 року "Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури".

Національний перелік містить:

– Перелік об'єктів КІ з розподілом за категоріями критичності.

– Інформацію про кожен об'єкт КІ, включає:

– Назва об'єкта о Місцезнаходження о Власни о Відомості про вид економічної діяльності о Категорія критичності

– Інші дані, які визначені уповноваженим органом

Ведення Національного переліку здійснюється:

– Уповноваженим органом в сфері управління КІ, яким є Державна служба з питань безпеки інформаційних технологій та зв'язку (ДССЗІТ).

– На основі інформації, що надається: о Власниками або керівниками об'єктів о Іншими органами державної влади

Доступ до Національного переліку КІ:

• Обмежений згідно з вимогами законодавства про державну таємницю.

• Надається уповноваженим органам державної влади та іншим особам, які мають законні підстави для його отримання.

Національний перелік КІ є важливим інструментом для:

• Забезпечення захисту КІ від різноманітних загроз.

• Визначення пріоритетів у сфері фінансування та ресурсного забезпечення заходів з захисту КІ.

• Здійснення державного контролю за діяльністю об'єктів КІ.

Висновки для розділу 1

Ідентифікація та категоризація об'єктів критичної інфраструктури є фундаментальним кроком у забезпеченні їх ефективного захисту. Цей процес дозволяє визначити механізм та критерії віднесення об'єкта до певної категорії критичності, що, в свою чергу, впливає на рівень захисту та управління ризиками. Використання галузевих та міжгалузевих критеріїв для категоризації активів дозволяє об'єктивно оцінити їх важливість та рівень критичності. Розробка галузевих переліків об'єктів критичної інфраструктури та їх класифікація за категоріями критичності забезпечує ефективне управління на галузевому рівні. Ведення Національного переліку об'єктів критичної інфраструктури та Реєстру об'єктів критичної інфраструктури є важливим інструментом для координації дій національної системи захисту. Внесення інформації про об'єкти до Реєстру, присвоєння унікальних реєстраційних номерів та встановлення порядку доступу до інформації дозволяє забезпечити

належний рівень управління та захисту критичної інфраструктури. Віднесення об'єктів критичної інфраструктури до категорій критичності здійснюється відповідно до методичних рекомендацій. Цей підхід передбачає віднесення ідентифікованих об'єктів до певної категорії критичності, зміну категорії критичності об'єктів та виключення об'єктів з відповідного переліку. Категорії критичності допомагають визначити рівень важливості та потенційний вплив кожного об'єкта на функціонування системи критичної інфраструктури. Таким чином, ідентифікація та категоризація об'єктів критичної інфраструктури створює основу для подальшої оцінки ризиків, розробки заходів захисту та ефективного управління критично важливими об'єктами. Цей етап є невід'ємною частиною процесу забезпечення безпеки та стійкості критичної інфраструктури.

РОЗДІЛ 2. ОЦІНКА РИЗИКІВ ТА ВРАЗЛИВОСТЕЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Оцінка ризиків та вразливостей є важливим етапом у забезпеченні безпеки об'єктів критичної інфраструктури. Цей процес включає в себе аналіз можливих наслідків порушення функціонування таких об'єктів, що можуть мати серйозні наслідки для економіки, енергетичної, фінансової та обороноздатності держави. Оцінка ризиків проводиться на основі аналізу можливих наслідків для основних послуг у всіх секторах економіки1. Визначаються економічні збитки при заподіянні шкоди навколишньому природному середовищу у разі порушення функціонування об'єкта критичної інфраструктури. Наслідки класифікуються за видами збитків (наприклад, енергетичні, економічні, фінансові, безпекові) та визначаються основні види збитків для кожного типу та виду об'єкта критичної інфраструктури. Паралельно проводиться оцінка вразливостей критичної інфраструктури, зокрема критичної інформаційної інфраструктури. Це дозволяє виявити можливі точки проникнення та слабкі місця в системах управління та контролю, що може бути використано для розробки ефективних заходів захисту. Оцінка вразливостей включає проведення аудиту безпеки, аналіз захищеності систем управління та контролю, а також визначення ймовірності реалізації кожного виду загроз. На основі оцінки ризиків та вразливостей визначається рівень ризику для кожного об'єкта критичної інфраструктури. Ризик розраховується як добуток ймовірності реалізації загрози на величину можливого збитку. Отримані значення рівня ризику порівнюються з встановленими критеріями ризику для визначення його значущості та необхідності вжиття заходів щодо його зниження. Таким чином, оцінка ризиків та вразливостей дозволяє сформувати цілісне розуміння загроз для об'єктів критичної інфраструктури та визначити пріоритетні напрямки для вжиття

заходів щодо їх мінімізації. Це є невід'ємною складовою процесу управління ризиками та забезпечення безпеки критичної інфраструктури.

2.1 Аналіз можливих наслідків порушення функціонування об'єктів критичної інфраструктури

Аналіз можливих наслідків порушення функціонування об'єктів критичної інфраструктури є важливим етапом у процесі захисту критичної інфраструктури. Це дозволяє визначити можливі наслідки порушення функціонування об'єктів критичної інфраструктури, що можуть мати серйозні наслідки для економіки, енергетичної, фінансової та обороноздатності держави. Аналіз можливих наслідків порушення функціонування об'єктів критичної інфраструктури проводиться на основі аналізу можливих наслідків для основних послуг у всіх секторах економіки. Визначаються економічні збитки при заподіянні шкоди навколишньому природному середовищу у разі знищення об'єкта критичної інфраструктури. Наслідки класифікуються за видами збитків (наприклад, енергетичні, економічні, фінансові, безпекові) та визначаються основні види збитків для кожного типу та виду об'єкта критичної інфраструктури. На основі аналізу можливих наслідків проводиться оцінка ризиків порушення функціонування об'єктів критичної інфраструктури. Визначається рівень ризику для кожного об'єкта критичної інфраструктури на основі оцінки можливих наслідків. Розробляється методика розрахунку збитків від наслідків порушення функціонування об'єктів критичної інфраструктури та визначаються необхідні ресурси для забезпечення ефективного функціонування об'єкта критичної інформаційної інфраструктури. Таким чином, аналіз можливих наслідків порушення функціонування об'єктів критичної інфраструктури дозволяє сформувати цілісне розуміння ризиків та визначити пріоритетні напрямки для вжиття заходів щодо їх мінімізації. Це є важливою складовою забезпечення безпеки та стійкості критичної інфраструктури.

Порушення функціонування об'єктів КІ може мати катастрофічні наслідки для життя та здоров'я людей, економіки, національної безпеки та довкілля країни.

Наслідки можуть бути класифіковані за кількома напрямками:

– Вплив на життя та здоров'я людей:
– Загибель та травмування людей: Аварії на об'єктах КІ, що призводять до вибухів, пожеж, викидів небезпечних речовин, можуть призвести до масових жертв.
– Погіршення стану здоров'я: Перебої в постачанні питної води, тепла, електроенергії, медичних послуг можуть негативно вплинути на здоров'я людей, особливо вразливих груп населення, таких як літні люди, діти, люди з інвалідністю.

Психосоціальні наслідки: Надзвичайні ситуації, викликані порушенням функціонування КІ, можуть призвести до паніки, стресу, психологічних травм, масового виїзду людей з небезпечних зон.

1. Економічні наслідки:

• Прямі збитки: Руйнування об'єктів КІ, втрата продукції, перебої в роботі транспортної системи, телекомунікацій, сфери послуг можуть призвести до значних фінансових втрат.

• Непрямі збитки: Зниження темпів економічного зростання, втрата інвестицій, погіршення ділового клімату, зростання безробіття.

• Вплив на міжнародну торгівлю та співпрацю: Порушення функціонування КІ може негативно вплинути на експортно-імпортні операції, участь країни в міжнародних проектах та програмах.

2. Наслідки для національної безпеки:

• Підвищення ризику виникнення техногенних катастроф: Аварії на об'єктах КІ можуть мати транскордонний характер, що призводить до загрози безпеці сусідніх країн.

- Використання КІ як цілей для кібератак та диверсій: Порушення функціонування КІ може бути використано як інструмент для політичного тиску, шантажу, дестабілізації внутрішньої ситуації в країні.
- Зниження обороноздатності країни: Порушення функціонування КІ, що забезпечують роботу армії, правоохоронних органів, інших силових структур, може негативно вплинути на обороноздатність країни.

3. Вплив на довкілля:

- Забруднення навколишнього середовища: Викиди небезпечних речовин, аварії на об'єктах атомної енергетики, нафтогазового комплексу можуть призвести до забруднення ґрунту, води, повітря, негативно вплинути на флору та фауну.
- Природні катаклізми: Порушення функціонування об'єктів гідроенергетики може призвести до повеней, зсувів ґрунту, інших природних катаклізмів.
- Зміна клімату: Зниження ефективності енергогенеруючих об'єктів може призвести до збільшення викидів парникових газів, що негативно впливає на зміну клімату.

Захист КІ від різноманітних загроз є пріоритетним завданням для держави. Для цього необхідно:

- Вдосконалювати систему кіберзахисту КІ.

Підвищувати фізичний захист об'єктів КІ.

- Здійснювати регулярні навчання персоналу КІ.
- Розробляти та впроваджувати плани реагування на надзвичайні ситуації.
- Співпрацювати з міжнародними партнерами з питань захисту КІ.

.

2.2. Виявлення ключових загроз та вразливостей критичної інформаційної інфраструктури.

Виявлення ключових загроз та вразливостей критичної інформаційної інфраструктури є важливим етапом у процесі забезпечення її безпеки та стійкості. Це включає в себе виявлення нових векторів атак та вразливостей критичної інформаційної інфраструктури, розуміння потенційних кіберзагроз та їх впливу на об'єкти критичної інфраструктури. Це дозволяє визначити можливі точки проникнення та слабкі місця в системах управління та контролі критичної інфраструктури, що може бути використано для розробки ефективних заходів захисту. Оцінка ризиків та виявлення вразливостей критичної інформаційної інфраструктури є невід'ємною частиною забезпечення її безпеки. Це дозволяє визначити можливі наслідки порушення функціонування об'єктів критичної інфраструктури та розробити комплекс заходів для мінімізації ризиків. КІІ - це система інформаційних ресурсів та об'єктів, що забезпечують функціонування державних органів, військових структур, підприємств та організацій, порушення роботи яких може призвести до значних збитків державі та суспільству.

Ключові загрози для КІІ:

- Кібератаки: Найбільш поширена та небезпечна загроза. Кібератаки можуть бути спрямовані на крадіжку інформації, виведення з ладу систем, блокування доступу до даних, пошкодження або знищення інформаційних ресурсів.
- Шкідливе програмне забезпечення: Віруси, трояни, черв'яки, шпигунські програми та інші види шкідливого програмного забезпечення

•

можуть проникнути в інформаційні системи КІІ, завдаючи шкоди даним та інфраструктурі.

- Несанкціонований доступ: Витік інформації, несанкціоноване використання даних, проникнення в системи КІІ з метою крадіжки інформації або диверсій.
- Людський фактор: Ненавмисні дії або бездіяльність персоналу КІІ можуть призвести до порушення правил безпеки, витоку інформації, збоїв у роботі систем.

Технічні збої та аварії: Відмови обладнання, програмні помилки, природні катаклізми та інші фактори можуть призвести до порушення роботи систем КІІ.

- Соціальні інженерні атаки: Маніпулювання людьми з метою отримання доступу до інформації або систем КІІ.
- Фізичні атаки: Диверсії, саботаж, пошкодження або знищення об'єктів КІІ.

- Вразливості КІІ:
  - Недостатній рівень кіберзахисту: Застарілі програмні продукти, неналаштовані брандмауери, відсутність системи моніторингу та реагування на кіберінциденти.
  - Недостатній рівень фізичного захисту: Відсутність контролю доступу до об'єктів КІІ, слабкий захист від проникнення, неякісне обладнання для зберігання та обробки даних.
  - Недостатній рівень знань та навичок персоналу: Недостатня обізнаність про кіберзагрози, відсутність навичок роботи з системами безпеки, недбале ставлення до правил безпеки.
  - Недостатнє фінансування: Недостатні кошти на закупівлю сучасних програмних продуктів, обладнання, навчання персоналу, модернізацію інфраструктури.

- Відсутність чітких правил та процедур: Немає чіткої політики кібербезпеки, не розроблені плани реагування на кіберінциденти, не визначені ролі та відповідальні особи за кіберзахист.

Виявлення та усунення ключових загроз та вразливостей КІІ є пріоритетним завданням для забезпечення безпеки інформаційного простору країни. Для цього необхідно:

- Провести комплексну оцінку ризиків для КІІ.
- Розробити та впровадити систему кіберзахисту, що включає в себе:
- Застосування сучасних програмних продуктів та обладнання для кіберзахисту.
- Налаштування брандмауерів та систем моніторингу. о Регулярне оновлення програмного забезпечення.
- Забезпечення захисту даних.
- Підвищити рівень фізичного захисту об'єктів КІІ.
- Провести навчання персоналу КІІ з питань кібербезпеки.
- Забезпечити належне фінансування заходів з кіберзахисту КІІ.
- Розробити та впровадити чіткі правила та процедури з питань кібербезпеки КІІ.

2.3. Оцінка ймовірності реалізації загроз та потенційного збитку.

Оцінка ймовірності реалізації загроз - це процес визначення ймовірності того, що загроза може бути реалізована.

Даний процес дозволяє:

- Визначити пріоритети у сфері захисту КІ.
- Оптимізувати використання ресурсів для захисту КІ.
- Розробити ефективні заходи щодо запобігання та реагування на кіберінциденти.

•

Методи оцінки ймовірності реалізації загроз:

- Кількісні методи:
- Аналіз статистики кіберінцидентів. о Використання моделей оцінки ризиків.
- Якісні методи:
- Оцінка експертів. о Аналіз методів роботи зловмисників.

Методи оцінки потенційного збитку:

- Кількісні методи:
- Оцінка вартості активів КІ. о Оцінка економічних збитків, які можуть бути завдані внаслідок порушення функціонування КІ.
- Якісні методи:
- Оцінка впливу на життя та здоров'я людей. о Оцінка впливу на національну безпеку. о Оцінка впливу на довкілля.

Приклади оцінки ймовірності реалізації загроз та потенційного збитку:

- Загроза: Кібератака з метою викрадення персональних даних.
- Ймовірність реалізації: Висока.
- Потенційний збиток: Фінансові збитки для компанії, втрата довіри клієнтів, штрафи з боку регуляторів.
- Загроза: Диверсія на об'єкті критичної інфраструктури.
- Ймовірність реалізації: Низька.
- Потенційний збиток: Масові жертви, значні матеріальні збитки, екологічна катастрофа.

Оцінку ймовірності реалізації загроз можна проводити за допомогою різних методів, таких як:

Експертні оцінки: Цей метод передбачає опитування експертів у галузі інформаційної безпеки з метою отримання їхніх оцінок ймовірності реалізації загроз.

- **Аналіз статистики:** Цей метод передбачає аналіз статистики кіберінцидентів для визначення ймовірності реалізації різних типів загроз.
- **Моделювання ризиків:** Цей метод передбачає використання математичних моделей для оцінки ймовірності реалізації загроз та їхніх наслідків.

Потенційний збиток - це шкода, яка може бути завдана в результаті реалізації загрози. Його можна оцінити за допомогою таких методів, як:

- **Аналіз активів:** Цей метод передбачає визначення цінності інформаційних активів та оцінку шкоди, яка може бути завдана їм у результаті кіберінциденту.
- **Аналіз сценаріїв:** Цей метод передбачає розробку сценаріїв можливих кіберінцидентів та оцінку їхніх наслідків для організації.
- **Метод аналізу впливу на бізнес (BIA):** Цей метод передбачає оцінку впливу кіберінциденту на бізнес-процеси організації.

Фактори, які впливають на ймовірність реалізації загроз та потенційний збиток:

- **Характеристики загрози:** Тип загрози, її складність, доступність інформації про загрозу, наявність уразливих місць в системах організації.
- **Характеристики активу:** Цінність активу, його доступність, конфіденційність, цілісність.
- **Захисні заходи:** Наявність та ефективність захисних заходів, таких як брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення.
- **Мотивація зловмисника:** Мотивація зловмисника може впливати на те, які загрози він буде використовувати та як він буде їх реалізовувати.

В результаті оцінки ймовірності реалізації загроз та потенційного збитку можна:

- Прийняти рішення про те, які загрози потребують пріоритетної уваги.
- Розробити план реагування на інциденти.
- Визначити ресурси, необхідні для реалізації плану реагування на інциденти.
- Прийняти рішення про те, які інвестиції в інформаційну безпеку є виправданими.

Оцінка ймовірності реалізації загроз та потенційного збитку є важливою частиною процесу управління ризиками інформаційної безпеки. Цей процес дозволяє організаціям розуміти ймовірність виникнення кіберінцидентів та їхні наслідки, а також приймати обґрунтовані рішення щодо захисту своїх інформаційних активів.

Інструменти для оцінки ймовірності реалізації загроз та потенційного збитку:

Національний інститут стандартів і технологій (NIST): NIST пропонує ряд інструментів для оцінки ризиків інформаційної безпеки, таких як Cybersecurity Framework (CSF) та NIST SP 800-30.

Open Web Application Security Project (OWASP): OWASP пропонує ряд інструментів для оцінки вразливості веб-додатків, таких як OWASP Top 10.

Factor Analysis of Information Security (FAIR): FAIR - це метод кількісної оцінки ризиків інформаційної безпеки.

Важливо зазначити, що оцінка ймовірності реалізації загроз та потенційного збитку - це постійний процес. Загрози та вразливості постійно змінюються, тому необхідно регулярно переглядати та оновлювати оцінки ризиків.

Висновки до розділу 2

Оцінка ризиків та вразливостей є ключовим етапом у забезпеченні безпеки та стійкості об'єктів критичної інфраструктури. Цей розділ визначає методи та процедури для ідентифікації потенційних загроз, оцінки можливих наслідків порушень функціонування об'єктів та визначення рівня ризику. Оцінка ризиків та вразливостей дозволяє систематично визначити потенційні загрози, ідентифікувати слабкі місця в системах управління та контролю, а також визначити можливі наслідки порушень функціонування об'єктів критичної інфраструктури. Цей процес допомагає визначити пріоритетні напрямки для вжиття заходів щодо мінімізації ризиків та підвищення стійкості систем. Аналіз можливих наслідків порушень функціонування об'єктів критичної інфраструктури проводиться на основі оцінки впливу на основні послуги у всіх секторах економіки. Визначення економічних збитків, класифікація наслідків за видами збитків та оцінка рівня ризику для кожного об'єкта дозволяє сформувати цілісне розуміння загроз та визначити необхідні заходи для їх запобігання. Отже, розділ 2 відіграє важливу роль у процесі забезпечення безпеки та стійкості об'єктів критичної інфраструктури. Адекватна оцінка ризиків та вразливостей дозволяє вчасно виявляти потенційні загрози, реагувати на них та розробляти ефективні заходи для забезпечення безпеки та неперервності функціонування критичних систем.

РОЗДІЛ 3. РОЗРОБКА СТРАТЕГІЇ ТА ЗАХОДІВ ЗАХИСТУ

Після проведення оцінки ризиків та вразливостей, необхідно розробити стратегію та план заходів захисту, спрямованих на запобігання можливим загрозам та мінімізацію можливих ризиків.Розробка стратегії захисту включає в себе визначення основних цілей та завдань захисту критичної інфраструктури, встановлення пріоритетів заходів, розробку планів дій у разі виникнення кризових ситуацій, а також визначення відповідальних осіб та структур за впровадження стратегії.План заходів захисту включає в себе конкретні заходи та процедури, спрямовані на запобігання загрозам, виявленим під час оцінки ризиків, та забезпечення безпеки об'єктів критичної інфраструктури. Це може включати впровадження систем моніторингу та виявлення вторгнень, регулярні аудити безпеки, навчання персоналу з питань кібербезпеки та кризового управління, а також розробку планів відновлення після інцидентів. Розробка стратегії та заходів захисту є важливим етапом у підвищенні стійкості та надійності критичної інфраструктури перед можливими загрозами та ризиками. Цей процес допомагає підготуватися до потенційних небезпек та ефективно реагувати на них, забезпечуючи безпеку та неперервність функціонування об'єктів критичної інфраструктури.

3.1. Визначення основних етапів розробки стратегії захисту критичної інфраструктури.

Розробка стратегії захисту КІ є комплексом заходів, спрямованих на визначення пріоритетів, цілей та методів захисту об'єктів КІ від різноманітних загроз. Ефективна стратегія КІ гарантує стійкість та безперебійне функціонування критично важливих систем, що є життєво необхідними для національної безпеки та економічного розвитку країни.

Основні етапи розробки стратегії захисту КІ:

1. Визначення та аналіз об'єктів КІ:

- ***Ідентифікація об'єктів*:** чітке визначення переліку об'єктів, що належать до КІ, з урахуванням їх критичності та впливу на національну безпеку.
- ***Класифікація об'єктів*:** поділ КІ на категорії за рівнем критичності, залежно від їх важливості для функціонування держави та потенційних наслідків їх виведення з ладу.
- ***Аналіз ризиків:*** комплексне оцінювання потенційних загроз для кожного об'єкта КІ, таких як кібератаки, природні катаклізми, диверсії, людська помилка тощо.

2. Визначення цілей та завдань захисту КІ:

- ***Формулювання загальних цілей:*** визначення основних напрямків та очікуваних результатів реалізації стратегії захисту КІ.
- ***Постановка конкретних завдань:*** розробка чітких та вимірюваних завдань з урахуванням виявлених ризиків та потреб кожного об'єкта КІ.
- ***Встановлення пріоритетів:*** визначення пріоритетних завдань, які потребують першочергового вирішення з огляду на їх критичність та ймовірність виникнення загроз.

3. Вибір методів та засобів захисту КІ:

- ***Аналіз доступних методів:*** вивчення та оцінка різних методів та засобів захисту КІ, таких як організаційно-технічні заходи, кіберзахист, фізичний захист, резервування даних тощо.
- ***Підбір оптимальних методів:*** вибір найбільш ефективних та економічно доцільних методів захисту з урахуванням специфіки кожного об'єкта КІ та його потреб.
- ***Впровадження та інтеграція:*** інтеграція обраних методів та засобів захисту в існуючу систему безпеки КІ.

4. Розробка плану реалізації стратегії:

- ***Визначення ресурсів:*** визначення необхідних людських, фінансових та матеріально-технічних ресурсів для реалізації стратегії.
- ***Розробка календарного плану:*** визначення чітких етапів та термінів виконання завдань стратегії.
- ***Розподіл відповідальності:*** визначення відповідальних осіб та структур за виконання кожного етапу стратегії.

5. Моніторинг та оцінка ефективності:

- ***Встановлення показників ефективності*****:** визначення показників, що дозволяють оцінити рівень захищеності КІ та ступінь досягнення цілей стратегії.
- ***Регулярний моніторинг*****:** постійний контроль та оцінка ефективності реалізації стратегії.
- ***Внесення коректив*****:** внесення необхідних змін та доповнень до стратегії з урахуванням нових загроз, технологічних змін та результатів моніторингу.

Важливі аспекти розробки стратегії захисту КІ:

- Комплексний підхід**:** стратегія повинна охоплювати всі аспекти захисту КІ, включаючи організаційні, технічні, фізичні, кадрові.

3.2. Впровадження організаційно-технічних заходів для забезпечення безперервного функціонування об'єктів.

Організаційно-технічні заходи (ОТЗ) - це комплекс заходів, спрямованих на захист об'єктів від різноманітних загроз та забезпечення їх безперебійного функціонування. Впровадження ОТЗ є важливою складовою частиною системи безпеки будь-якого об'єкта, незалежно від його специфіки.

Основні групи ОТЗ:

Організаційні заходи:

-
  - Розробка та впровадження нормативних документів, що регламентують питання безпеки об'єкта. о Створення системи управління безпекою, що включає планування, організацію, контроль та вдосконалення заходів з захисту.
  - Підготовка та навчання персоналу з питань безпеки.
  - Забезпечення інформаційної безпеки об'єкта.
  - Організація пропускного режиму та контролю доступу до об'єкта.
- Технічні заходи:
  - Застосування технічних засобів охорони, таких як відеоспостереження, сигналізація, контроль доступу.
  - Захист інформаційних систем та даних. о Забезпечення інженерно-технічної стійкості об'єкта. о Регулярне обслуговування та ремонт технічних засобів.

Впровадження ОТЗ повинно ґрунтуватися на:

- Комплексному аналізі ризиків: Виявлення та оцінка потенційних загроз для об'єкта.
- Визначення пріоритетів: Визначення найбільш критичних загроз та заходів, необхідних для їх нейтралізації.
- Економічній доцільності: Вибір ОТЗ з урахуванням їх ефективності та бюджетних можливостей.
- Відповідності нормативним вимогам: Дотримання вимог законодавства та галузевих стандартів з питань безпеки.

Важливі аспекти впровадження ОТЗ:

- Системний підхід: Всі ОТЗ повинні бути взаємопов'язані та утворювати єдину систему безпеки об'єкта.
- Постійне вдосконалення: ОТЗ повинні регулярно переглядатися та оновлюватися з урахуванням нових загроз та технологічних змін.
- Навчання персоналу: Персонал об'єкта повинен володіти знаннями та навичками, необхідними для виконання своїх обов'язків з питань безпеки.

- Контроль та моніторинг: Ефективність ОТЗ повинна регулярно оцінюватися та контролюватися.

Впровадження ефективних ОТЗ дозволяє:

- Підвищити стійкість об'єкта до різноманітних загроз.
- Забезпечити безперебійне функціонування об'єкта.
- Зменшити ризики фінансових втрат та шкоди репутації.
- Захистити життя та здоров'я людей.

3.3. Розробка методик розрахунку потреб ресурсного забезпечення об'єктів критичної інфраструктури.

Методики розрахунку потреб ресурсного забезпечення КІ - це комплексні методи, що дозволяють визначити обсяги та види ресурсів, необхідних для безперебійного та безпечного функціонування цих об'єктів.

Основні етапи розробки методик:

1. Визначення видів ресурсів:

Людські ресурси: Кількість та кваліфікація персоналу, необхідні для експлуатації, обслуговування та захисту КІ.

Матеріально-технічні ресурси: Технічне обладнання, програмне забезпечення, інструменти та інші матеріальні ресурси, необхідні для роботи КІ.

Інформаційні ресурси: Дані, інформаційні системи та мережеві ресурси, необхідні для функціонування КІ.

Фінансові ресурси: Кошти, необхідні для придбання, експлуатації та обслуговування ресурсів КІ.

2. Аналіз ризиків:

- Виявлення та оцінка потенційних загроз для КІ, таких як природні катаклізми, кібератаки, людська помилка тощо. о Визначення ймовірності та наслідків реалізації кожної загрози.

•

3. Визначення потреб у ресурсах:

- Розрахунок обсягів ресурсів, необхідних для нейтралізації виявлених ризиків та забезпечення стійкості КІ.
- Урахування нормативних вимог, галузевих стандартів та кращих практик з питань ресурсного забезпечення КІ.

4. Оптимізація потреб у ресурсах:

- Аналіз можливостей для оптимізації та економного використання ресурсів.
- Застосування принципів раціонального та ефективного використання ресурсів.

5. Розробка методичних рекомендацій:

- Створення чітких та зрозумілих методичних рекомендацій з розрахунку потреб ресурсного забезпечення КІ. о Визначення показників та критеріїв оцінки достатності ресурсного забезпечення.

6. Впровадження та тестування методик:

- Запровадження розроблених методик на КІ з урахуванням їх специфіки. о Тестування та оцінка ефективності методик у реальних умовах.

7. Оновлення та вдосконалення методик:

- Періодичний перегляд та оновлення методик з урахуванням нових загроз, технологічних змін та нормативних вимог. о Вдосконалення методик на основі досвіду їх практичного застосування.

Важливі аспекти розробки методик:

- Комплексний підхід: Методики повинні враховувати всі види ресурсів, необхідних для КІ, а також взаємозв'язки між ними.
- Об'єктивність та наукова обґрунтованість: Розрахунки потреб у ресурсах повинні ґрунтуватися на даних аналізу ризиків, нормативних вимогах та кращих практиках.
- Гнучкість та адаптивність: Методики повинні бути гнучкими та адаптивними до змінних умов та нових викликів.

- Практична орієнтованість: Методики повинні бути чіткими, зрозумілими та простими у використанні.
- Врахування специфіки КІ: Методики повинні розроблятися з урахуванням особливостей функціонування та потреб конкретного об'єкта КІ.

Розробка та впровадження методик розрахунку потреб ресурсного забезпечення КІ - це важливий крок до підвищення стійкості та безпечного функціонування цих об'єктів, що є ключовим фактором національної безпеки та економічного розвитку країни.

3.4. Цільова модель технічних засобів забезпечення інформаційної безпеки.

Цільова модель технічних засобів ІБ описує бажаний стан системи ІБ з точки зору використовуваних технологій та методів. Вона слугує орієнтиром для розвитку та вдосконалення системи ІБ, ґрунтуючись на кращих практиках та актуальних загрозах.

Основні компоненти цільової моделі:

- Ідентифікація та аутентифікація: Забезпечення чіткої ідентифікації користувачів та автентифікації їхнього доступу до систем та ресурсів.
- Контроль доступу: Регулювання доступу користувачів до інформації та систем на основі принципів найменшого привілею та розділення обов'язків.
- Захист даних: Захист даних від несанкціонованого доступу, розкриття, зміни або знищення.
- Захист мережі: Захист мережевої інфраструктури від кібератак, таких як DDoS-атаки, вторгнення та перехоплення даних.
- Захист кінцевих точок: Захист робочих станцій, мобільних пристроїв та інших кінцевих точок від шкідливого програмного забезпечення та інших кіберзагроз.

- Моніторинг та реагування на інциденти: Постійна моніторинг систем ІБ для виявлення та реагування на кіберінциденти.
- Відновлення після збоїв: Забезпечення можливості відновлення систем та даних у разі кібератаки або іншого збою.

Переваги використання цільової моделі:

- Підвищення стійкості до кіберзагроз: Цільова модель допомагає організаціям визначити та усунути слабкі місця в системі ІБ, що зменшує ризик кібератак.
- Покращення ефективності ІБ: Цільова модель сприяє більш ефективному використанню ресурсів ІБ та спрощує управління системою.
- Підвищення відповідності вимогам: Цільова модель допомагає організаціям відповідати вимогам законодавства та галузевих стандартів у сфері ІБ.

3.4.1. Розробка та впровадження цільової моделі ІБ

Кроки з розробки та впровадження цільової моделі ІБ:

1. Оцінка ризиків:
   - Визначте всі активи ІБ, які потребують захисту.
   - Проаналізуйте ймовірні загрози та вразливості для цих активів.
   - Оцініть потенційний вплив кіберінцидентів на організацію.
2. Визначення цілей ІБ:
   - Визначте цілі ІБ, які мають захистити ваші активи.
   - Ці цілі повинні бути чіткими, вимірюваними, досяжними, релевантними та обмеженими в часі (SMART).
3. Вибір заходів безпеки:
   - Виберіть технічні, організаційні та фізичні заходи безпеки, які допоможуть вам досягти ваших цілей ІБ.

- Заходи безпеки повинні бути пропорційними ризикам, які вони мають пом'якшити.

4. Впровадження заходів безпеки:

- Розробіть та впровадьте політики та процедури ІБ.
- Навчіть персонал основам ІБ та того, як використовувати заходи безпеки.
- Впровадьте технічні рішення ІБ, такі як брандмауери, антивірусне програмне забезпечення та системи запобігання вторгненням.

5. Моніторинг та тестування:

- Регулярно моніторьте та тестуйте ваші заходи безпеки, щоб переконатися, що вони ефективно працюють.
- Проводьте періодичні оцінки ризиків, щоб оновити вашу цільову модель ІБ у разі потреби.

6. Вдосконалення та оновлення:

- Постійно вдосконалення та оновлювання цільової моделі ІБ, щоб вона відповідала новим загрозам та викликам.
- Будьте в курсі нових технологій та найкращих практик ІБ.

Переваги цільової моделі ІБ:

- Підвищення рівня захисту інформації: Цільова модель ІБ допомагає організаціям ідентифікувати та пом'якшити кіберзагрози, що призводить до кращого захисту інформації.
- Зниження ризиків: Цільова модель ІБ допомагає організаціям зменшити ризик кіберінцидентів, які можуть призвести до фінансових втрат, шкоди репутації та порушень нормативних вимог.
- Підвищення ефективності: Цільова модель ІБ допомагає організаціям більш ефективно керувати своїми ресурсами ІБ.
- Покращення прийняття рішень: Цільова модель ІБ надає організаціям чітке розуміння їхніх ризиків ІБ, що допомагає їм приймати обґрунтовані рішення щодо інвестування в безпеку.

3.5. Безпека мережі та способи її забезпечення.

Безпека мережі - це комплекс заходів, спрямованих на захист мережі та підключених до неї пристроїв від несанкціонованого доступу, використання, розкриття, зміни, руйнування або порушення конфіденційності.

Основні загрози для безпеки мережі:

Шкідливе програмне забезпечення: Віруси, трояни, хробаки, шпигунське програмне забезпечення та інші типи шкідливого програмного забезпечення можуть завдати шкоди даним, порушити роботу системи або викрасти конфіденційну інформацію.

Кібератаки: Хакери можуть використовувати різні методи, такі як DDoS-атаки, вторгнення та перехоплення даних, для крадіжки інформації, виведення з ладу систем або шантажу організацій.

Внутрішні загрози: Ненавмисні дії або зловмисні дії співробітників можуть призвести до витоку даних, порушення безпеки або інших проблем.

Соціальна інженерія: Хакери можуть використовувати методи соціальної інженерії, щоб обдурити людей і змусити їх розкрити конфіденційну інформацію або надати доступ до систем.

Способи забезпечення безпеки мережі:

Використання надійних паролів: Створення та використання надійних паролів для всіх облікових записів може допомогти запобігти несанкціонованому доступу.

Встановлення оновлень програмного забезпечення: Регулярне встановлення оновлень програмного забезпечення може допомогти усунути вразливості, які можуть бути використані хакерами.

Використання брандмауера: Брандмауер може допомогти захистити мережу від несанкціонованого доступу з Інтернету.

- Використання антивірусного програмного забезпечення: Антивірусне програмне забезпечення може допомогти виявити та видалити шкідливе програмне забезпечення.
- Фільтрація веб-трафіку: Фільтрація веб-трафіку може допомогти заблокувати доступ до шкідливих веб-сайтів.
- Навчання користувачів: Навчання користувачів основам безпеки мережі може допомогти їм уникнути поширених помилок, які можуть призвести до порушення безпеки.
- Шифрування даних: Шифрування даних може допомогти захистити їх від несанкціонованого доступу, навіть якщо вони будуть перехоплені.
- Резервне копіювання даних: Регулярне резервне копіювання даних може допомогти відновити їх у разі порушення безпеки.
- Створення політик безпеки: Розробка та впровадження політик безпеки може допомогти гарантувати, що всі користувачі дотримуються однакових правил щодо використання мережі.

Важливо зазначити, що безпека мережі - це постійний процес. Необхідно постійно оновлювати методи та інструменти захисту для того, щоб бути на крок попереду нових загроз.

Висновки до розділу 3

Розробка стратегії та заходів захисту є ключовим етапом у забезпеченні безпеки та стійкості об'єктів критичної інфраструктури. Цей процес передбачає комплексний підхід до визначення цілей, завдань та пріоритетів захисту, а також розробку конкретних заходів та процедур, спрямованих на запобігання можливим загрозам та мінімізацію ризиків.

Розділ 3 визначає основні етапи розробки стратегії захисту, включаючи аналіз ризиків та вразливостей, встановлення пріоритетів заходів, розробку планів дій у разі кризових ситуацій та визначення відповідальних структур. Цей

процес вимагає комплексного підходу, який враховує усі можливі загрози та ризики, які можуть вплинути на безпеку об'єктів критичної інфраструктури.

Особливу увагу слід приділити впровадженню організаційно-технічних заходів, спрямованих на забезпечення безперервного функціонування критичних об'єктів. Це включає в себе розробку внутрішніх регламентів та процедур, навчання персоналу, проведення аудитів безпеки, а також впровадження сучасних систем захисту, моніторингу та управління.

Розробка методик розрахунку потреб ресурсного забезпечення є важливим аспектом ефективного управління ресурсами та забезпечення готовності об'єктів до можливих загроз. Ці методики дозволяють точно визначити необхідні ресурси для забезпечення відповідного рівня безпеки та стійкості критичних об'єктів.

Створення системи управління інцидентами та реагування на кризові ситуації є невід'ємною складовою комплексного підходу до забезпечення безпеки критичної інфраструктури. Ефективна взаємодія між різними суб'єктами системи захисту, розробка планів дій на випадок надзвичайних ситуацій та забезпечення необхідними ресурсами дозволяють мінімізувати наслідки інцидентів та забезпечити безперервність функціонування критично важливих систем.

ВИСНОВКИ

Забезпечення безпеки та стійкості об'єктів критичної інфраструктури є комплексним та багатогранним процесом, який вимагає системного підходу та злагодженої взаємодії всіх зацікавлених сторін. Розроблена методологія охоплює ключові аспекти, необхідні для ефективного захисту критичних об'єктів від можливих загроз та забезпечення їх безперебійного функціонування.

Ідентифікація та категоризація об'єктів критичної інфраструктури, оцінка ризиків та вразливостей, розробка стратегії та заходів захисту, забезпечення ефективного функціонування, створення системи управління інцидентами та реагування на кризові ситуації, а також проведення регулярних навчань та тренувань персоналу є важливими складовими цього процесу. Кожен з цих елементів відіграє ключову роль у підвищенні рівня безпеки та стійкості об'єктів критичної інфраструктури.

Особливу увагу слід приділити налагодженню взаємодії між органами влади, операторами критичної інфраструктури та приватним сектором, а також обміну інформацією про загрози та кращі практики захисту на міжнародному рівні. Ефективна співпраця на національному та міжнародному рівнях, з урахуванням специфіки кожного об'єкта та категорії його критичності, дозволить підвищити рівень безпеки та стійкості критичної інфраструктури до сучасних загроз.

Гармонізація національних підходів до забезпечення кібербезпеки критичної інфраструктури є важливим напрямком роботи, який сприятиме створенню єдиної моделі забезпечення безпеки на основі найкращих практик та міжнародних стандартів. Це дозволить підвищити ефективність заходів захисту та реагування на кіберзагрози, що є ключовим для забезпечення стійкості та безпеки критичних об'єктів інфраструктури.

Таким чином, комплексне впровадження запропонованої методології, з урахуванням усіх її складових, дозволить підвищити рівень безпеки та стійкості

критичної інфраструктури України, забезпечити її ефективне функціонування та захист від сучасних загроз. Це сприятиме підвищенню рівня національної безпеки та забезпеченню сталого розвитку держави.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Критична інфраструктура: що саме до неї входить?". URL:https://pro-op.com.ua/question/9004-kritichna-infrastruktura-shcho-same-donei-vkhodit

2. "Як захистити критичну інфраструктуру України від ударів ...". URL:https://defence-ua.com/minds_and_ideas/jak_zahistiti_kritichnu_infrastrukturu_ukrajini_vid_udariv_rf_dalekobijnimi_raketami-9156.html

3. "Про затвердження Загальних вимог до кіберзахисту об'єктів критично...". URL : https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

"Розробка дорожньої карти ...: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2FVchnu_ekon_2014_6%281%29__30.pdf&P21DBN=UJRN

4. "Стратегія забезпечення інформаційної безпеки в організації". URL:https://www.itsec.com.ua/strategiya-zabezpechennya-informatsiynoyibezpeki-v-organizatsiyi/

5. "Інформаційна безпека: визначення, завдання та принципи". URL:https://www.itsec.com.ua/informatsiyna-bezpeka-viznachennya-zavdannya-taprincipi/

6. "Кібербезпека: що це таке і чому вона важлива". URL:https://www.itsec.com.ua/kiberbezpeka-shho-tse-take-i-chomu-vonavazhliva/

7. "Інформаційна безпека: основні аспекти та методи захисту". URL : https://www.itsec.com.ua/informatsiyna-bezpeka-osnovni-aspekti-ta-metodizakhistu/

8. "Заходи забезпечення інформаційної безпеки в організації". URL : https://www.itsec.com.ua/zakhodi-zabezpechennya-informatsiynoyi-bezpekiv-organizatsiyi/

9. “Об'єкти критичної інфраструктури України: все, що варто знати”. URL : https://www.kyivpost.com/uk/post/28283

10. Методика розрахунку потреб ресурсного забезпечення об’єктів критичної інформаційної інфраструктури. URL: https://sit.nuou.org.ua/article/view/252736

11. Кваліфікаційна робота КПІ ім.Ігоря Сікорського. URL : https://ela.kpi.ua/server/api/core/bitstreams/cadb137a-0a51-48f6-9f21-9457186aa739/content

12. Методика розрахунку потреб ресурсного забезпечення об’єктів критичної інформаційної інфраструктури. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1685796

13. Класифікація видів економічної діяльності. URL : https://kved.ukrstat.gov.ua/KVED2010/kv10_i.html–

14. Learning Guide VU21990 Recognise The Need For Cyber Security in An Organisation v9.1. URL:https://ru.scribd.com/document/496763437/Learning-Guide-VU21990Recognise-the-need-for-cyber-security-in-an-organisation-v9-1

16. "Developing an Effective Critical Infrastructure Protection Strategy" by the Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/

15. 17. "Critical Infrastructure Protection: A Primer" by the National Academies of Sciences, Engineering, and Medicine URL : https://nap.nationalacademies.org/

18. "Protecting Critical Infrastructure from Cyberattacks" by the Carnegie Endowment for International Peace URL : https://carnegieendowment.org/

19. "Cybersecurity for Critical Infrastructure: A Practical Guide" by Cybersecurity Insights URL : https://www.bitsight.com/glossary/critical-infrastructure-cybersecurity

20. "Developing a Comprehensive Cybersecurity Program for Critical Infrastructure" by Palo Alto Networks URL :https://www.paloaltonetworks.com/

21. "Protecting Critical Infrastructure from Cyber Attacks: A Framework for Developing a Comprehensive Strategy" by the National Academies of Sciences, Engineering and Medicine URL:https://nap.nationalacademies.org/catalog/27024/cybersecurity-issues-and-protection-strategies-for-state-transportation-agency-ceos-volume-1-project-summary-report

22. "Critical Infrastructure Protection: A Guide for Business and Industrial Leaders" by the American Society of Civil Engineers (ASCE) URL : https://ascelibrary.org/doi/book/10.1061/9780784410639

23. "Critical Infrastructure Protection: A Multi-Stakeholder Approach" by the Organization for Economic Cooperation and Development (OECD) URL:https://www.oecd.org/gov/risk/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm

24. "Cybersecurity and Critical Infrastructure Protection: A Primer for Electric Utilities" by the U.S. Department of Energy URL:https://www.energy.gov/sites/default/files/2021-06/Marjorie%20Kennedy%20JennerBlockLLP-A1.pdf

25. "Cybersecurity for Critical Infrastructure: A Landscape Review" by the European Union Agency for Cybersecurity (ENISA) URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cybersecurity-research