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: “ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРИМЕТРА КОРПОРАТИВНИХ МЕРЕЖ ”

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

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

_____ Андрій МАЗУРИК

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Андрій МАЗУРИК

Керівник:
к.т.н., доцент кафедри
Дмитро РАБЧУН

Рецензент:

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_____ Світлана ЛЕГОМІНОВА

“____” _____2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Мазурику Андрію Володимировичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Ефективність корпоративного управління інформаційною безпекою в Україні”

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

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

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

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

3. Вихідні дані до кваліфікаційної роботи: *підвищення ефективності захисту периметра корпоративних мереж, методи та засоби управління підвищення ефективності захисту корпоративних мереж, нормативні документи, стандарти, міжнародні стандарти.*

4. Перелік питань, які потрібно розробити:
   1. Здійснити теоретичний аналіз підвищення ефективності захисту периметра корпоративних мереж в Україні.
   2. Проаналізувати стан периметра корпоративних мереж інформаційної безпеки підприємств в Україні, особливо в галузі зв’язку.
   3. Розробити пропозиції та рекомендації щодо покращення та підвищення ефективності захисту периметра корпоративних мереж та управління інформаційною безпекою.
   4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання “02” жовтня 2023р

КАЛЕНДАРНИЙ ПЛАН

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

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	15.10.2023	виконано
3.	Аналіз підвищення ефективності захисту периметра корпоративних мереж, управління інформаційною безпекою.	25.10.2023	виконано
4.	Огляд стану периметра корпоративних мереж інформаційної безпеки підприємств в Україні, особливо в галузі зв’язку.	11.11.2023	виконано
5.	Формування загального результату тенденцій та проблем периметрів корпоративних мереж інформаційної безпеки підприємств в Україні особливо в галузі зв’язку.	15.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	18.01.2024	виконано

Здобувач вищої освіти _____ Андрій МАЗУРИК _
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН _
к.т.н., доцент кафедри
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

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

Направляється здобувач Мазурик А. В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Підвищення ефективності захисту периметра корпоративних мереж"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **МАЗУРИК Андрій** у кваліфікаційній роботі дослідив сучасний стан захисту периметра корпоративних мереж в Україні особливо в галузі зв'язку, визначив основні проблеми та розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності захисту периметра корпоративних мереж (підприємств). **МАЗУРИК Андрій** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на трьох науково-практичних конференціях.

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

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
к.т.н., доцент кафедри *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

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

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти: Мазурика Андрія Володимировича
на тему "ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРИМЕТРА КОРПОРАТИВНИХ МЕРЕЖ"

Актуальність:

Події останніх місяців в Україні показали нагальну необхідність забезпечення кібербезпеки об'єктів критичної інфраструктури, нагальний приклад компанія «Київстар» яка налічує більше 20 000 000 абонентів по всій території України. Для поневолення сучасної держави не обов'язково штурмувати військами всі її стратегічні об'єкти. Достатньо серед них виділити ключові підприємства та установи, які забезпечують життєдіяльність держави та управління нею і впливати на них. Нині такі підприємства та установи називають критичною інфраструктурою. Питання захисту критичної інфраструктури держави, насамперед від кібератак, є актуальною проблемою для всіх незалежних країн. Тому дослідження за темою кваліфікаційної роботи є актуальним і своєчасним.

Позитивні сторони:

1. Зміст кваліфікаційної роботи відповідає завданню. Студент показав достатній рівень знань і ступінь підготовленості до майбутньої роботи за фахом.
2. Обґрунтовано розглянуті основні управлінські процеси в сфері кібербезпеки: управління ризиками і інцидентами кібербезпеки.
3. Проведений аналіз можливостей доступних існуючих – рішень і запропоновані рекомендації щодо вдосконалення процесів управління подіями кібербезпеки.
3. Текст викладено грамотно, послідовно. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. недостатньо розкритий зміст розділу 2

Висновок:

кваліфікаційна робота заслуговує позитивну оцінку, а студент – Мазурик Андрій Володимирович гідний присвоєння освітньої кваліфікації Магістр з кібербезпеки за спеціалізацією управління інформаційною та кібернетичною безпекою.

Рецензент: _____

підпис *(Ім'я ПРІЗВИЩЕ)*

ВІДГУК КЕРІВНИКА

на кваліфікаційну магістерську роботу

здобувача вищої освіти: Мазурика Андрія Володимировича
на тему “ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРИМЕТРА КОРПОРАТИВНИХ МЕРЕЖ”

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних інформаційних впливів на інформаційні системи об’єктів критичної інфраструктури, під якими в першу чергу сьогодні розуміють атомні і гідроелектростанції, нафто – і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв’язку..

Для досягнення поставленої в роботі мети студент вирішив такі основні завдання: провести аналіз вимог до організації кібербезпеки на підприємстві критичної інфраструктури; З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб’єктів критичної інфраструктури в умовах інформаційного протиборства.

Мета і завдання дослідження полягає у дослідженні механізмів захисту об’єктів критичної інфраструктури від кібератак.; визначено напрями та методи забезпечення кібербезпеки підприємств критичної інфраструктури за допомогою автоматизованих систем.

Робота має науковий інтерес, стиль викладення матеріалу забезпечує доступність його сприйняття. Запропоновані студентом рекомендації можуть бути використані в процесі створення нової чи аналізі вже існуючої інформаційної системи підприємства критичної інфраструктури для майбутнього захисту від кібератак. Основні положення роботи обговорювалися на науковій та науково-технічних конференціях. Пояснювальна записка та графічний матеріал виконані самостійно, грамотно, з дотриманням вимог діючих стандартів і нормативних документів.

Висновок: кваліфікаційна робота Мазурика Андрія Володимировича “Підвищення ефективності захисту периметра корпоративних мереж” є завершеною, виконаною у відповідності з календарним планом самостійної розробки та націленою на вирішення актуального завдання.

Робота може бути допущена до захисту і заслуговує позитивної оцінки, а її автору може бути присвоєно освітню кваліфікацію Магістр з кібербезпеки за спеціалізацією управління інформаційною та кібернетичною безпекою.

Науковий керівник:
к.т.н., доцент кафедри . Дмитро РАБЧУН
(посада, вчене звання, ступінь) (підпис) (ініціали, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 87 стор., 6 рис., 0 табл., 33 джерел.

Метою роботи Метою даної науково-дослідної практики є визначення підвищення ефективності захисту периметра корпоративних мереж підприємств України.

Об'єктом дослідження – управління інформаційною безпекою, підвищення ефективності захисту периметра корпоративної мережі підприємства оператора зв'язку.

Предмет дослідження – ефективність захисту периметра корпоративної мережі підприємства оператора зв'язку.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі були застосовано метод системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення, аналізу та синтезу.

Короткий зміст роботи. У роботі проведено аналіз та визначення підвищення ефективності захисту периметра корпоративних мереж підприємств України, за приклад було взято одного з операторів стільникового зв'язку, визначено основні поняття, принципи, закони та стандарти. Розглянуто актуальний стан, фактори та виклики для ефективного корпоративного управління ІБ. В заключному розділі висвітлені та розглянуті реальні приклади кібератак ворога на підприємство зв'язку в стані війни, проблеми та надані рекомендації для покращення корпоративного управління інформаційною безпекою через системи моніторингу та протидії інформаційній та кібербезпеці.

Галузь застосування. Розглянуті стандарти та закони, розроблений базисні пункти та методи боротьби з кібератаками та загрозами на корпоративні системи управління інформаційною безпекою можуть бути використанні на початковому етапі захисту від кібератак в компаніях середнього та малого сегменту, або відповідно покращення вже наявного стану в контексті захисту та оптимізації роботи відділу кібербезпеки.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, КОРПОРАТИВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТИ, ЗАКОНИ.

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 106 pages, 6 figures, 0 tables, 33 sources.

The purpose of the work - The purpose of this research practice is to determine the effectiveness of the protection of the perimeter of the corporate networks of Ukrainian enterprises.

The object of the study is information security management, increasing the effectiveness of the protection of the perimeter of the corporate network of the telecommunications operator's enterprise.

The subject of the study is the effectiveness of the perimeter protection of the corporate network of the telecommunications operator.

Research methods. The method of system analysis, the theory of information security and the method of comparison and theoretical generalization, analysis and synthesis were used in the work to solve the scientific task.

Brief content of the work. The work analyzed and determined the improvement of the effectiveness of the protection of the perimeter of corporate networks of Ukrainian enterprises, one of the cellular operators was taken as an example, and the main concepts, principles, laws and standards were defined. The current state, factors and challenges for effective corporate IT management are considered. In the final section, real examples of enemy cyberattacks on a communications enterprise at war are highlighted and discussed, problems and recommendations are provided for improving corporate information security management through information and cyber security monitoring and countermeasures systems.

Field of application. The considered standards and laws, the developed basic points and methods of combating cyber attacks and threats to corporate information security management systems can be used at the initial stage of protection against cyber attacks in medium and small segment companies, or, accordingly, to improve the existing situation in the context of protection and optimization of the department's work cyber security.

KEYWORDS: INFORMATION SECURITY OF CORPORATE ENTERPRISE NETWORKS, INFORMATION SECURITY THREAT, CORPORATE INFORMATION SECURITY MANAGEMENT, STANDARDS, LAWS.

ЗМІСТ

ВСТУП

Актуальність. Події останніх місяців в Україні показали нагальну необхідність забезпечення кібербезпеки об’єктів критичної інфраструктури, нагальний приклад компанія «Київстар» яка налічує більше 20 000 000 абонентів по всій території України. Для поневолення сучасної держави не обов'язково штурмувати військами всі її стратегічні об'єкти. Достатньо серед них виділити ключові підприємства та установи, які забезпечують життєдіяльність держави та управління нею і впливати на них. Нині такі підприємства та установи називають критичною інфраструктурою. Питання захисту критичної інфраструктури держави, насамперед від кібератак, є актуальною проблемою для всіх незалежних країн.

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних інформаційних впливів на інформаційні системи об’єктів критичної інфраструктури, під якими в першу чергу сьогодні розуміють атомні і гідроелектростанції, нафто – і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, **загальнодержавні системи зв’язку**.

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує багато об’єктів критичної інфраструктури, виведення з ладу яких може призвести до надзвичайних ситуацій, пов’язаних із загибеллю людей, екологічними катастрофами, заподіянням великих матеріальних та **економічних збитків**.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб’єктів критичної інфраструктури в умовах інформаційного протиборства.

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні механізмів захисту об’єктів критичної інфраструктури від кібератак.

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

1. Провести аналіз основних характеристик об’єктів критичної інфраструктури, випадки кібератак на неї та нормативно-правову базу.
2. Дослідити особливості управління інформаційною безпекою на об’єктах критичної інфраструктури в умовах інформаційного протиборства, зокрема представити схему актуальних загроз інформаційній безпеці об’єктам критичної інфраструктури.

3. Визначити механізми захисту об’єктів критичної інфраструктури від кібератак відповідно до запропонованої класифікації загроз.

Об’єкт дослідження - засади забезпечення інформаційної безпеки об’єктів критичної інфраструктури в галузі зв’язку.

Предмет дослідження – виступає розвиток механізмів забезпечення та шляхи вдосконалення безпеки об’єктів критичної інфраструктури.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, теорії інформаційного протиборства.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою об’єкта критичної інфраструктури у контексті протидії загрозам, пов’язаним із веденням інформаційного протиборства.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу підприємства у відповідності до цілей бізнесу, корпоративних можливостей та ресурсів в умовах інформаційного протиборства.

РОЗДІЛ 1.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1 Характеристика об'єктів критичної інфраструктури

Поняття "інфраструктура" утворюється від злиття двох латинських слів "infa" - "нижче, під", і "struktura" - "структура, розташування" [1-4]. Під інфраструктурою розуміють комплекс взаємно пов'язаних обслуговуючих об'єктів або структур, що становлять і забезпечують основу функціонування системи.

До основних типів інфраструктур можна віднести:

- соціальну інфраструктуру як сукупність галузей і підприємств, що забезпечують нормальну життєдіяльність населення;
- транспортну інфраструктуру як сукупність галузей і підприємств транспорту [5-7];
- інженерну інфраструктуру як сукупність систем інженерно-технічного забезпечення будівель і споруд [8-15] та багато інших.

Між наявними інфраструктурами є складні зв'язки та взаємовідносини. Наприклад, інфраструктура економіки [16-20] являє собою сукупність галузей і видів діяльності, що обслуговують виробництво і господарство загалом, і включає в себе інфраструктури важкої та легкої промисловості, енергетики, транспорту та інших. Транспортна ж інфраструктура, у свою чергу, складається з інфраструктур авіаційного та залізничного транспорту, морського і річкового флотів, регіональних і міських транспортних інфраструктур [21-31].

Крім того, у державних інфраструктурах є низка специфічних інфраструктур, які повноцінно функціонують за наявності закордонних, зовнішніх зв'язків:

- інноваційна, що обслуговує інноваційну діяльність [32-33];
- ринкова, що забезпечує вільний рух товарів і послуг [34-35];
- інформаційна [36] та інші.

Є й інші спеціалізовані інфраструктури, наприклад, військова [37], діяльність яких має закритий характер.

Під національною або державною інфраструктурою прийнято розуміти сукупність усіх галузей промисловості та сільського господарства, споруд, установ, транспорту і комунікаційних мереж, що дають змогу забезпечити життєдіяльність організацій і виробництв конкретної країни. Наприклад, залізні та автомобільні дороги, трубопроводи та лінії електропередач, стаціонарні та розвідні мости, аеродроми і порти, житлові будинки і виробничі споруди, електростанції та сховища різного призначення, телефон і телеграф, радіо і телебачення, інтернет та інші засоби масової інформації.

В інфраструктурі суверенної держави особливо виділяють мережі, системи та сектори (сукупність елементів різних інфраструктур), від безпечної діяльності яких залежить стан навколишнього природного середовища, здоров'я і життя громадян та існування суспільства загалом. Комплекс таких секторів, систем або мереж, вихід з ладу або порушення функціонування яких здатне призвести до кризи на загальнодержавному, регіональному або місцевому рівні, стали називати критичною інфраструктурою [38-39].

Наприкінці 20-го століття у зв'язку зі зростанням кібернетичної загрози в розвинених країнах почалися дискусії про вразливість національних інфраструктур [40]. Увагу експертів було спрямовано не тільки на інформаційні (кібернетичні) інфраструктури, а й на всі інші сфери забезпечення життєдіяльності суспільства.

Серед країн Європи проблематикою забезпечення безпеки об'єктів критичної інфраструктури першими стали займатися у Великій Британії, де було дано визначення критичної національної інфраструктури як сукупності систем, які насамперед важливі для функціонування держави. До таких віднесли об'єкти, ліквідація або порушення роботи яких могла б піддати загрозі життя громадян або завдати серйозних негативних економічних чи соціальних наслідки для суспільства або його великої частини, а саме: державне управління, рятувальні служби, джерела енергії та сховища палива, водопровід, каналізація, телекомунікації, продовольство, санітарія (утилізація сміття), фінанси та економіка, комунікаційні мережі та служби, юстиція та захист громадського порядку, соціальне обслуговування, освіта, наука, прогноз погоди [41].

У 1998 році доктриною 63-го президента США критична інфраструктура була визначена як сукупність основних систем, які мають матеріальну або віртуальну платформу і впливають на фундаментальність економіки держави [42] - це телекомунікації, енергосистеми, банківський і фінансовий сектори, транспортна система, система водопостачання та рятувальні служби [43-44].

Усі європейські держави згодом також стали виділяти критичні національні інфраструктури, під якими розуміли сукупність систем, порушення функціонування однієї з яких може завдати серйозної шкоди економіці держави або призвести до негативних соціальних наслідків для суспільства.

Після подій 11 вересня 2001 року в лютому 2003 року в США було ухвалено Національну стратегію фізичної охорони критичної інфраструктури. Порівняно з доктриною 1998 року до її складу було включені ядерні електростанції, греблі, хімічна промисловість, сховища небезпечних речовин, бази оборонної промисловості.

Нині в країнах Євросоюзу визначено, що критична інфраструктура включає в себе фізичні об'єкти, ресурси, послуги та інформаційно-технічні засоби, мережі та інші інфраструктурні активи, порушення або знищення яких призводить до серйозних наслідків для здоров'я, безпеки або економічного добробуту громадян або ефективного функціонування уряду.

Таким чином, під критичною інфраструктурою слід розуміти сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може спричинити втрату управління або завдати істотної шкоди на загальнодержавному, регіональному, місцевому або об'єктовому рівні. Атомні та гідроелектростанції, що входять до її складу, хімічні та нафтохімічні комбінати, металургійні заводи і безліч інших державних підприємств і приватних установ стратегічного призначення належать до потенційно-небезпечних і критично важливих об'єктів.

Потенційно-небезпечний об'єкт (ПНО) - це об'єкт, на якому використовують, виробляють, переробляють, зберігають або транспортують радіоактивні, вибухопожежонебезпечні, небезпечні хімічні та біологічні речовини, що створюють реальну загрозу виникнення джерела надзвичайної ситуації [45].До подібних об'єктів відносять і об'єкти, на яких, відповідно до проектної документації, може перебувати понад п'ять тисяч осіб. Такі об'єкти також прийнято розділяти на технічно складні та унікальні об'єкти. До перших, тобто технічно складних об'єктів, прийнято відносити такі споруди:

1) об'єкти атомної енергетики (АЕС, сховища ядерного палива та радіоактивних відходів);

2) гідроелектричні станції та інші гідротехнічні споруди;

3) морські порти і термінали;

4) споруди зв'язку (радіо- і телевізійні вишки, наземні та підземні пункти комунікаційних вузлових з'єднань, антенні поля і телефонні станції);

5) теплові електростанції та котельні;

6) лінії електропередач і трансформаторні розподільні станції;

7) об'єкти авіаційної та космічної інфраструктури;

8) об'єкти інфраструктури залізничного та автомобільного транспорту (тунелі, шляхопроводи, розв'язки), а також канатні дороги;

9) метрополітен;

10) небезпечні виробництва (підприємства).

До других, тобто унікальних об'єктів, прийнято відносити споруди, які не ввійшли до групи технічно складних, але мають одну з таких технічних характеристик:

1) висота об'єкта понад 100 метрів;

2) прольоти або один із прольотів об'єкта понад 100 метрів;

3) консолі або одна з консолей об'єкта понад 20 метрів;

4) заглиблення підземної частини об'єкта понад 15 метрів нижче планувальної позначки землі.

Критично важливий об'єкт (КВО) - це об'єкт, порушення або припинення функціонування якого призведе до втрати управління економікою держави, одного або декількох державних суб'єктів або адміністративно-територіальних одиниць державного суб'єкта, їх незворотної негативної зміни (руйнування) або істотного зниження безпеки життєдіяльності населення [46].

За значущістю або масштабами потенційних загроз КВО прийнято поділяти на об'єкти загальнодержавного, суб'єктового або регіонального рівня, муніципального (територіального) або місцевого рівня.

За видами специфічних загроз КВО характеризують як небезпечні підприємства або об'єкти за однією або кількома класифікаційними ознаками. Це ядерно небезпечні об'єкти, до яких належать АЕС, ядерні установки науково-дослідного та виробничого призначення, а також підприємства зі зберігання, переробки та утилізації ядерних матеріалів та ядерного палива.

До **радіаційно небезпечних об'єктів** належать підприємства зі зберігання, переробки та утилізації радіоактивних відходів, а також науково-дослідні, виробничі та медичні установи, які використовують у своїй повсякденній діяльності радіоактивні матеріали та речовини.

Хімічно небезпечні об'єкти - це хімічні та нафтохімічні виробництва, металургійні та машинобудівні комбінати, підприємства з виробництва радіоелектронного та електротехнічного обладнання, а також підприємства харчової промисловості.

Біологічно небезпечні об'єкти - це підприємства з переробки та зберігання різної сільськогосподарської продукції, фармацевтичні та текстильні комплекси, а також фермерські господарства різного профілю (птахівницькі, м'ясомолочні, бавовницькі та інші).

До **техногенно небезпечних об'єктів** належать залізничні вузли, морські порти й аеропорти, метрополітени, мости, шляхопроводи й тунелі, об'єкти паливно-енергетичного комплексу, теплові електростанції та котельні, лінії електропередач і трансформаторні розподільні станції.

До **вибухопожежонебезпечних** об'єктів відносять магістральні нафто- і газопроводи, газокомпресорні та нафтоперекачувальні станції, сховища нафти і скрапленого газу, а також підприємства з виробництва і переробки рідкофазних і твердих вибухових речовин.

До **гідродинамічних небезпечних об'єктів** відносять гідротехнічні споруди промислового та водно-господарського призначення, такі як греблі, шлюзи, доки та інші.

Останній вид, відповідно до класифікаційних специфічних загрозам, - це **інформаційно та телекомунікаційно небезпечні об'єкти**. До них належать об'єкти державного управління (стаціонарні та мобільні пункти управління, вузли телефонного, телевізійного та радіозв'язку), а також об'єкти інформаційної та телекомунікаційної інфраструктури, такі як телевізійні та радіоцентри, серверні та комутаційні станції, концертні та кінозали, місця проведення публічних заходів. Крім цього, національними системами може бути передбачено встановлення додаткових класів КВО залежно від їхньої значущості, рівня очікуваних загроз і прогнозованих просторово-часових наслідків від їх настання.

Таким чином, з погляду оцінки складових частин критичної інфраструктури поняття потенційно-небезпечний об'єкт інфраструктури і критично важливий об'єкт можна вважати тотожними.

На кожному об'єкті критичної інфраструктури є інформаційно-управлінська складова, так звана критична інформаційна інфраструктура, виведення з ладу якої може не тільки зупинити виробничий процес підприємства, а й призвести до масштабних аварій і катастроф.

По-перше, національна (державна) критична інформаційна інфраструктура є складовою частиною національної (державної) критичної інфраструктури.

По-друге, оскільки під критичною інфраструктурою прийнято розуміти сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може спричинити втрату управління або завдати істотної шкоди на загальнодержавному, регіональному, місцевому або об'єктовому рівні то і критичну інформаційну інфраструктуру, як складову частину критичної інфраструктури, слід розглядати на відповідних рівнях.

По-третє, національна (державна) критична інформаційна інфраструктура призначена для забезпечення процесу управління життєдіяльністю держави, тому до її складу входять автоматизовані системи управління залізничним і автотранспортом, авіаційними та водними транспортними засобами, лініями електропередач, трубопроводами та іншими інфраструктурами, сукупність автоматизованих систем управління виробничими та технологічними процесами потенційно-небезпечних і критично важливих об'єктів, телефон і телеграф, радіо і телебачення, інтернет та інші засоби масової інформації.

По-четверте, на об'єктовому рівні під критичною інфраструктурою можуть розглядатися потенційно-небезпечні об'єкти, критично важливі об'єкти та інші об'єкти критичної інфраструктури, які не увійшли до перших двох груп.

З урахуванням вищеописаних чотирьох аспектів критична інформаційна інфраструктура (КІІ) об'єкта може бути як самостійною АСУ ТП об'єкта, так і сукупністю автоматизованих систем різного призначення, інформаційно-телекомунікаційних мереж і пристроїв. Головною ознакою належності цих систем, мереж і пристроїв до КІІ об'єкта - це розв'язання хоча б одного з трьох таких завдань [47]:

- здійснення управління виробничим або технологічним процесом на об'єкті, що розглядається;
- здійснення інформаційного забезпечення управління виробничим або технологічним процесом, що розглядається на об'єкті;

- здійснення інформування громадян про надзвичайні ситуації, що виникають на об'єкті.

Під КІІ, як правило [48], мається на увазі сукупність автоматизованих систем управління виробничими та технологічними процесами потенційно-небезпечних, критично важливих і інших об'єктів критичної інфраструктури та інформаційно-телекомунікаційних систем і мереж зв'язку, що забезпечують їхню взаємодію. Щоб впливати на КІІ об'єкта, до неї необхідно отримати фізичний доступ, який може бути легальним або санкціонованим, і несанкціонованим. Безумовно, негативний вплив на КІІ об'єкта здійснюється за допомогою несанкціонованого фізичного доступу до системи.

Як правило, такий доступ реалізується трьома шляхами: впливом на апаратну частину системи, впливом на провідні лінії телекомунікацій і впливом на бездротові лінії зв'язку. Інакше кажучи, якщо виключити вплив на КІІ об'єкта, що охороняється безпосередньо з приміщень і територій, розташованих усередині периметра, що охороняється, то головними вразливими місцями КІІ будуть дротові та бездротові лінії зв'язку й апаратно-програмні пристрої, розташовані за межами периметра.

Таким чином, під критичною інформаційною інфраструктурою розуміють сукупність автоматизованих систем управління виробничими та технологічними процесами потенційно-небезпечних, критично важливих та інших об'єктів критичної інфраструктури, інформаційно-телекомунікаційні системи та мережі зв'язку, що забезпечують їхню взаємодію. Її головними вразливими місцями є провідні та бездротові лінії зв'язку й апаратно-програмні пристрої, що розташовуються за межами периметра, що охороняється.

1.2 Історія кібератак на об'єкти критичної інфраструктури

Останні десятиліття в усьому світі бурхливо розвивається кіберзлочинність, що зумовлена розвитком інтернету і пов'язаних із ним інформаційних технологій, їх повсюдним впровадженням, як у виробничу діяльність, так і в повсякденне побутове життя кожної людини і всього соціуму загалом. Кожна з інфраструктур своїм функціонуванням забезпечує певний бік життєдіяльності суспільства. Будь-який збій у роботі інфраструктур, зумовлений природними причинами, технічними неполадками або навмисними діями, спричиненими злим умислом, одразу супроводжується певними негативними наслідками.

Як було зазначено раніше, до критично важливої інфраструктури належать об'єкти, мережі, служби та системи, збій у роботі яких у будь-якому разі

позначиться на здоров'ї, безпеці та добробуті громадян країни. У зв'язку з цим гарантоване надання життєво важливих послуг в умовах нових кіберзагроз визначає новий рівень відповідальності і державних органів, і приватних структур, що надають ці послуги. Крім цього, практично всі технологічні процеси, що протікають на критично важливих об'єктах, належать до автоматизованих виробництв, що використовують інформаційні технології, і тому є вразливими в плані кібер-вторгнення. Такого роду вторгнення або кібератаки спостерігаються вже протягом десятиліть. Розглянемо докладніше історію кібератак на об'єкти критичної інфраструктури, що відбулися у світі[49].

Термін "Інтернет" спадає на думку щоразу, коли ми думаємо про кібер-атаки на критичну інфраструктуру Але перша подібна кібер-атака сталася ще до появи Інтернету - у 1982 році. Тоді група хакерів змогла встановити троян у SCADA-систему, яка контролювала роботу сибірського нафтопроводу, що призвело до потужного вибуху.

Наступний інцидент стався через десять років, у 1992 році, коли було звільнено робітника нафтової компанії Chevron, який зламав комп'ютери в офісах компанії в Нью-Йорку і Сан-Хосе, що відповідали за системи попереджень, пере налаштувавши їх на аварію після запуску системи. Цей саботаж не було розкрито доти, доки не сталося витоку отруйної речовини в Редмонді (штат Каліфорнія), при цьому система не видала відповідних попереджень. У результаті тисячі людей були піддані величезному ризику протягом 10 годин, поки систему було відключено.

Колишній співробітник Maroochy Water System (Австралія) дістав два роки тюремного ув'язнення за злом у 2000 році системи управління водопостачанням, внаслідок чого мільйони літрів стічних вод потрапили в найближчу річку, що призвело також до затоплення місцевого готелю.

У 2003 році нафтова компанія зі США постраждала від хробака SQLSlammer, який проник у внутрішню мережу. Хоча це не призвело до зупинки виробництва, але він вплинув на внутрішні комунікації. Довелося витратити кілька днів для повного видалення хробака з мережі та оновлення систем для запобігання подальшим атакам. До речі, цей хробак був одним із найбільш руйнівних для компаній. Для поширення він використовував уразливість у серверах баз даних SQL (стандартний інструмент у корпоративних мережах). Вразливість було виправлено Microsoft у січні 2003 року. До речі, інша американська нафтова компанія почала оновлювати всі свої об'єкти одразу ж після появи цього патча, щоб убезпечити себе від цього хробака. Однак, для завершення оновлення необхідно було перезавантажити сервери, на яких цей патч

був встановлений, в той час як деякі з них знаходилися на нафтових платформах, де не було виділеного IT-персоналу. Для цього довелося відправляти фахівців на вертольоті. І поки вони летіли, хробак проник у деякі корпоративні системи і заразив ті з них, які ще не встигли оновити.

У 2005 році в Японії комп'ютер співробітника компанії Mitsubishi Electric був заражений шкідливою програмою, що призвело до витоку конфіденційних інспекційних документів щодо двох атомних електростанцій, що належать цій компанії.

У 2006 році два комп'ютери в лікарні (Велика Британія), що відповідають за управління комплексом променевої терапії для хворих на рак людей, були заражені шкідливою програмою. У результаті цього довелося відкласти лікування 80 пацієнтів. Через два роки ще три лікарні у Великій Британії були заражені варіантом хробака Mytob, після чого довелося відключити всі комп'ютери від мережі на 24 години для вирішення інциденту.

Незважаючи на довгий список інцидентів, перша в історії кібер-атака на Інтернет-інфраструктуру сталася 27 квітня 2007 року, коли в Естонії низка атак обвалила сайти різних організацій, включно з парламентом, різноманітними міністерствами, банками, газетами, різноманітними ЗМІ тощо.

У 2008 році була проведена кібератака на критичні інфраструктури: Stuxnet. Нині вже відомо, що це була скоординована атака ворожих спецслужб, спрямована на зрив ядерної програми Ірану. Вони створили хробака, який заразив комп'ютери, що керують урановими центрифугами на іранському заводі в Натанзі, унаслідок чого вони стали працювати на повній швидкості, тоді як інженери на своїх моніторах спостерігали нормальний режим роботи. Це завдало фізичної шкоди всім урановим центрифугам на заводі. Після цього випадку громадськість дізналася про такого роду загрози.

У 2012 році найбільша нафтова компанія у світі Saudi Aramco стала жертвою спрямованої атаки на свої офіси. Хакери отримали доступ до мережі завдяки атаці на одного зі співробітників компанії, через якого змогли отримати доступ до 30 000 комп'ютерів у мережі. У якийсь момент хакерам вдалося видалити вміст усіх комп'ютерів, тоді як на екранах показувався палаючий американський прапор. Відповідальність за атаку взяла на себе група хакерів, які називали себе "Меч правосуддя".

У 2013 році було заражено 200 комп'ютерів Департаменту автомобільних доріг і транспорту в окрузі Кук (штат Іллінойс, США). Ці системи відповідали за

підтримку сотні кілометрів доріг у передмісті Чикаго. У результаті атаки довелося відключати мережу на 9 днів, щоб вилікувати всі комп'ютери.

У 2014 році в Німеччині жертвою атаки став один із металургійних заводів. Використовуючи соціальну інженерію, хакери зуміли отримати доступ до комп'ютера одного співробітника, з якого вони змогли отримати доступ до внутрішньої мережі системи управління. У результаті цього стало неможливим вимкнути одну з домен, що завдало величезної шкоди підприємству.

2 січня 2014 року системний адміністратор японської AEC Monju виявив багаторазові віддалені підключення до одного з 8 комп'ютерів у центрі управління реактором. Причиною цього інциденту стало встановлення одним із співробітників оновлення безкоштовного відеоплеєра GOM Media Player. Унаслідок інциденту зловмисники вкрали частину інформації, зокрема конфіденційної, хоча наслідки виконання зловмисного програмного коду в центрі управління реактором могли б бути набагато небезпечнішими.

Українська енергосистема стала жертвою масштабної кібератаки у 2015 році, коли хакерам вдалося отримати доступ до критично важливих систем трьох великих енергорозподільчих компаній (так званих "обленерго") в Україні. Вони спричинили значні перебої в електропостачанні відключення електроенергії в більшій частині країни, яке тривало близько шести годин і залишило приблизно 225 000 домогосподарств без електроенергії через відключення близько 30 підстанцій. Атака розглядається як APT, оскільки вона була дуже добре підготовлена супротивником, а також була високотехнологічною. **Крім того, атака 2015 року також відома як перша кібератака, яка безпосередньо спричинила відключення електроенергії.**

В 2016 році разом із бумом різноманітних пристроїв, що підключаються до інтернету, - роутерів, "розумних будинків", онлайн-кас, систем відеоспостереження або ігрових приставок - з'явилися і нові можливості для кіберзлочинців. Подібні девайси зазвичай слабо захищені, тому їх легко заразити ботнетом. З його допомогою хакери створюють мережі зі зламаних комп'ютерів та інших пристроїв, які потім контролюють без відома їхніх власників. У результаті заражені ботнетами девайси можуть поширювати вірус і атакувати визначені хакерами цілі. Наприклад, завалити зверненнями сервер так, що той перестане встигати обробляти запити і зв'язок із ним пропаде. Це називається DDoS-атакою. І ось у жовтні 2016 року вся ця армада отримала сигнал завалити зверненнями провайдера доменних імен Dyn. Це призвело до того, що впали PayPal, Twitter, Netflix, Spotify, онлайн-сервіси PlayStation, SoundCloud, The New York Times, CNN і близько 80 інших компаній-користувачів Dyn. Відповідальність за напад

взяли на себе хакерські угруповання New World Hackers і RedCult. Жодних вимог вони не висували, проте загальний збиток від простою онлайн-сервісів склав близько 110 мільйонів доларів. Від Mirai вдалося відбитися за допомогою перерозподілу трафіку і перезапуску окремих компонентів системи Dyn. Однак те, що сталося, змушує замислитися про безпеку розумних пристроїв, які можуть становити майже половину потужностей усіх ботнетів.

В 2016-2017 роках від вірусу "NotPetya" постраждали найрізноманітніші компанії по всьому світу. Наприклад, в Австралії зупинилося виробництво шоколаду, **в Україні вийшли з ладу касові апарати**, а в Росії було порушено роботу туроператора. Збитків зазнали і деякі великі компанії, наприклад "Роснефть", Maersk і Mondelez. Атака могла мати і більш небезпечні наслідки. Так, "NotPetya" вдарив навіть по інфраструктурі моніторингу за ситуацією в Чорнобилі. "NotPetya" був спеціально націлений на бізнеси. Зловмисникам вдалося захопити контроль над сервером фінансового програмного забезпечення MeDoc. Звідти вони почали поширювати вірус під виглядом оновлення. Загальний збиток від злому склав понад 10 мільярдів доларів. Більше, ніж від будь-якої іншої кібератаки. Влада США звинуватила у створенні "Петі" угруповання Sandworm, яке також відоме як Telebots, Voodoo Bear, Iron Viking і BlackEnergy. На думку американських законників, воно складається з російських розвідників[50].

У 2017 році інтернет захлеснула справжня епідемія wcry-файлів. Звідси й пішла назва шифрувальника - WannaCry. Для зараження вірус використовував уразливість Windows на пристроях з операційною системою, яка ще не оновилася. Потім заражені девайси самі ставали розсадниками вірусу і поширювали його в Мережі. Вперше виявлений в Іспанії WannaCry за чотири дні заразив 200 тисяч комп'ютерів у 150 країнах. Програма також атакувала банкомати, автомати для продажу квитків, напоїв та їжі або інформаційні табло, що працюють на Windows і підключені до Мережі. Ще від вірусу постраждало обладнання в деяких лікарнях і заводах.

В 2019 хакери зламали системи понад 10 світових телекомунікаційних компаній і викрали великі обсяги персональних і корпоративних даних. Згідно з даними компанії з кібербезпеки Cybereason, зловмисники зламали компанії в більш ніж 30 країнах з метою отримати інформацію про членів уряду, співробітників правоохоронних органів і політиків. Атакуючі використали помилки в захисті веб-серверів мобільних мереж, що дало їм змогу залишатися непоміченими як для операторів, так і для самих користувачів. Хакери отримали доступ до управління доменами і банків докладних записів про виклики різних

мобільних мереж. Незважаючи на те що зловмисники не отримали доступ безпосередньо до записів телефонних розмов або змісту SMS-повідомлень, за цей час вони могли зберегти сотні гігабайт персональних даних про дзвінки користувачів.

В 2020 році американські спецслужби й самі виявилися вразливими перед хакерськими кібератаками. Причому злочинці продемонстрували, що теж можуть застосовувати хитрі схеми. Так, зловмисники проникли не в урядові системи, а зламали компанію з веб-розробки Netsential, яка надавала федеральним і місцевим агентствам технічні можливості для обміну інформацією. У підсумку хакерам з угруповання Anonymous вдалося вкрасти понад мільйон файлів американських правоохоронців і спецслужб: загалом 269 гігабайт інформації. Зломщики опублікували ці дані на сайті DDoSecrets. У відкритий доступ потрапили відео- та аудіоролики, електронні листи, службові записки, фінансова звітність, а також плани і розвідувальні документи.

На початку травня 2021 року найбільший у США трубопровід Colonial Pipeline став жертвою шифрувальника DarkSide. Унаслідок цього мережу компанії було зашифровано, а злочинці стали володарями великого масиву даних. Colonial Pipeline була змушена призупинити роботу паливопроводу. Через два дні після атаки влада оголосила надзвичайний стан у 17 штатах і окрузі Колумбія. Частину АЗС тимчасово закрили, а середня по країні ціна галона бензину піднялася до рекордних значень за останні 7 років. Через брак палива авіакомпанія American Airlines була змушена змінити деякі рейси. За дешифрувальник компанія заплатила викуп у розмірі 4,4 млн дол. США.

У середині жовтня 2021 року стало відомо, що зловмисник отримав доступ до бази даних уряду Аргентини, в якій міститься інформація про всі посвідчення особи громадян. Дані було виставлено на продаж: в інтернеті опинилися ID-картки всього населення Аргентини, вся вкрадена база містить інформацію про понад 45 млн громадян. Як підтвердження зловмисник надавав дані 44 відомих особистостей, зокрема президента країни і політичних діячів, а також пропонував подивитися дані будь-якого громадянина Аргентини. Злочинець продавав ці дані, даючи можливість реалізації інших атак, наприклад, шахрайства щодо користувачів.

У грудні 2023 – го року була здійснена нещадна хакерська атака на одного з найбільшого телекомоператора України. Атака принесла колосальні збитки для оператора та Країни загалом. Декілька діб було відключено близько 20 000 000 абонентів від мобільної мережі, вони могли здійснювати голосові дзвінки та користуватись доступом до мережі інтернет через технологію 4G/3G/2G. Не працювала велика кількість мобільних банківських терміналів по всій країні, охоронних систем, банківських сервісів, Дуже величезна проблема була створена для наших військових та оборонного комплексу – атака на оператора мобільного зв'язку також призвела для колосальних втрат для економіки Країни. Також одночасно з атакою на оператора булу здійснено атаку на одного з найкрупніших банків України. Відповідальність взяли на себе Російські спеціальні служби. Наразі причинені збитки телекомоператора та банку остаточно не підраховані нині, також не підраховані збитки причинені державному фінансовому сектору.

Цей список інцидентів показує, що небезпека кібер-атак на критичні інфраструктури цілком реальна, і сьогодні уряди всіх країн знають про ці ризики.

Історія кібератак, що відбулися у світі, показує, що на кожному об'єкті критичної інфраструктури є інформаційно-управлінська складова, так звана критична інформаційна інфраструктура, виведення з ладу якої може не тільки зупинити виробничий процес підприємства, а й призвести до масштабних аварій і катастроф.

1.3 Нормативно-правове забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Основними нормативно-правовими документами на даний час, які стосуються питання забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури в Україні є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р., Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», яке було введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 , Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» , Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 , Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 та деякі інші.

Так Закон України «Про основні засади забезпечення кібербезпеки України» [51] визначає правові та організаційні основи забезпечення захисту

життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У даному Законі України, серед інших, дано визначення таких термінів, як «інцидент кібербезпеки», «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «критична інформаційна інфраструктура», «об'єкти критичної інфраструктури», «об'єкт критичної інформаційної інфраструктури». Даним Законом України визначено, що об'єкти критичної інфраструктури являються об'єктами кібербезпеки, а об'єкти критичної інформаційної інфраструктури являються об'єктами кіберзахисту. Зазначені об'єкти, які можуть бути віднесені до критичної інфраструктури, сформульовані принципи забезпечення кібербезпеки, приведений перелік заходів для функціонування національної системи кібербезпеки. Положеннями цього Закону України визначено заходи, спрямовані на забезпечення кібербезпеки та кіберзахисту, а також визначена відповідальність за порушення законодавства у сфері кібербезпеки.

Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введене в дію Указом Президента України від 13 лютого 2017 року №32/2017 [52], серед іншого, передбачається формування пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту відповідних об'єктів. Крім того, передбачається протокол дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків.

Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [53], визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури. У відповідності до п.3 даних Вимог «кіберзахист об'єкта критичної інфраструктури

забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю». Відповідно до п.7 зазначених Вимог «у випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури». У цьому ж пункті зазначається, що «створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки». А технічне завдання, в свою чергу, формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005. Тобто, ми можемо констатувати, що технічне завдання на створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Крім того, у даних Загальних вимогах наведено перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та вимоги до формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки.

Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» [4], визначає механізм формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави. У відповідності до п.2 даного Порядку «об’єкти критичної інфраструктури» - це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні

комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення. Відповідно до п.4 зазначеного Порядку, включені до переліку **інформаційно-телекомунікаційні** системи об'єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно). У п. 8 даного Порядку зазначено, що заінтересовані органи формують пропозиції до переліку з урахуванням негативних наслідків, до яких може призвести кібератака **на інформаційно-телекомунікаційну систему**. Такими негативними наслідками є [54]:

- виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) ;
- негативний вплив на стан енергетичної безпеки держави (регіону) ;
- негативний вплив на стан економічної безпеки держави ;
- негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі ;
- негативний вплив на систему управління державою ;
- негативний вплив на суспільно-політичну ситуацію в державі ;
- негативний вплив на імідж держави ;
- порушення сталого функціонування фінансової системи держави ;
- порушення сталого функціонування транспортної інфраструктури держави (регіону);
- порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав .

Крім того, у даному Порядку вказано, що до переліку не включаються інформаційно-телекомунікаційні системи, які не мають виходу каналами електрозв'язку за межі контрольованої зони.

Стратегія національної безпеки України від 26 травня 2015 р. №287/2015 [55], спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16

вересня 2014 року № 1678-VII, і Стратегією сталого розвитку "Україна - 2020", схваленою Указом Президента України від 12 січня 2015 року № 5. Стратегією визначено цілі Стратегії національної безпеки України, актуальні загрози національній безпеці України, основні напрями державної політики національної безпеки України. У відповідності до п.3 Стратегії актуальними загрозами, серед інших є загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсів, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, загрози безпеці критичної інфраструктури. У відповідності до п. 4.12 Стратегії одним з основних напрямів державної політики національної безпеки України є Забезпечення кібербезпеки і безпеки інформаційних ресурсів. При цьому, пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Доктрина інформаційної безпеки України від 25 лютого 2017р. №47/2017 [56] визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Доктриною визначено її мета та принципи, національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, механізм реалізації Доктрини. У відповідності до п. 3. Стратегії встановлено, що національними

інтересами України в інформаційній сфері, серед іншого, є розвиток та захист національної інформаційної інфраструктури, розвиток інформаційного суспільства, зокрема його технологічної інфраструктури, розвиток системи стратегічних комунікацій України, забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України, захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом.

Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту .

Оскільки, у відповідності до статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я.

Висновки до першого розділу

1. Під критичною інфраструктурою слід розуміти сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може спричинити втрату управління або завдати істотної шкоди на загальнодержавному, регіональному, місцевому або об'єктовому рівні. Атомні та гідроелектростанції, що входять до її складу, хімічні та нафтохімічні комбінати, металургійні заводи і безліч інших державних підприємств і приватних установ стратегічного призначення належать до потенційно-небезпечних і критично важливих об'єктів. Таким чином, під критичною інформаційною інфраструктурою розуміють сукупність автоматизованих систем управління виробничими та

технологічними процесами потенційно-небезпечних, критично важливих та інших об'єктів критичної інфраструктури, **інформаційно-телекомунікаційні системи та мережі зв'язку**, що забезпечують їхню взаємодію. Її головними вразливими місцями є **провідні та бездротові лінії зв'язку** й апаратно-програмні пристрої, що розташовуються за межами периметра, що охороняється.

2.Історія кібератак, що відбулися у світі, показує, що на кожному об'єкті критичної інфраструктури є інформаційно-управлінська складова, так звана критична інформаційна інфраструктура, виведення з ладу якої може не тільки зупинити виробничий процес підприємства, а й призвести до масштабних аварій і катастроф.

3. Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту.

РОЗДІЛ 2

КІБЕРЗАГРОЗИ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Управління кіберризиками критичної інфраструктури

Зусилля промисловості та уряду щодо управління ризиками кібербезпеки були зосереджені на розробці програмного забезпечення для забезпечення безпеки, найкращих практик для проектування та експлуатації систем, а також збільшення інвестицій в кібернетичну робочу силу. Контрзаходи з кібербезпеки включають встановлення брандмауерів, програмного забезпечення шифрування, виявлення вірусів і розмежування систем. На питання про те, що є найбільш вразливим і які заходи є найбільш ефективними, керівники галузі, як правило, відповідають "все". Однак обмеженість ресурсів вимагає визначення пріоритетів на основі економічної ефективності заходів безпеки, а не сліпого прийняття всеохоплюючого підходу. У більшості випадків потреба в безпеці має бути збалансована з продуктивністю, оскільки різні варіанти можуть бути громіздкими і заважати функціонуванню системи та організації. Наприклад, випадково згенерований пароль з 16 символів навряд чи буде легко запам'ятовуватися, навіть якщо він буде ефективним.

Багато зусиль з управління кібернетичними ризиками ґрунтуються на управлінському підході "зверху вниз", з метою заохочення розробників та операторів систем до впровадження найкращих практик, але часто без конкретних міркувань щодо структури системи[57]. Наприклад, Міністерство оборони США зобов'язує свої відомства і служби враховувати питання кібербезпеки при розробці та експлуатації промислових систем управління (ПСУ), але без особливих вказівок щодо того, як це зробити. Існує низка загальних документів на цю тему. Більшість практик управління кіберризиками для захисту інфраструктури можна розділити на три групи:

а) Структурні (склад і структура ПСУ та апаратних комплексів)

б) Процедурні (управління та функціонування системи)

в) Реагування (реагування та контроль збитків після виявлення інциденту)

Адаптовані ймовірнісні методи аналізу ризиків призначені для оцінки ефективності кожного з цих варіантів для конкретних організацій більш детально, ніж загальні рекомендації. Основна увага приділяється загальній структурі проблеми аналізу ризиків з трьома ілюстративними прикладами для подальшого розгляду компромісів і пріоритетів: емпіричний аналіз бази даних інцидентів кібербезпеки, оптимізаційна модель, розроблена для інцидентів кібербезпеки, оптимізаційна модель, призначена для збалансування операційної ефективності системи з її захистом від кібератак, а також динамічна ігрова модель деяких взаємодій операторів інфраструктури та їх супротивниками у кіберпросторі.

Загальна система аналізу кібернетичних ризиків призначена для підтримки рішень, які приймаються захисниками в умовах невизначеності, з якими вони стикаються. Ця всеохоплююча модель кіберризику та ефективності різних контрзаходів, яка має бути адаптована до випадку конкретної організації. В її основі все лежить на взаємодії, зведеної до одного ходу з кожного боку, між керівником системи та потенційними зловмисниками різного роду[58]. Ця діаграма впливу представляє структуру моделі, яка повинна бути розроблена для представлення характеристик організації, що представляє інтерес, та її інформаційної системи.

Рис. 2.1: Структура діаграми прийняття рішень щодо вибору варіантів забезпечення кібербезпеки.

Особа, яка приймає рішення, як правило, знає більшу частину відповідної інформації про організацію, отже, детермінований вузол у верхній частині Рисунку 2.1. Цей детермінований вузол визначає тип об'єкт та його активи. Це може бути, наприклад, національна лабораторія, промислова компанія, що володіє чутливою інтелектуальною власністю, комерційне підприємство з фінансовими даними, такими як інформація про кредитні картки, **бази даних з персональними**

даними абонентів мобільного оператора та їх рахунків або лікарня, вразлива до здирництва. Кожен з цих типів організацій більшою чи меншою мірою піддається загрозі з боку різних типів зловмисників - країн, окремих осіб або злочинних угруповання. Вразливість описана на рис. 1, відноситься до можливих точок доступу і характеризується ймовірністю вторгнення через ці точки. Ці точки вторгнення можуть бути виявлені шляхом аналізу структури інформаційної системи та її зв'язки з операціями. Вони, як правило, відомі або можуть бути виявлені, але це не завжди так буває. Декілька питань, можливо, доведеться вирішити спочатку і за необхідності, розглядати їх як невизначеності:

- Які основні активи організації, де вони знаходяться і з чим пов'язані?

Наприклад, компанії, що випускають кредитні картки, такі як Master Card та Visa, у 2012 році стали жертвами атак шляхом злому сторонніх процесорів. У цьому випадку питання полягає у визначенні структуру та місцезнаходження інформації про клієнтів та їх зв'язок з клієнтами та продавцями, які користуються їх послугами.

- Які заходи захисту можна розглянути, враховуючи практичні, а також юридичні обмеження від наступальних дій у відповідь?
- Які ризики інсайдерської атаки з огляду на те, хто має доступ до всіх або деяких частин інформаційної мережі?

Ця основна складова ризику залежить від характеру організації та управління її персоналом і підрядниками (процедури найму, перевірки, процедури звільнення та доступ до інформації). Одним із прикладів є атака Сноудена на інформаційні системи NSA на інформаційні системи NSA, що зберігалися в компанії Booz Allen, де інсайдерам був наданий широкий доступ до цих файлів. Інший випадок - злам кредитних карток Target у 2013 році підрядниками з технічного обслуговування.

Решту невизначеностей загальної моделі можна розділити на три основні групи: демографічні характеристики нападників, сценарії атак та їх наслідки.

Зловмисники різняться за ресурсами та рівнем кваліфікації, від хакерів низького класу до добре забезпечених, досвідчених[59]. Спектр включає в себе:

- Хакери та дрібні злочинці, які як правило, не завдають великої шкоди, але можуть, наприклад, серйозно змінити або зіпсувати веб-сайти.

- Злочинні організації, які прагнуть отримати грошову вигоду шляхом крадіжки інтелектуальної власності, фінансової інформації або викупу за викрадені дані. Деякі з них, наприклад, останнім часом спеціалізуються на "програмах-вимагачах", які наразі націлені на лікарні, або на викраденні фінансових записів, таких як інформація про кредитні картки.
- Спонсоровані державою наполегливі зловмисники, які намагаються перешкоджати функціонуванню організацій і країн, а також викрадати інтелектуальну власність країн, а також викрадати інтелектуальну власність, прагнучи до негайного вторгнення або засобів для цього пізніше.
- Інші компанії або організації, які можуть прагнути отримати вигоду від заподіяння шкоди конкуренту або викрадення його інтелектуальної власності шляхом промислового шпигунства.
- Терористичні організації, які можуть просто мати на меті завдати максимальної шкоди суспільству та отримати ресурси для підтримання своєї діяльності.
- Зловмисні інсайдери, до яких можуть належати незадоволені працівники або особи, чиї цінності не збігаються з цінностями організації, в тому числі люди, які просто прагнуть отримати грошову вигоду.
- Підрядники, такі як оператори з технічного обслуговування, які можуть мати або знайти доступ до внутрішньої інформаційної мережі з метою порушення роботи організації, або як чисте зловживання службовим становищем, або для продажу викраденої інформації, **так як це сталося в грудні 2023 року в Україні**.

У кожному випадку виникають питання: Хто може бути цими зловмисниками, чого вони хочуть, що вони знають і що у них є? У глобальній моделі певна компанія, виходячи зі свого досвіду і характеру своїх активів, може бути в змозі скласти розподіл ймовірності на тип зловмисників, з якими вона може зіткнутися, та їхні методи атаки.

Наступною невизначеністю для захисника є його вразливості та точки входу, через які зловмисники можуть проникнути в його систему. До них відносяться:

- Ненавмисні дефекти або "баги" в програмному забезпеченні захисника, які могли бути внесені під час початкового програмування.
- Навмисні дефекти, які можуть бути внесені в комп'ютерне обладнання або програмне забезпечення по ланцюгу поставок потенційними зловмисниками з метою їх подальшого використання.
- Периферійні дефекти - недоліки або "помилки" в системах, що знаходяться поза контролем особи, яка приймає рішення які можуть бути внесені через обладнання, підключене до основної системи. Вірус на ноутбуці підрядника може бути використаний для проникнення в захищену систему, якщо вони підключені до мережі, і, як згадувалося раніше, активи компанії, що випускає кредитні картки можуть бути вразливими до злому сторонніх процесорів.

Таким чином, різні організації можуть піддаватися різним видам атак з ймовірними розподілами, які залежать від характеру їх діяльності[60]. Найпоширеніші сценарії атак включають втрату або крадіжку пристроїв, витік даних, зловмисні атаки через електронну пошту (фішинг), атаки на веб-сайти, а також шкідливе програмне забезпечення, що впроваджується через веб-браузер або USB-накопичувачі. База даних Common Vulnerability and Exposures (CVE), створена корпорацією MITRE, надає числову систему оцінок призначену для класифікації ймовірності різних відомих недоліків програмного забезпечення, які можуть бути використані для завдання шкоди, або надати противнику контроль чи доступ до системи.

Успішна атака, наприклад, з метою викрадення або пошкодження інтелектуальної власності, як правило, включає чотири етапи:

- Вхід в систему.
- Переміщення всередині системи для отримання несанкціонованого доступу до різних її частин.
- Завдання шкоди як програмному, так і апаратному забезпеченню.
- Отримання, фільтрування та використання інформації, що вас цікавить.

Контрзаходи можуть бути застосовані для боротьби з кожною або декількома з цих фаз атаки, включаючи протипожежні стіни для захисту від

проникнення, системний "лабіринт" для перешкоджання вільній навігації, бар'єри для проникнення та моніторинг використання даних для якнайшвидшого виявлення атаки та мінімізації збитків (наприклад, втрата файлів викрадених кредитних карток). Реалізація кожного з цих імовірнісних вузлів і відповідні вузли прийняття рішень з боку цільової організації представляють різні способи, якими вказаний супротивник може атакувати конкретну мережу і їх шанси на успіх.

Вплив успішної атаки, таким чином, залежить від характеру організації, пошкоджених або викрадених активів, а також від ефективності заходів з контролю за пошкоджених або викрадених активів. Як згадувалося раніше, ключовим фактором є час, що пройшов між інцидентом та його виявленням. Наприклад, втрата інформації про кредитну картку може бути виявлена самими потерпілими, але після цього банкам та організаціям можуть знадобитися тижні для того, щоб ефективно контролювати збитки.

Таким чином, збитки від кібератак на бізнес-операції та репутація компанії-захисника сильно варіюються залежно від характеру та цінності цілей. Вплив на бізнес-операції може бути суттєвими, з втратою виробництва під час простою, розслідуванням інциденту, усуненням наслідків, а також втратою активів, таких як критичні технології в космічній компанії. Крім того, організація може зазнати шкоди репутації, яка, в деяких випадках, може бути виміряна шляхом втратою вартості акцій. Наскільки відомо, оцінка збитків від атаки може бути переважно якісною. Проте кількісні, аналітичні та економічні методи існують і можуть бути використані для агрегування цих на основі фактичних даних або експертних оцінок.

Відключення електроенергії в Україні 23 грудня 2015 року - перший відомий випадок кібератаки що призвела до відключення електроенергії - демонструє цінність кількісної оцінки ризиків та переваг розумної об'єднаної електричної мережі. У цьому інциденті три українські електророзподільні компанії стали жертвами скоординованої компанії, яка включала в себе фішингову кампанію з метою закріпитися в корпоративних мережах; реєстратори натискання клавіш для отримання облікових даних для доступу до мереж промислових систем управління (АСУ ТП); та доступ до систем диспетчерського контролю та збору даних Acquisition (SCADA), які дозволяють здійснювати віддалений моніторинг та управління, і використовувалися для перехоплення людино-машинних інтерфейсів та видачі команд на відкриття вимикачів. Початковий аналіз свідчить про те, що ці три розподільчі компанії могли стати мішенню, оскільки вони були найбільш пов'язані між собою. Зокрема, рівень

автоматизації та зв'язку в їхніх розподільчих мережах дозволив зловмисникам не тільки перейти з корпоративної мережі в мережу управління, а й отримати віддалений контроль над SCADA-системою для відкриття вимикачів підстанцій. Таке підключення дозволило зловмисникам відключити тридцять розподільчих підстанцій, що призвело до знеструмлення близько 225 000 мешканців на кілька годин. Це вторгнення відбулося, незважаючи на сильні контрзаходи з кібербезпеки, які були запроваджені розподільчими компаніями, включаючи мережу управління, яка була добре відокремлена від бізнес-мережі за надійним брандмауером.

Дійсно, поява розумної мережі обіцяє забезпечити багато переваг для загального функціонування системи розподілу електроенергії, включаючи підвищення ефективності, поліпшення надійності, краще включення відновлюваних джерел енергії, а також більший вибір для споживачів електроенергії. Проте, через збільшення кількості міждержавних з'єднань, ті ж самі технології, що покращують продуктивність розумних енергосистем, не можуть бути застосовані до технології, які покращують продуктивність інтелектуальної мережі, також піддають її цифровим загрозам, таким як атаки на відмову в обслуговуванні, крадіжка інтелектуальної власності, вторгнення в приватне життя та саботаж критично важливих об'єктів національної інфраструктури. Розумна мережа збільшує кількість потенційних точок доступу і вразливостей, а враховуючи інтегрований характер цих кіберфізичних систем, кібернетичні збої в електромережі можуть каскадом поширюватися на інші об'єкти критично важливої інфраструктури, наприклад, транспортні мережі, системи водопостачання або фінансові системи і спричинити значні фізичні збитки та економічну кризу.

Таким чином, переваги від збільшення підключення повинні бути зважені з ризиком підвищеної вразливості до кібератак, оскільки зацікавлені сторони в електроенергетичному секторі розглядають можливість модернізації традиційної архітектури електромереж шляхом впровадження технологій "розумних мереж" та нових інтелектуальних компонентів.

Для того, щоб визначити оптимальний ступінь приєднання, розглянемо, по-перше, фізичну електричну мережу, представлену у вигляді неорієнтованого графа, де кожен вузол є окремою електричною точкою мережі (генераторами, споживачами або підстанціями), а ребра - лініями електропередач між ними (див. рис. 6). У будь-який момент оператор системи може вирішити підключити підмножину вузлів до хмари, створюючи накладену інформаційну мережу поверх фізичної мережі. Кожне нове підключення до інформаційного вузла є

потенційним вектором для кібервторгнення, а кожне інформаційне з'єднання надає можливість для кібератаки, яка може поширитися на сусідні вузли фізичної мережі[61]. Оператори системи та органи влади, які балансують розподіл електроенергії, як правило, зазвичай об'єднують споживачів у великі навантаження. Тому в моделі має сенс об'єднати загальне навантаження системи в агреговані вузли таким же чином.

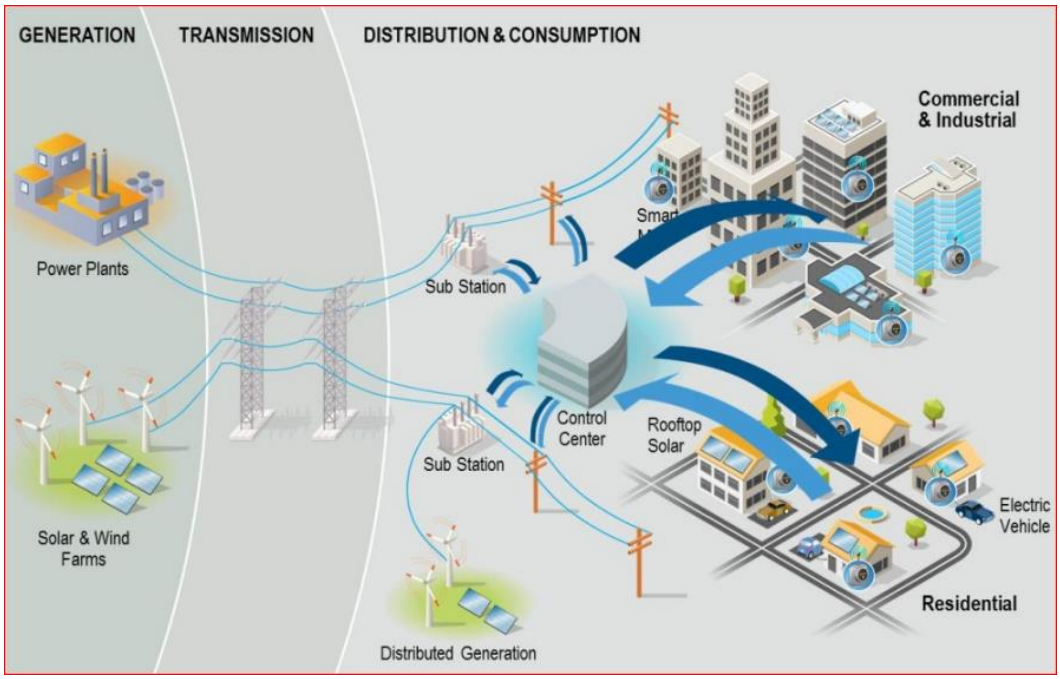

Рис. 2.2 Концептуальний огляд системи, в якій електропостачальна компанія послідовно розглядає граничні вигоди та ризики від приєднання одного додаткового вузла до своєї інтелектуальної мережі.

Інтуїтивно, коли мережа стає розумнішою, можна очікувати двох речей:

а) Гранична вигода зменшиться. Для багатьох технологій "розумних" мереж більша частина вигоди може бути отримана при помірному рівні підключення. Наприклад, звіт показав, що встановлення технології зниження напруги на 40 відсотках розподільчих фідерів досягає 80 відсотків вигоди, отриманої від модернізації всіх фідерів. Аналогічна тенденція була продемонстрована для "розумних" лічильників, які складають вдосконалену інфраструктуру обліку.

б) Зросте ризик кібербезпеки. Хоча форма залежності не є одразу очевидною, збільшення зв’язків може спричинити збільшення кібератак (через збільшення кількості шляхів атак), так і їх наслідків (через більш тісні зв'язки між компонентами управління в електромережі).

Імовірнісний аналіз ризиків , запропонований для кількісної оцінки цього компромісу для різних технологій "розумних" електромереж зображено на

Рисунку 2.3. Цей підхід доповнює існуючі статистичні дані інженерними моделями електромережі, мережі зв'язку мобільного оператора, або підприємства з критичної інфраструктурою, стохастичними моделями, імітацією сценаріїв атак та мережевим аналізом для того, щоб простежити динамічну еволюцію режимів відмов, викликаних кібернетичними вразливостями. На першому етапі виконується аналіз системи для визначення класів відмов сценаріїв, які можуть бути викликані експлуатацією кібервразливостей в мережі інтелектуальних мереж, як на основі думок галузевих експертів та відомих інцидентів. Потім використовується економічна диспетчерська модель для оцінки фінансових вигод і ризиків від підвищення інтелектуальності, виходячи з фізики та економіці її впливу на систему. Результати економічного аналізу є, таким чином, вихідними даними для імовірнісної моделі, що використовується для визначення стратегії оптимального розподілу ресурсів кібернетичної безпеки. Наприкінці, модель аналізу рішень (припускаючи нейтральність ризику) використовується для порівняння ефективності можливих заходів зі зниження ризиків, таких як покращення кіберзахисту, сегментація мереж критичної інфраструктури, встановлення систем резервного копіювання та кіберстрахування. На основі цих результатів можна оцінити оптимальний ступінь підключення.

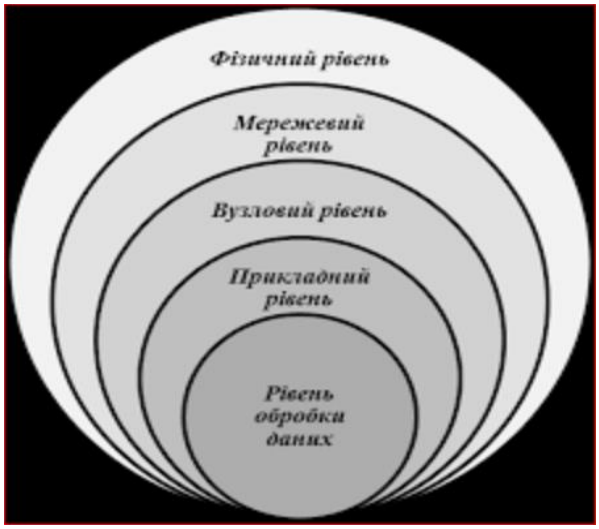

Рис. 2.3 Огляд підходу до аналізу кіберризиків "розумної" енергосистеми.

Такий підхід до моделювання має багато переваг: він надає інструменти для полегшення поєднання статистичних даних з експертними оцінками та інженерними моделями; він дозволяє особам, які приймають рішення, виконувати аналіз чутливості для ключових параметрів, включаючи їх власну толерантність до ризику та деякі інші специфічні для організації фактори безпеки; він добре підходить для роботи з багатьма рівнями невизначеності що вносяться складністю інженерних систем та впливом людської поведінки; і вказує на те, на чому слід зосередити додаткові зусилля з моделювання[62].

Другим наймасштабнішим випадком втручання кіберзлочинців спеціальних служб Російської Федерації на ІТ інфраструктуру одного з найбільших телекомоператорів України в грудні 2023 року. Було виявлено втручання в мережу за допомогою використання доступу до мережі (логіну та паролю) одного зі співробітників. Підготовка до втручання готувалась мінімум пів року. Втручання принесло дуже серйозні наслідки та величезні фінансові втрати для оператора та економіки Держави. Було знищено всю віртуальну ІТ інфраструктуру залишено без будь-якого зв'язку та доступу мережі інтернет біль ніж 20 000 000 абонентів України.

Офіційні коментарі компанії:

Частково зруйнована IT-інфраструктура: CEO Київстару про головну ціль атаки на оператора

Компанія Kyivstar наразі не може окреслити терміни повноцінного відновлення роботи мобільного оператора після здійснення на нього хакерської атаки. На цьому в ефірі "Ми-Україна" наголосив CEO "Київстару" Олександр Комаров.

Він наголосив на тому, що інформацію про запуск роботи через 4-5 годин повідомляла не сама компанія.

"Дуже потужна хакерська атака на віртуальну інфраструктуру компанії, частково зруйнована IT-інфраструктура. Ми ще зараз знаходимося в опрацюванні питання, скільки займе часу відновлення, тому жодних стейтментів ми ще не робили", - зауважив Комаров.

Він уточнив, що термін "пошкодження IT-інфраструктура" означає втрату доступу до систем компанії, тому що весь "периметр, яких захищається директорією, в якій прописані всі права - повністю зруйнований". Тому нині фахівцям доводиться працювати на фізичному рівні, "підключаючись умовно через патч-коди до кожного елементу мережі," щоб оцінити рівень її руйнування.

За його словами, сьогоднішня атаки є однієї і складових війни, в якій Україна перебуває вже майже два роки.

"Це війна, вона проходить не лише на полі бою, а і у кіберпросторі. Насправді це проникнення в інфраструктуру і її руйнування. Основна ціль цієї атаки - максимально можливе руйнування віртуальної IT-інфраструктури оператора", - підкреслив CEO "Київстару".

Товариство з обмеженою відповідальністю «МИ-УКРАЇНА»

Поштова адреса: 01135, Київ, вул. Дмитрівська (Шевченківський р-н), будинок 82, квартира 54

Телефон: +380 (44) 356-57-13

Адреса електронної пошти: we.ukraine.tv@gmail.com

Ідентифікатор медіа в Реєстрі суб'єктів у сфері медіа: L10-01783

Вранці 12 грудня мережа зв'язку Київстару стала мішенню потужної хакерської атаки, що стала причиною технічного збою, у результаті якого були тимчасово недоступні послуги зв`язку та доступу в інтернет. СБУ відкрила кримінальне провадження за фактом кібератаки на "Київстар". Одна із версій, яку наразі досліджують слідчі СБУ, – за цією хакерською атакою можуть стояти спецслужби РФ.

Monobank 12 грудня також зазнав масованої DDoS-атаки. Про це повідомив співзасновник фінустанови Олег Гороховський. Згодом він уточнив, що напад вдалося відбити і дані користувачів не скомпрометовані.

Президент «Київстару» пояснив, як хакерам вдалося зламати захист компанії

Олександр Комаров пояснив, що питання не в технологіях, а в тому, що в будь-якій організації можуть бути люди, які «умовно наводять російські ракети або віддають свої паролі, тому що добре працюють соціальні інженери». Про це повідомляє Upmp. news з посиланням на Польське радіо.

Хакерам вдалося уразити кіберзахист українського оператора мобільного зв’язку «Київстар» за допомогою скомпрометованого облікового запису одного зі співробітників.

Про це повідомляє Громадське телебачення з посиланням на президента компанії Олександра Комарова.

Він пояснив, що питання не в технологіях, а в тому, що в будь-якій організації можуть бути люди, які «умовно наводять російські ракети або віддають свої паролі, тому що добре працюють соціальні інженери».

«Потрібно визнати, що ця атака пробила наш захист. Це сталося, оскільки було скомпрометовано обліковий пул, скомпрометовано обліковий запис когось зі співробітників і ворог зміг потрапити в середину інфраструктури компанії. Про це ведеться слідство», — наголосив Комаров.

За його словами, компанія використовувала для захисту від кіберзагроз найсучасніші технології та з початку повномасштабного вторгнення рф відбила близько 500 кібератак.

«Робили вони це, щоб покласти найбільшу телекомінфраструктуру в країні, щоб посіяти неприємності, емоційно вразити українців… триває війна — це один зі способів війни проти України», — резюмував президент «Київстару».

Зазначимо, що російські хакери із так званої групи «Солнцепек», які відповідальні за злам мобільного оператора, висловили «подяку небайдужим співробітникам “Київстар”».

Під вечір 13 грудня в «Київстарі» почали включення голосового зв’язку по всій Україні. Відновлення послуг відбуватиметься поступово. Наразі спеціалісти компанії працюють над відновленням послуг передачі даних та SMS. Згодом компанія почне надання компенсацій абонентам.

hromadske.ua/О.Т.

2.2 Модель управління кібербезпекою об'єктів критичної інфраструктури

Кіберзлочинці концентрують свою увагу на об'єктах критичної інфраструктури, оскільки у разі успішної атаки можна отримати фінансову або політичну вигоду. Найбільшою вразливістю цієї ситуації є те, що системи використовують комерційні продукти і маючи певні технічні знання зловмисник може використати вразливості, які існують в цих продуктах, телекомунікаційні методи та загальні операційні системи.. Кібератаки на критичні сектори зазвичай

мають великий вплив на уряд і приватний сектор. Відстежити винуватців інциденту вкрай складно. З метою запобігти кіберінцидентам, найкращою відповіддю є **підвищення рівня кібербезпеки**. Важливо зазначити, що кіберзагрози особливо важко спрогнозувати, передбачити та вчасно вжити превентивних заходів, тому ризик того, що кібератаки будуть успішно реалізовані, зростає. Багато країн не розробили стратегії реагування на кібератаки та неочікувані сценарії і недооцінюють свої вразливості. Надзвичайно важливим та актуальним є розгляд аспектів кібербезпеки в контексті критичної інфраструктури з метою забезпечення захисту життєво важливих національних інтересів критичної інфраструктури.

Слід зазначити, що самі по собі технологічні рішення не вирішують всіх проблем кібербезпеки, а модель управління кібербезпекою об'єктів критичної інфраструктури має вдосконалюватися разом з оперативним реагуванням на кібератаки інфраструктури, повинна вдосконалюватися разом із швидким розвитком технологій, правових аспектів тощо. Атаки можуть бути описані п'ятьма основними групами, які розрізняються за цілями, які переслідує зловмисник системи:

- Спотворення інформації - коли дані в системі або каналі зв'язку зазнають неналежної модифікації.
- Відмова в обслуговуванні (DoS) - відмова в доступі до системи авторизованим користувачам.
- Розголошення інформації - коли критична інформація розкривається неавторизованим особам або системам.
- Крадіжка ресурсів - коли ресурси системи використовуються неавторизованими суб'єктами.
- **Фізичне руйнування - коли за допомогою використання КСЗІ досягається фізична шкода або руйнування**

Кіберсередовище буде змінюватися, а отже, зміняться і вектори атак на об'єкти критичної інфраструктури, а це означає, що власники та оператори будуть змушені боротися з новими загрозами. Безпека об'єктів критичної інфраструктури буде піддаватися все більшим викликам, оскільки технології, бізнес-практики і ринкові тенденції продовжують змінювати ландшафт безпеки. Зміни технологій значитимуть великі зміни у сфері управління системами та стійкості до вразливостей. Було визначено, що кібернетичні вразливості ПСУ беруть свій

початок в точці, де зв'язок є найбільшим, а контроль доступу - найслабшим. Можна виділити 4 області кібернетичних вразливостей (кожен домен має свої вектори атак, які використовуються кіберзлочинцями для досягнення своїх цілей):

- Домен IT.
- Домен ПСУ.
- Домен комунікацій.
- Фізичний домен.

На сьогоднішній день сферу ПСУ та IT неможливо відокремити один від одного. Фахівці зазначають, що сучасні інфраструктури, і особливо енергетична та телекомунікаційна інфраструктура, інтегрують компоненти ПСУ з компонентами IT, і найбільшим аргументом для цієї ситуації є технологічна еволюція і прогрес. Управління урядової звітності США ідентифікує групи кібер-зловмисників за цілями, які зловмисник намагається досягти своєю діяльністю:

- Оператори бот-мереж;
- Злочинні угруповання;
- Іноземні спецслужби;
- Хакери;
- Інсайдери;
- Фішери ;
- Спамери;
- Автори шпигунського/шкідливого програмного забезпечення;
- Терористи.

Всі ці групи націлені на об'єкти критичної інфраструктури або інші інформаційно-технологічні активи з різними цілями, але всі вони дійсно небезпечні. Кожен зловмисник, як правило, намагається використати вразливості системи і використовувати кілька векторів атаки, щоб отримати контроль над системою, яку він намагається пошкодити або експлуатувати. У більшості випадків зловмисники вивчають вразливості для того, щоб досягти своїх цілей. Кібератака часто розвивається в п'ять різних етапів: пошук вразливості системи, отримання контролю над системою або її частиною, впровадження шкідливого програмного забезпечення в систему, зараження інших компонентів системи та здійснення атаки на всю систему або на окрему її частину[63].

Прогалини в кібербезпеці створюють великі проблеми для кожного власника або оператора системи, але вони можуть не сприйматися як критичними, як прогалини в системах критичної інфраструктури, оскільки вплив атаки на них буде здебільшого невидимим. Атака на систему може мати різні наслідки. Деякі атаки на критичну інфраструктуру описані нижче. Хоча це найпоширеніші типи атак, ми повинні розуміти, що це не остаточний список, і зловмисники можуть переслідувати й інші цілі, атакуючи не лише об'єкти критичної інфраструктури:

- Окремі атаки на інфраструктуру мають на меті викликати паніку серед населення та порушити звичне життя. Прикладами таких атак є атака на світлофори в Лос-Анджелесі в 2006 році, атаки на Волгодонську АЕС в 2007 році.
- Шпигунські атаки на кшталт атак на енергетичні об'єкти США 2006-2013 рр.
- Напади, основною метою яких є знищення або порушення нормальної роботи системного обладнання. Наприклад австралійський витік каналізаційних стоків 2000 року, найвідоміша атака на АЕС - STUXNET 2010 та інші.

Сьогодні ми не можемо уявити собі магістраль енергопостачання чи іншу критичну інфраструктуру без контролю ПСУ середовища. Сфера управління критичною інфраструктурою сьогодні неможлива без сучасних технологій, які спрощують та зменшують операційні витрати, але в той же час ці технології сформували прогалини в безпеці та створили ворота для використання кібервразливостей. Технологічні компанії намагаються підвищити стійкість критично важливої енергетичної інфраструктури та усунути кіберзагрози шляхом створення централізованої моделі управління системою, яка захищає критичну інфраструктуру від кібервразливостей, але іноді нові технології просто відкривають нові можливості для зловмисників і вони будуть атакувати, якщо їм буде надано найменший шанс.

Важливим є те, що кіберзагрози дуже важко спрогнозувати, передбачити і вчасно вжити превентивних заходів, тому ризик того, що кібератаки будуть успішно реалізовані, зростає. Наразі не розроблена модель управління кібербезпекою, яка дозволяє реагувати на кібератаки, неочікувані сценарії та вразливості, тому життєво важливо вирішувати питання кібербезпеки в контексті критичної інфраструктури, з метою забезпечення базових інтересів держави. Слід зазначити, що самі по собі технологічні питання та рішення не вирішують всіх проблем, оскільки модель управління кібербезпекою об'єктів критичної

інфраструктури повинна постійно вдосконалюватися разом з технологіями, що швидко розвиваються.

Існують типові помилки, яких припускаються організації, коли думають про кібербезпеку своїх активів:

- Помилково вважати, що кожну інфраструктуру можна убезпечити від будь-якої вразливості. Кожна організація, яка експлуатує інфраструктуру, а особливо об'єкти критичної інфраструктури, повинна розуміти, що повна безпека - це лише мрія. Найважливішим аспектом безпеки є розуміння того, які є найбільш вразливі місця, які заходи необхідно проводити, щоб уникнути загроз, які механізми потрібні для виявлення аномальної інфраструктурної активності, а також мати чіткий план, який описує, як зменшити втрати та відновити нормальну діяльність вашої інфраструктури. Однак, фундаментальним аспектом, який повинен бути найбільш важливим для організації є виявлення та реагування на критичні ситуації. Це може значно зменшити втрати, пов'язані з порушеннями кібербезпеки .
- Хибна думка, що залучення найкращих професіоналів врятує вас від кіберзагрози. Кожна організація повинна розуміти, що кібербезпека - це не відділ, а підхід всієї організації. Кваліфікація кібербезпеки як одного з відділів та професійного об'єднання формує оманливе відчуття невразливості. Такий підхід є хибним. Кібербезпека має бути фундаментальним завданням і має стати ключовою метою кожного члена команди організації, адже людський фактор є найбільш вразливою частиною. Це означає, що, наприклад, кібербезпека має стати однією з політик організації, яка може впливати на прибутки.
- Хибне уявлення про технології безпеки та інструменти, які використовуються для забезпечення безпеки. Компанії, які виробляють технічні засоби та програмне забезпечення, ніколи не гарантують, що їхня продукція захистить вас від 100 відсотків кібератак. Технології та обладнання, що використовуються в сучасному світі для виконання певних функцій безпеки, таких як виявлення зловмисника тощо. Ці заходи та інструменти є дуже важливими і повинні використовуватися в технологічній інфраструктурі, але це

лише технології, і вони не можуть забезпечити вам повну кібербезпеку. Інструменти повинні бути певним продуктом, який з'являється після того, як розгорнуті хороші і сильні засоби кіберзахисту. Але продукти самі по собі не роблять IT-відділ, кожен несе відповідальність за кібербезпеку, і людський фактор залишається найслабшою ланкою по відношенню до безпеки. Інвестиції в інструменти мають сенс тільки тоді, коли люди усвідомлюють свою особисту відповідальність і прагнуть зберегти свої мережі в безпеці.

- Соціальна інженерія, яка все ще залишається одним з основних ризиків, з якими стикаються організації, що піклуються про власну безпеку. Технології можуть допомогти в цьому плані, але дуже важливо, щоб менеджери брали на себе відповідальність у вирішенні цієї проблеми. Організації повинні розуміти, що кожна людина в компанії повинна розвиватися в освіті і повинна розуміти загрозу кібератак.
- Хибною є думка, що кібербезпека - це лише ефективний моніторинг. Моніторинг у цьому контексті має більш широке значення, ніж просто моніторинг обладнання та об'єктів інфраструктури. Моніторинг - це не вузько технічний погляд, який пов'язаний з конкретними інформаційними ресурсами, інформаційними системами та мережевим моніторингом, а є широким поглядом, який поєднує в собі всю організацію навколишнього середовища та відстеження сучасних тенденцій кіберзлочинності. Моніторинг нічого не вартий, якщо ніхто не може на ньому вчитися. Якщо ви розумієте зовнішні зміни та тенденції у сфері кібербезпеки, ви зможете використовувати ці знання та розробляти відповідну політику і стратегії для досягнення успіху в боротьбі з кіберзлочинністю в довгостроковій перспективі. Політика та стратегія кібербезпеки повинні базуватися на безперервному навчанні та розвитку. Організації повинні розуміти, як загрози еволюціонують і розвиваються в майбутньому, і які є можливості підготуватися до майбутніх загроз. Такий підхід в кінцевому підсумку є більш економічно ефективним оскільки вони мають певні переваги перед короткостроковим підвищенням рівня безпеки шляхом побудови все більш високих і міцних стін. Кожна організація повинна забезпечити передачу

інформації про вразливість системи безпеки іншим організаціям, тому що тільки обмін інформацією про вразливість системи безпеки може забезпечити загальну картину реальної ситуації з безпекою в місті, державі або у світовому масштабі .

- Хибна думка про те, що заходи безпеки, які використовуються організацією для захисту від кіберзагроз є вищими. Безпека повинна спочатку бути визначена для досягнення своїх цілей. Зловмисники розробляють нові методи і прийоми, а захисники завжди на крок позаду. Здається, що корисно інвестувати у все більш досконалі заходи безпеки для запобігання атакам, але реальність дещо інша. Політика кібербезпеки повинна надавати пріоритет інвестиціям у критично важливу інфраструктуру та ресурси, а не в новітні технології або системи, здатні виявити будь-яку загрозу . Перш за все, потрібно розуміти, якого роду загарбники можуть цікавитися діяльністю організації і чому. Треба розуміти вартість їхніх активів, вміти оцінювати і брати на себе певний ризик, оскільки незмірні за вартістю технології, як вже було сказано, не забезпечують повної безпеки.

Головним аспектом кібербезпеки є те, що кібербезпека має бути нарізним каменем при розробці нових IT-рішень та систем, а не, як це часто буває, згадуватися лише наприкінці проекту, як це сталося з архітектурою Інтернету, яка була розроблена для сприяння зв'язку, а не безпеці.

Надалі надано модуль управління кібербезпекою, яку може бути використано для забезпечення безпеки будь-якої критичної інфраструктури, а також для підвищення рівня кібербезпеки будь-якої бізнес-компанії чи державної організації. В цілому модель представлена на рис. 2.4

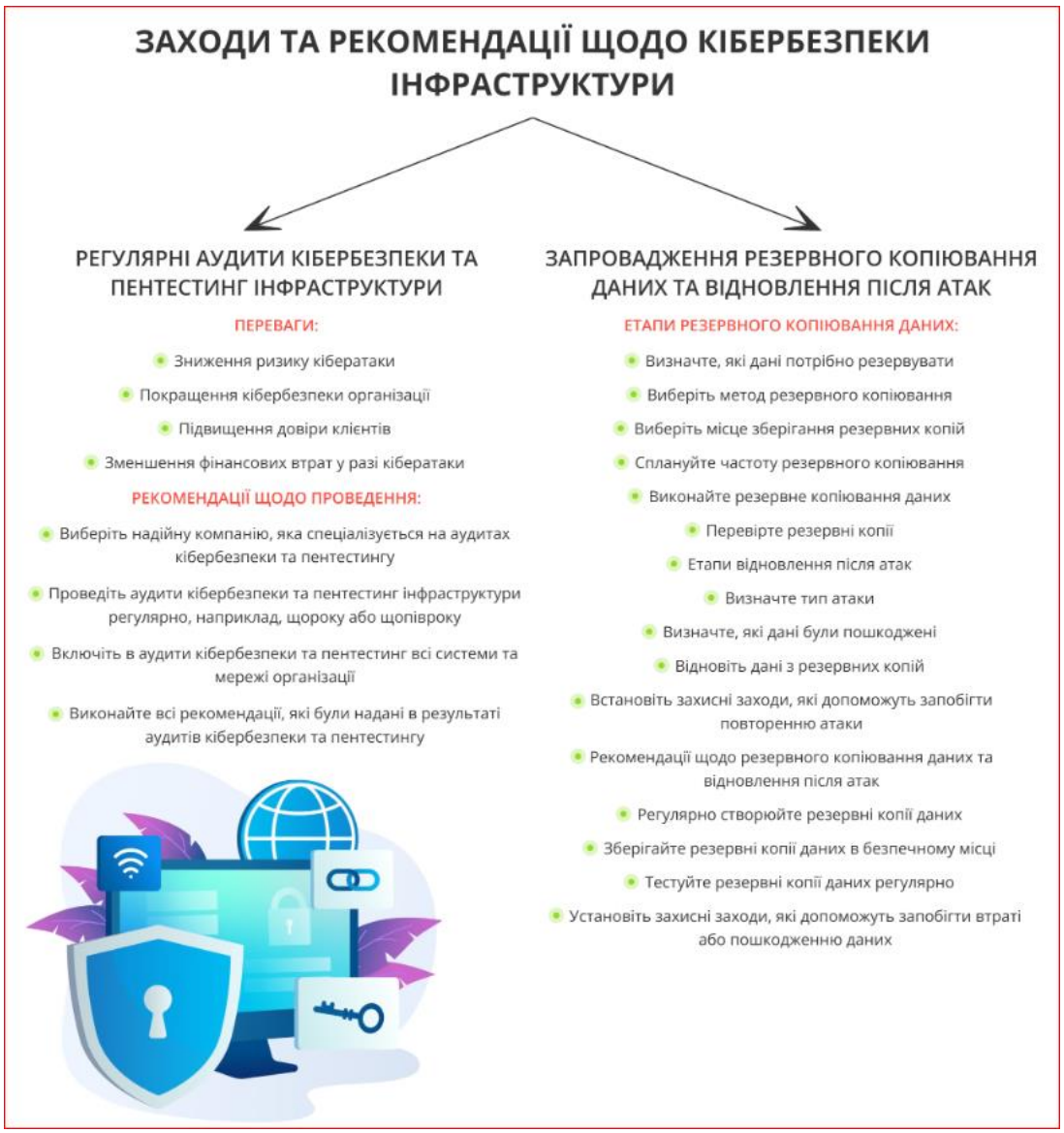

Рис. 2.4 Модель управління кібербезпекою

Представлена[64] модель побудована з багатьох напрямків та шістьма основними напрямами, які фахівці вважають найбільш важливими у процесі забезпечення кібернетичної безпеки. Всі ці елементи мають однакову важливість і потребують розвитку в рамках всієї організації в цілому, оскільки розвиток лише однієї частини моделі не призведе до значних великих змін у безпеці організації.

Як показано на попередньому рисунку, модель складається з шести основних розділів:

1. Правове регулювання. Ця частина моделі побудована з вимог та юридичних процедур та аспектів, які повинні бути досягнуті організацією, що думає про сучасну кібернетичну безпеку. Вона повинна містити цілісне бачення всіх законодавчих актів, які будуть використовуватися в організації в

повсякденному житті (інструкції з безпеки для співробітників, спеціалістів з інформаційної безпеки та мережевих адміністраторів, будь-які стандарти, які використовуються або плануються до використання в організації).

2. Ефективне управління. З точки зору досягнення кібербезпеки, це, можливо, найважливіша частина моделі управління кібербезпекою. Кожен сучасний організаційний лідер повинен розуміти основні цілі кібербезпеки в своїй організації та усвідомлювати, що ризики, які він несе, ніколи не будуть виключені з організаційного життя. Організація повинна розуміти, що не можливо зробити нічого, щоб уникнути всіх кіберризиків, але можна мінімізувати вплив кіберінцидентів на організацію, якщо вони трапляються. Кібербезпека повинна бути першим каменем на п'єдесталі будь-якого проекту. Будь-який проект або діяльність, який запланований в організації, повинен спочатку бути повністю переглянутий з точки зору безпеки. Тільки хороше розуміння того, що безпека, і особливо кібербезпека, є ключовим елементом будь-якого проекту, забезпечить успіх проектів організації та допоможе заощадити кошти та ресурси.

3. Управління ризиками. Це здатність організації належним чином ідентифікувати ризики, які зростають навколо організації, та забезпечення наявності у них спеціальних навичок для контролю за впливом цих ризиків. Як згадувалося раніше, організації не можуть уникнути всіх ризиків. Іноді важливіше визначити всі ризики та мати план на випадок надзвичайних ситуацій, ніж намагатися уникнути всіх ризиків. Насправді, організація повинна навчитися не тільки уникати ризиків, але й навчитися приймати їх. Іноді вміння ідентифікувати ризики та підготувати план дій на випадок непередбачуваних обставин зробить для організації більше, ніж намагання уникнути виявлених ризиків. Тільки після ретельного розгляду всіх ризиків можна відповісти на питання; що є більш ефективним, уникнення, використання чи контрзаходи?

4. Культура безпеки. Це має бути інтегровано в модель управління кібербезпекою. Цей вимір мабуть, найскладніший для впровадження та контролю. Можна використовувати інформатику, математику або технології управління ризиками, щоб спробувати розрахувати, що вигідніше для організації - купити нову систему безпеки або прийняти ризики крадіжок,. з персоналом набагато складніше, адже це люди. Цей аспект дуже важливий і організація повинна розуміти, що вона вразлива так само, як і люди, які в ній працюють. Безпека має бути зрозумілою для кожного члена організації, і кожен член повинен мати можливість навчитися захищати організацію та себе від кібернетичних інцидентів, оскільки помилки можуть мати вирішальне значення для безпеки організації. Одна з найбільших помилок у сфері кібербезпеки в цьому вимірі

зазвичай пов'язана з думкою вищого керівництва та IT-спеціалістів про те, що вони повинні мати більше привілеїв і доступу до своїх систем. Якщо ви дійсно потребуєте захисту і хочете мати менше проблем з кібербезпекою, потрібно розуміти, що всі заходи безпеки повинні бути доступними для всього персоналу; інакше ви програєте боротьбу з кіберзагрозами.

5. Управління технологіями. Як вже згадувалося раніше, кібербезпека - це не тільки технологічний підхід до організації, але вам потрібно буде використовувати його для досягнення ваших організаційних цілей організації. Спробуйте зрозуміти, що ваші знання про кожен компонент, який контролюється IT, може бути вразливим. Потрібно знати кожен компонент, який ви використовуєте для роботи вашої організації. Ці знання дозволять вам знати, чи є якісь компоненти, які є вразливими і можуть бути порушені. Управління технологіями та компонентами дозволить вам скоротити час, необхідний для усунення наслідків інциденту безпеки або запобігання виникненню інциденту безпеки.

6. Управління інцидентами. Цей вимір тісно пов'язаний з правовим виміром модуля. Ви повинні мати конкретні плани управління наслідками інцидентів. Ці плани повинні включати інструкції для членів організації, які будуть застосовуватися у випадку будь-якого інциденту, пов'язаного з безпекою. Необхідно визначити, які дії слід вжити, щоб спробувати зменшити вплив інциденту та як відновити нормальну роботу організації.

Кожна сфера (вимір) запропонованої моделі управління кібербезпекою має бути чітко визначена, виміряна та оцінена, а організація повинна розробити чіткий план щодо проблем, які виявлені в кожній сфері (вимірі) моделі управління кібербезпекою. Кожен вимір запропонованої моделі управління кібербезпекою можна розділити на 3 рівні: початковий рівень, середній рівень та рівень повної інтеграції.

Початковий рівень всіх вимірів пов'язаний зі здатністю організації чітко визначити, які проблеми можуть бути вирішені організацією під час впровадження моделі кібербезпеки:

- Правовий вимір скрадатиметься з глибокого аналізу правової бази всередині та поза межами організації та виявлення всіх прогалин у правових аспектах, що можуть вплинути на кібербезпеку політики організації;
- Вимір належного врядування включатиме аналіз системи врядування в організації, з можливістю визначити, який відділ або особа залучені до процесу

прийняття рішень. Навіть невелике розуміння процесу управління в організації та взаємодії процесу управління зі сферою кібербезпеки зробить організацію трохи сильнішою в питаннях кібербезпеки;

- Початковий рівень виміру управління ризиками об'єднує всі ризики, які мають будь-яку можливість з'явитися всередині або за межами організації і можуть вплинути на нормальну життєдіяльність організації;
- Вимір культури безпеки потребує чіткого розуміння організацією та її членами про всі заходи безпеки, які можуть бути використані всередині організації для посилення кібербезпеки;
- Вимір управління технологіями повинен включати чітке бачення всіх технологій, що використовуються в організації на щоденні робочі процеси. Тільки чітке бачення існуючих технологій, які використовуються в організаційному житті, може визначити, що може бути використано як вектори атаки на ці технології та які заходи можуть бути застосовані для запобігання або мінімізації атак;
- Початковий рівень виміру управління інцидентами в організації повинен містити організаційну здатність розуміти, що кожній організації може бути завдано шкоди через технологічні або соціальні аспекти і ця шкода може з'явитися в будь-який час з будь-якого сегменту інфраструктури (апаратного або програмного забезпечення) або персоналу. Управління інцидентами на цьому рівні може містити прості інструкції для організації, які можуть бути використані у випадку аномальної активності проти організації. Розуміння природи кіберінциденту є першим, а може і головним, кроком до підвищення рівня кібербезпеки в організації.

Помірний рівень кожного з шести вимірів моделі управління кібербезпекою включає чіткий план та видимість змін, які необхідно здійснити в організації:

- Необхідно чітко визначити правові аспекти, підготувати всі робочі інструкції та ознайомити з ними кожного члена організації;

- Вимір належного врядування повинен чітко визначати ланцюжок управління в організації з чіткими межами відповідальності для кожного підрозділу, який бере участь у житті організації;
- Вимір управління ризиками повинен визначити чіткий план уникнення або прийняття ризиків, які були визначені на початковому рівні моделі управління кібербезпекою, оскільки іноді кращим рішенням є прийняття деяких ризиків, ніж намагання їх уникнути (це коштує дорожче або забирає величезні ресурси);
- Вимір культури безпеки на помірному рівні повинен включати чіткий план управління персоналом та забезпечення чіткої ідентифікації навичок, яких повинен досягти кожен член організації (необхідно спланувати додаткове навчання для ваших спеціалістів з IT-безпеки та користувачів IT-систем оскільки лише кваліфікований IT-персонал не повинен бути гарантією вашої кібербезпеки);
- Управління технологіями повинно включати чітку та зрозумілу інформацію про програмне забезпечення та технології, які використовуються в організації, включаючи життєвий цикл використовуваного обладнання та програмного забезпечення, оскільки більшість порушень безпеки приховані всередині систем, які є застарілими, але все ще використовуються в робочому процесі організації (цей технологічний аудит необхідно проводити постійно, оскільки він дозволить вам фінансово спланувати, які оновлення потрібні для вашого існуючого обладнання);
- Вимір управління інцидентами на цьому рівні повинен містити детальні плани та інструкції щодо відновлення організації у разі виникнення будь-яких інцидентів кібербезпеки та порушення нормальної роботи організації. Кожен відділ організації або член організації повинен знати план аварійного відновлення на випадок успішної атаки на організацію в сфері кібербезпеки.

Організаціям необхідно проводити своєчасний аудит моделі управління кібербезпекою та своєчасно оновлювати всі плани. Організаціям необхідно пам'ятати, що світ змінюється під впливом комп'ютерних технологій, і цей процес змін все ще триває. Коли організації намагаються вижити в реальному світі, вони повинні адаптуватися до змін і грати за правилами сьогоднішніх технологій,

технологій, які з'являться в майбутньому. В іншому випадку сучасна організація буде боротися за виживання у взаємопов'язаному світі.

Найвищим рівнем моделі управління кібернетичною безпекою є рівень повної інтеграції (взаємосумісності). Він визначається повним взаємозв'язком усіх вимірів моделі управління. На цьому рівні організація функціонує як велика армія солдатів, що працюють над однією загальною місією, а кожен вимір моделі управління кібербезпекою є невід'ємною частиною моделі кібербезпеки, є невід'ємною частиною організації.

Інтеграція моделі управління кібербезпекою в організації є дуже складним процесом, який потребує суттєвого розуміння, і ці знання не можуть бути пов'язані з технологіями чи інформаційною безпекою. Найбільша проблема полягає в тому, щоб пов'язати технології та управління разом, тому що часто технічні та управлінські фахівці розмовляють різними мовами. Організація зміниться, коли члени почнуть розуміти кібербезпеку не як технологічну дисципліну, а як реальний управлінський виклик.

Модель надає певні переваги організаціям, які її впроваджують. Всі аспекти представленої моделі повинні перевірятися та своєчасно оновлюватися, і цей процес дасть організації кращого розуміння навколишнього світу кіберзлочинності та інформацію про тенденції в сфері кібербезпеки, що допоможе організації приймати правильні рішення та бути більш стійкою до кібератак. Це також надає можливість керівникам організації брати активну участь у прийнятті рішень та формуванні політики кібербезпеки, а також можливість належним чином оцінювати ризики, пов'язані з безпекою, та належним чином ідентифікувати такі ризики. Здатність навчитися управляти інцидентами та зменшувати наслідки успішної атаки допомагає всім членам організації розуміти загрози кібербезпеки, знаючи, які дії необхідно зробити для зменшення поточних симптомів атаки або які дії необхідно вжити, щоб уникнути вразливостей. Можливість покращити репутацію організації у зовнішньому середовищі, оскільки організація дійсно дбає про кібербезпеку, є більш привабливою для споживачів або ділових партнерів, включаючи здатність модерувати комунікацію всередині організації, що допомагає зробити організацію більш стійкою до атак. Технології і менеджмент повинні йти пліч-о-пліч для того, щоб забезпечити ефективну кібербезпеку об’єктів критичної інфраструктури.

3.3 Аналіз кібератак на критичну інфраструктуру з IoT технологіями

Більшість високорозвинених країн у світі мають інформаційні системи, інформаційно-телекомунікаційні мережі, автоматизовані системи управління суб'єктів критичної інформаційної інфраструктури, що надають важливі послуги, такі як електронний, мобільний зв'язок, енергетика, банківська справа і фінанси,

громадські послуги, транспорт і управління водними ресурсами, які мають бути надійно захищені від різних зовнішніх загроз. У зв'язку з поширеним використанням IoT(Internet of Things)-додатків, що дають змогу керувати через інтернет практично всім, одночасно виникають уразливості в системі безпеки. Інтернет Речі є значущою інновацією нашого часу, але вони також несуть серйозну загрозу кібербезпеки для критично важливих об'єктів інформаційних систем. Уразливість у системі безпеки ставить під загрозу безпеку всієї системи загалом і дає можливість зловмисникам для атаки.

Коли IoT-додатки використовуються в критичних об'єктах інфраструктури, деякі серйозні проблеми кібербезпеки виникають самі по собі . Якщо кібератака зловмисників спрямована на критичну інформаційну інфраструктуру, результат такої атаки може бути катастрофічним. Вимкнення зв’язку по всій країні, вимкнення живлення в лікарнях, зміна температури в системах охолодження на атомних реакторах, навмисно спотворене використання функцій у "розумних" автомобілях - усе це лише кілька з безлічі руйнівних сценаріїв. Почастішали випадки навмисного злому критичної інформаційної інфраструктури різних країн з метою крадіжки, шпигунства, залякування, руйнування, кібертероризму та ін., що слугує приводом до ескалації конфлікту, і ймовірності збройного протистояння[65]. Очевидно, що проблема кібербезпеки є однією з найактуальніших і найважливіших на сьогоднішній день. Кібератаки можуть знищити фізичні системи організації або держави, передати контроль над цими системами третій стороні, зробити їх непрацездатними або поставити під загрозу конфіденційність особистих даних людей.

Кібератаки на об'єкти критичної інформаційної інфраструктури Інтернет Речей (IoT) - це еволюція в міжмашинному зв'язку, унікальне з'єднання, що дає змогу обчислювальним пристроям передавати дані по всій мережі без участі хоча б однієї людини[66-69]. Тривожною ситуацією є зростаючий взаємозв'язок об'єктів критичної інформаційної інфраструктури за допомогою технологій Інтернету Речей і супутнє збільшення кількості організованих кібератак по всьому світу. Було встановлено, що багато кібератак Stuxnet, Havex, Black Energy 3 і Industroyer, вчинені за останні роки, були спрямовані на системи управління SCADA, що належать до різних суб'єктів критичної інформаційної інфраструктури. Очевидним є той факт, що шкідливе ПЗ, яке націлене на водні та газові станції, електростанції і транспортні системи, є справою рук професіоналів і було спеціально розроблено для здійснення подібних дій. Багато пристроїв, що працюють на базі Інтернету Речей, інтегровані в суб'єкти критичної інформаційної інфраструктури для досягнення максимально ефективної взаємодії і комунікації. За прогнозами до 2025 року кількість пристроїв, підключених до

інтернету, досягне 75 мільярдів, що може значно погіршити ситуацію і призвести до збільшення зростання кібератак, націлених на критичну інформаційну інфраструктуру , які розробляються з використанням рішень на основі Інтернет Речей і відповідно можуть бути схильні до кібератак[70-73].

Можна сказати, що пристрої, під'єднані до інтернету, перебувають у межах концепції Інтернет Речей, завдяки існуючій інфраструктурі мережі Інтернет. Таким чином, всі пристрої, що використовують технологію Інтернету Речей, можуть бути піддані практично будь-яким кібератакам. Уразливості в системі безпеки мережі Інтернет так само можуть порушити роботу програм на базі Інтернету Речей. Можна зробити висновок, що ця інноваційна технологія крім позитивних перспектив так само несе і нові загрози для кібербезпеки[74]. Суб'єкти критичної інформаційної інфраструктури набувають більш ефективнішу продуктивність і зв'язок за допомогою додатків на базі Інтернет Речей. Але це може призвести до виникнення вразливостей у системі безпеки і збільшення кількості кібератак на них.

Кібератаки можуть бути націлені на IoT-додатки і системи управління промисловими підприємствами, що взаємодіють з ними. Цей вид атаки може нести загрозу людському життю, майну і навколишньому середовищу. Найчастіше подібні кібератаки дуже складні і продумані, що істотно відрізняє їх від звичайних кібератак, тому що вони поєднують у собі кілька різних методів і технологій. Розглянемо найпоширеніші методи.

Впровадження шкідливого ПЗ у кіберпростір системи управління з метою завдання шкоди або виведення з ладу всієї системи[75]. Рекламне ПЗ, кейлоггери, мережеві хробаки, шпигунські програми, руткіти, програми-вимагачі, трояни або віруси є найбільш відомими шкідливими програмами. Програма-вимагач WannaCry є одним із найвідоміших прикладів шкідливого ПЗ. Це ПЗ використовується для того, щоб позбавити людей доступу до своїх файлів і важливих мережевих сервісів, поки, для повернення доступу, не буде виплачено певну суму грошей.

Фішинг - це запит на отримання конфіденційних даних користувача для ненадійного мережевого ресурсу. Зловмисник, власник подібного ресурсу, намагається переконати користувачів у безпеці та надійності свого, припустимо, сайту. Жертва подібного обману виконує певні дії, заздалегідь обрані зловмисником, наприклад, переходить за посиланням на шкідливий сайт або вводить свої конфіденційні дані. У цьому разі жертва передає свої особисті дані зловмиснику власноруч.

Цільовий фішинг - це більш поширена фішингова атака, особливо серед різних суб'єктів критичної інформаційної інфраструктури. Вкладені в електронний лист дані використовуються для того, щоб змусити потенційну жертву натиснути на посилання, тим самим активувавши шкідливе ПЗ.

Злом (Хакерство) - це процес отримання несанкціонованого доступу до системи. Найважливішим етапом цього процесу є отримання пароля для доступу в систему. Злом, як правило, здійснюється за допомогою різних методів, таких як брутфорс.

Атаки типу "Відмова в обслуговуванні" (англ. DoS - Denial of Service) спрямовані на переповнення мережі системи надлишковим трафіком і спам даними. Система зв'язку виявляється перевантаженою занадто великим числом зайвих запитів на підключення. Подібне перевантаження сильно уповільнює роботу системи або вводить її в неробочий стан. DDoS атаки, потенційно, можуть бути здійснені з будь-якого пристрою, підключеного до мережі Інтернет.

Впровадження в SQL код - це кібератака, мета якої вкрасти, змінити або видалити вміст бази даних. Подібний метод використовується для атаки систем, які безпосередньо управляються наявними в них даними[76]. Зловмисники активують оператори SQL-запитів для доступу до сервера бази даних.

Людина-по-середині (англ. Man-in-the-middle) - це різновид атаки, метою якої є прослуховування каналу зв'язку між пристроями. Оскільки передача даних здійснюється через пристрій зловмисника, то передача даних мережею може бути вкрадена і змінена зловмисником. Коли передача даних не має надійного алгоритму шифрування, атака може бути легко досягнута в IoT-додатках.

Цільова кібератака (також англ. advanced persistent threat - "розвинена стійка загроза") - це кібератака, під час якої зловмисники отримують доступ до мережі системи і залишаються непоміченими протягом деякого часу. Метою цієї атаки зазвичай є крадіжка даних. Цільова кібератака - це складний процес, що вимагає сучасних знань і засобів для реалізації, такі атаки, як правило, справа рук великих організацій або країн. Крім того, процес цільової кібератаки вимагає високий рівень скритності протягом усіх етапів реалізації.

Завдяки послугам і можливостям інтернет провайдерів, кількість мобільних і IoT-пристроїв зростатиме, разом із цим зростатиме і кількість вразливостей кібербезпеки в системах на базі Інтернету речей. Таким чином, системи забезпечення безпеки об'єктів критичних інформаційних інфраструктур будуть постійно випробовуватися зловмисниками до межі можливостей. Крім того, особисті та корпоративні дані можуть бути викрадені кіберзлочинцями з метою

отримання викупу, чому сприяє збільшення кількості пристроїв, підключених до мережі Інтернет.

Чергові кібератаки відбуваються щодня і запобігти кожній з них практично неможливо. Однак, початкові методи захисту мають велике значення з точки зору зменшення наслідків поточних і майбутніх атак. значення з точки зору зменшення наслідків поточних і майбутніх атак. Пом'якшення наслідків кібератак включає в себе як методи виявлення вторгнень, так і методи їх запобігання. Розглянемо деякі з методів пом'якшення наслідків кібератак об'єктів критичних інформаційних інфраструктур на базі Інтернет речей.

Контроль доступу: дуже важливо заздалегідь визначити, які ресурси, файли даних і компоненти можуть бути доступні користувачам і пристроям. Крім того, необхідно визначити області, до яких неуповноважені користувачі не повинні мати доступ. Використання заздалегідь встановлених правил доступу знижує ймовірність несанкціонованого доступу до мережі. Засоби контролю доступу, такі як дискреційні, обов'язкові і розподілені за ролями засоби контролю доступу можуть підвищити безпеку системи від потенційних загроз. Такі методи управління доступом як вибіркове управління доступом, мандатне управління доступом і правління доступом на основі ролей можуть значно підвищити ефективність системи забезпечення інформаційної безпеки. У віддалено керованих кіберфізичних системах, таких як розумні мережі електропостачання, контроль доступу дуже важливий для обмеження доступу користувачів і пристроїв у мережі.

Шифрування: найчастіше, метою атаки зловмисників є розкрадання даних із системи або перехоплення внутрішніх мережевих пакетів, однак використання надійних методів шифрування сильно знижує шанси проведення успішної атаки. Отже, коли додатки Інтернету Речей використовуються в критичних інфраструктурах, канал зв'язку між IoT-пристроями та системою управління має бути надійно зашифрований. Використання слабких методів шифрування може створити проблеми із забезпеченням інформаційної безпеки. Таким чином, **шифрування дуже важливе для захисту цілісності даних і конфіденційності в мережах зв'язку**.

Аутентифікація пристрою є основним етапом у процесі захищеної передачі даних. Цей етап відповідає за ідентифікацію пристроїв і узгодження завдань, які пристрої мають виконати в мережі. Аутентифікація гарантує, що "розумні" пристрої не виконають несанкціоновані команди. Авторизація та ідентифікація є невід'ємною частиною аутентифікації.

Регулярні віддалені оновлення системи безпеки: IoT-пристрої мають легко оновлюватися віддалено. Отже, оновлення системи безпеки пристроїв також повинні виконуватися легко і віддалено. Якщо пристрій не налаштований на регулярне отримання оновлень, то постійно оновлювати систему безпеки не представляється можливим. На жаль, більшість виробників наразі розробляють IoT-пристрої без урахування оновлення прошивки та системи безпеки. При цьому, через швидкий розвиток технологій, дуже важливо надавати регулярні оновлення для розв'язання проблем, з якими можуть зіткнутися операційні системи та програми через уразливості системи безпеки. Крім того, для розумної електромережі на базі Інтернет Речей, регулярне оновлення прошивки є більш розумним рішенням, ніж масова заміна застарілих елементів мережі.

Фізична безпека: дуже важливо забезпечити фізичну безпеку пристроїв у системі. Механізми захисту від несанкціонованого доступу мають бути інтегровані в елементи системи, щоб захистити їх від фізичного несанкціонованого доступу. Фізичний доступ сторонніх осіб до пристроїв може призвести до компрометації даних, що зберігаються в них. Збережені дані можуть бути пов'язані з ідентифікацією, обліковим записом або аутентифікацією. Тому пристрої повинні мати такі засоби захисту, як видалення або блокування даних, щоб захистити їх у разі захоплення пристрою зловмисниками. Крім того, слід пам'ятати, що фізична безпека диспетчерських кімнат і серверів має більш важливе значення, тому що фізична вразливість безпеки будь-якого пристрою створює загрозу для всієї мережі. Тому, запобіжні заходи мають бути вжиті на етапі створення системи забезпечення інформаційної безпеки.

Безпека середовищ на основі Інтернету Речей, таких як суб'єкти критичної інформаційної інфраструктури, є серйозною та актуальною проблемою. Мережі Інтернет Речей є однією з основних структур критичної інформаційної інфраструктури. Таким чином, будь-яка вразливість безпеки мереж Інтернет Речей може безпосередньо впливати на все середовище, в якому вони використовуються. Розробка надійних, зручних, інтегрованих і високопродуктивних гібридних систем є ефективним рішенням для виявлення різних типів кібератак.

Висновки до другого розділу

1.Обмеженість ресурсів вимагає визначення пріоритетів на основі економічної ефективності заходів безпеки, а не сліпого прийняття всеохоплюючого підходу. У більшості випадків потреба в безпеці має бути збалансована з продуктивністю, оскільки різні варіанти можуть бути громіздкими і заважати функціонуванню системи та організації. Більшість практик управління

кіберризиками для захисту інфраструктури можна розділити на три групи: структурні, процедурні та реагування. Основна складова ризику залежить від характеру організації та управління її персоналом і підрядниками.

2. Технологічні рішення не вирішують всіх проблем кібербезпеки, а модель управління кібербезпекою об'єктів критичної інфраструктури має вдосконалюватися разом з оперативним реагуванням на кібератаки інфраструктури, повинна вдосконалюватися разом із швидким розвитком технологій, правових аспектів. Кібератака часто розвивається в п'ять різних етапів: пошук вразливості системи, отримання контролю над системою або її частиною, впровадження шкідливого програмного забезпечення в систему, зараження інших компонентів системи та здійснення атаки на всю систему або на окрему її частину. Головним аспектом кібербезпеки є те, що кібербезпека має бути нарізним каменем при розробці нових IT-рішень та систем, а не, як це часто буває, згадуватися лише наприкінці проекту, як це сталося з архітектурою Інтернету, яка була розроблена для сприяння зв'язку, а не безпеці. Модель управління кібербезпекою складається з шести основних розділів: правове регулювання, ефективне управління, управління ризиками, культура безпеки, управління технологіями, управління інцидентами.

3.Безпека критичної інформаційної інфраструктури - стан захищеності критичної інформаційної інфраструктури, що забезпечує її стійке функціонування під час проведення щодо неї комп'ютерних атак. Суб'єкти критичної інформаційної інфраструктури схильні до кібератак з різних причин, в основному, через свою значущість. Також ясно, що фізичні або кібератаки ніколи не припиняться. Тому кожна країна повинна повсюдно застосовувати найдоступніші та найнадійніші заходи щодо забезпечення інформаційної безпеки для цих інфраструктур. Кібератаки на критично важливі інфраструктури можуть завдати серйозної шкоди. Кількість кібератак на підприємства зв’язку, ядерні об'єкти, енергосистеми, греблі та інші найважливіші об'єкти зростає з кожним днем. Зростаюча кількість підключених до інтернету смарт-пристроїв створює серйозні вразливості для безпеки мереж. Отже, якщо не буде вжито дуже важливих кроків для розв'язання проблем безпеки, то очевидно, що шкода, яку завдають кібератаки на суб'єкти критичної інформаційної інфраструктури, призведе до катастрофічних наслідків для держав і організацій. Додатки Інтернет Речей є найбільш важливими структурами з точки зору підвищення ефективності роботи та взаємодії суб'єктів критичної інформаційної інфраструктури. Однак усі атаки, які можуть статися в мережі Інтернет, можуть бути виконані і в середовищі Інтернет Речей. У роботі було представлено найпоширеніші методи, які використовуються при кібератаках на суб'єкти критичної інформаційної інфраструктури. Обговорено різні сучасні

способи пом'якшення наслідків кібератак з точки зору кібербезпеки. Особливо важливим аспектом кібербезпеки є використання відповідних методів ідентифікації, оскільки це допомагає заздалегідь вживати контрзаходів, а також дає змогу розробити прогнозуючу та попереджувальну стратегію кібербезпеки для суб'єктів критичної інформаційної інфраструктури з технологіями Інтернет Речей.

РОЗДІЛ 3

МЕХАНІЗМИ ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЗАРУБІЖНИЙ ДОСВІД КІБЕРЗАХИСТУ

3.1 Зарубіжний досвід організації захисту критичних інформаційних інфраструктур

Захист критичних інформаційних інфраструктур нині є одним із найбільш інтенсивно обговорюваних комплексів проблем інформаційної безпеки в усьому світі. Для розуміння заходів, що проводяться на державному і міждержавному рівні, представляє інтерес методологічний і практичний досвід різних країн щодо вирішення різних організаційно-технічних завдань у цьому напрямку. При цьому найбільший інтерес представляє досвід держав із **найрозвиненішою інформаційно-телекомунікаційною інфраструктурою**, яка використовується в управлінні державою, в економічній діяльності та для забезпечення суспільних процесів - це насамперед США і країни Європи. В останньому випадку необхідно враховувати, крім національних особливостей, політику Євросоюзу і НАТО в цій галузі.

У США з метою систематизації потенційно небезпечних об'єктів, знищення яких може мати значні **політичні та військові наслідки**, було запроваджено термін "критична інфраструктура". Під ним розуміється "сукупність фізичних або віртуальних систем і засобів, важливих для держави в такій мірі, що їх вихід з ладу або знищення можуть призвести до згубних наслідків у сфері оборони, економіки, охорони здоров'я та безпеки нації" (закон США "USA PATRIOT Act" від 2001 року, частина 1016 "Critical Infrastructures Protection")[77]. Розрізняють такі групи об'єктів критичної інфраструктури:

- власне інфраструктура, необхідна для вирішення завдань забезпечення національної безпеки;
- об'єкти, безпосередньо не задіяні при вирішенні завдань забезпечення національної безпеки, але необхідні для забезпечення функціонування інфраструктури вирішення цих завдань;
- об'єкти, необхідні для вирішення національних завдань, виведення з ладу яких матиме послаблювальний ефект для безпеки та економічного

добробуту або які можуть дати негативний ефект для національного престижу, моралі та довіри.

Перелік таких об'єктів включає системи забезпечення діяльності уряду, оборони, **підприємств зв'язку**, охорони здоров'я, кредитно-фінансового, банківського та науково-дослідного секторів, промисловості, енергетики, зокрема атомної, нафтогазового комплексу, забезпечення продовольством, транспорту, комунального господарства, включно з водопостачанням та цивільної оборони.

Аналізуючи сучасні підходи до організації забезпечення безпеки критичної інфраструктури у США, можна виокремити такі основні напрями державної політики в цій галузі:

- розроблення національного плану забезпечення безпеки критичної інфраструктури, що встановлює контрольні точки для аналізу вразливості та підготовки програм їх ліквідації в кожному секторі промисловості та економіки;
- організація тісної співпраці та взаємодії між державним і приватним секторами (бізнесом та інститутами громадянського суспільства);
- створення головних федеральних підрозділів, відповідальних за реалізацію завдань забезпечення безпеки елементів критичної інфраструктури в кожній галузі;
- здійснення спостереження за стратегічними змінами в кіберпросторі, виявлення тенденцій, підготовка відповідних доповідей і рекомендацій для державних органів;
- створення системи оповіщення (інформування) з актуальних питань інформаційної безпеки осіб, які ухвалюють рішення, представників бізнесу, широкої громадськості;
- надання підтримки силовим міністерствам у діяльності із забезпечення безпеки в аспекті інформаційної безпеки;
- створення системи виявлення та раннього реагування на кібератаки;
- впровадження в урядові мережі та критично важливі інфраструктури необхідних і достатніх захисних механізмів;
- здійснення діяльності з міжнародної взаємодії в галузі кібербезпеки.

Роботи в США із забезпечення безпеки в галузі захисту ключових об'єктів інфраструктури беруть початок із формування Президентської комісії із захисту критичної інфраструктури (President's Commissionfor Critical Infrastructure Protection) у 1996 році. Підсумки роботи комісії було покладено в основу урядової політики в галузі забезпечення інформаційної безпеки критичної інфраструктури, сформульованої в Директиві президента № 63, підписаній у травні 1998 року (PDD-63)[78]. На виконання вказівок президента, зазначених у цій директиві, було розроблено Національний план захисту інформаційних систем США, підписаний президентом 2000 року. План містить 10 програм, які умовно можна розділити на 2 частини: програми 1-5 "першочергові заходи" та їх підтримка та забезпечення (програми 6-10).

Першою у списку стоїть програма "Визначення критично важливих ресурсів інфраструктури, їхніх взаємозв'язків і загроз, що стоять перед ними". Основні етапи першої програми передбачають: попереднє вивчення критичних елементів інформаційної інфраструктури, вироблення рекомендацій, вжиття першочергових заходів, участь МО і створення необхідних організаційних структур з координації робіт, постійне відстеження перебігу робіт та їхнього впливу на обороноздатність.

Друга програма - "Виявлення нападів і несанкціонованих вторгнень" - спрямована на "створення багатоступеневої системи захисту для найважливіших комп'ютерних систем, включаючи сучасні технології мережевого сегментування та екранування, моніторів виявлення вторгнення, розпізнавання аномальної поведінки, глобальних систем управління тощо. Програмою передбачалося, що центри комп'ютерної безпеки, спочатку в Пентагоні (JTF-CND), а потім у масштабах усієї країни (NSIRC) отримуватимуть попередження від відповідних датчиків і систем, встановлених на найважливіших об'єктах національної інформаційної інфраструктури через створювану для цих цілей федеральну мережу виявлення вторгнення (FIDNet), що дає уявлення про системну роботу в цьому напрямку (рисунок 3.1).

Третя програма - "Розроблення розвідувального забезпечення та правових актів щодо захисту критичних інформаційних систем" - покликана збільшити роль розвідувального співтовариства і правоохоронної системи США в усуненні загроз і припиненні злочинів, спрямованих проти національних інформаційних мереж. У ФБР уже створено і діє так званий "Національний центр захисту інфраструктури" (NIPC), покликаний забезпечити раннє попередження про напад, використовуючи всі доступні джерела інформації. У центрі є представники Пентагону, АНБ, ЦРУ та інших федеральних відомств, які беруть участь в оперативних заходах з виявлення факту і локалізації джерела нападу, оцінки

масштабів збитків, пошуку злочинців. Передбачається, що надалі цією інформацією зможуть користуватися влада штатів і приватний сектор.

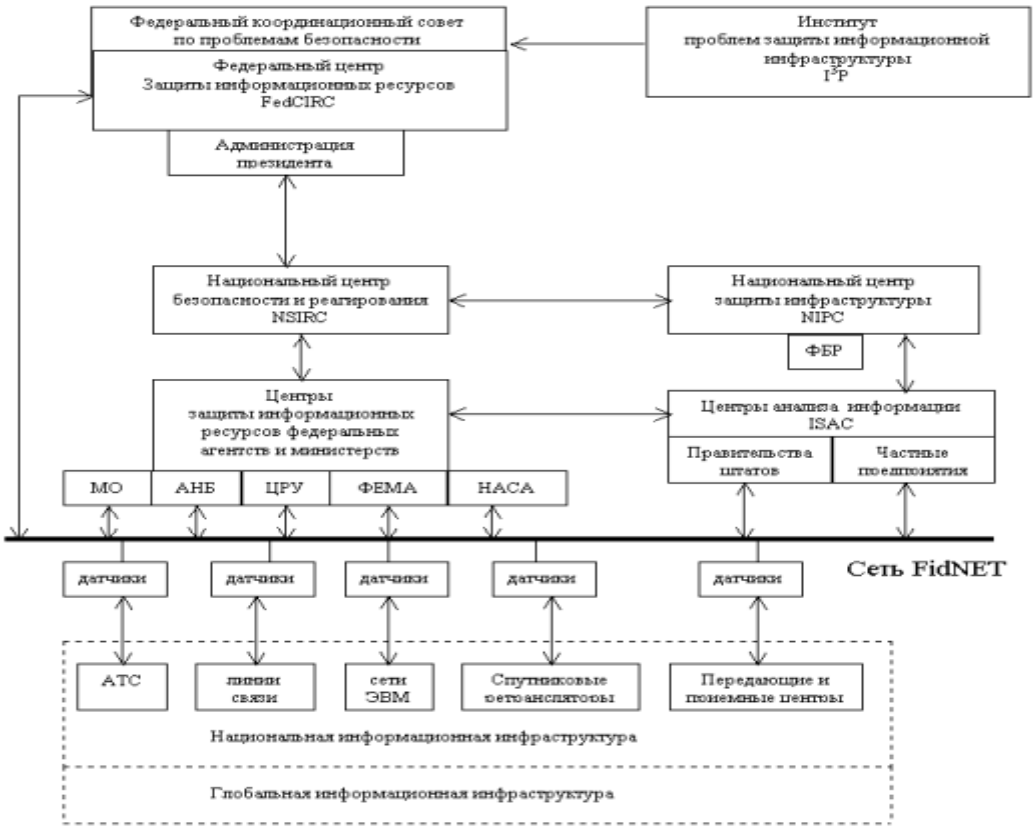

Рисунок 1. Структура FIDNet

Четверта програма - "Своєчасний обмін інформацією попередження про напад" -зачіпає один із найважливіших напрямів захисту інформаційних систем. Адміністратори федеральних інформаційних систем, накопичуючи інформацію щодо кожного окремого випадку аномалії або вторгнення, повинні своєчасно передавати її в головний Федеральний центр (FedCIRC), а в разі якщо дії підпадають під пряме порушення закону - в Національний центр захисту інфраструктури (NIPC) при ФБР, у якому зможуть визначити місце, звідки походить загроза та оперативно усунути її можливі негативні наслідки. Для приватного сектору та урядів штатів передбачено створення так званих центрів аналізу та обміну інформацією (Information Sharingand Analysis Centers - ISACs).

П'ята програма - "Створення можливостей з реагування, реконфігурації та відновлення" -націлена на обмеження масштабів шкоди інформаційній інфраструктурі вже безпосередньо під час вторгнення, на основі розроблення спеціальних корпоративних та індивідуальних планів дій. Після виявлення факту

нападу центри безпеки, обмінявшись інформацією, виробляють спільний план дій у відповідь, до переліку яких можуть входити: блокування доступу для підозрюваних, введення позаштатного режиму роботи, використання нових програмних "закладок", ізоляція елементів мережі, призупинення роботи фрагментів мережі, введення надзвичайних умов. Передбачається, що з часом на кожному об'єкті часом на кожному об'єкті буде розроблено відповідний план дій для ліквідації наслідків інформаційного вторгнення. Особлива роль у цьому напрямі відводиться федеральному агентству з дій у надзвичайних умовах (ФЕМА), модернізація системи зв'язку якого буде проведена в рамках цієї програми.

Програми 6-10 передбачають: "Активізацію НДДКР з підтримки програм 1-5", "Підготовку та розподіл необхідної кількості фахівців у галузі інформаційної безпеки", "Інформування американського суспільства про необхідність поліпшень в інформаційній безпеці", "Внесення змін і доповнень до законодавства в інтересах програм 1-8", "Забезпечення повної захисту громадянських свобод, особистих прав та особистих відомостей". Зазначимо, що попри всю важливість забезпечення безпеки інфраструктури, на першому плані стоїть захист громадянських прав і свобод, гарантованих конституцією. Будь-які дії урядових установ, пов'язані з пошуком інформації в особистих комп'ютерах та електронних повідомленнях, мають здійснюватися суворо відповідно до законодавства.

Крім цього, американська адміністрація ухвалила два директивні документи в інтересах внутрішньої безпеки - Національну стратегію кібернетичної безпеки (The National Strategy to Secure Cyberspace) і Національну стратегію фізичного захисту критичної інфраструктури (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets) і створила уповноважене Міністерство внутрішньої безпеки, яке на плановій основі реалізовує програми партнерства держави та бізнесу в частині безпеки КІІ.

Таким чином, було офіційно визнано залежність інфраструктури США від інформаційних систем і вразливість останніх. Нова стратегія безпеки націлена на створення так званої єдиної національної системи реагування на кібернетичні напади (National Cyberspace Security Response System). Основні завдання в галузі кібербезпеки полягають у тому, щоб "запобігти кібернетичним нападам на критичну інфраструктуру, знизити вразливість нації до таких нападів і мінімізувати збитки та час відновлення". Стратегія втілюється в життя за класичною схемою: навчання, попередження, оповіщення, ліквідація наслідків.

За американськими оцінками до 85% критичних інфраструктур у сфері інформаційних технологій належить приватному сектору. Частиною реалізації

плану партнерства з приватним сектором у сфері забезпечення захисту критичних інфраструктур у сфері інформаційних технологій є проведення щорічних національних навчань "Кібернетичний шторм" (Cyberstorm) із залученням понад 40 приватних компаній, що працюють у галузі інформаційних критичних інфраструктур. У навчаннях також відпрацьовувалася взаємодія з представниками Великої Британії, Австралії, Нової Зеландії та Канади.

У сфері забезпечення інформаційної безпеки в рамках державного і приватного партнерства діє низка центрів, організованих великими бізнес-структурами США в галузі фінансових послуг і телекомунікацій. Підприємства енергетичної галузі створили свій аналогічний Центр на базі Північноамериканської ради із забезпечення електрикою (North American Electricity ReliabilityCouncilNERC). А великі інформаційні компанії, такі як Cisco Systems, Microsoft, Intel, ComputerAssociates, Symantec, Computer Sciences Corporation, Oracle та інші виробники апаратного і програмного забезпечення, а також компанії, що працюють у сфері електронної комерції, також утворили Центр інформаційного обміну та аналізу.

Подібні Центри існують і в інших секторах критичних інфраструктур національного значення, включно з наземним транспортом, нафтовою та газовою галузями, водопостачанням, хімічною промисловістю, пожежні служби, харчова промисловість, охорона здоров'я.

У лютому 2013 р. президент США підписав указ №13636 "Посилення кібербезпеки критичних інфраструктур", у якому зобов'язав NIST розробити "базову модель захисту американських критичних інфраструктур". На виконання цього указу на основі наявних стандартів, керівних принципів і практик було створено й опубліковано першу версію документа "Framework for Improving Critical Infrastructure Cybersecurity//National Institute of Standards and Technology"[79] для зменшення кіберризиків для критично важливих об'єктів інфраструктури. У процесі роботи над цією моделлю NIST активно співпрацював з експертною спільнотою та комерційними компаніями.

Документ являє собою загальну мову для опису, розуміння та управління ризиками ІБ, як зовнішніми, так і внутрішніми. Він використовується для полегшення процесу ідентифікації та визначення пріоритету активностей з компенсації ризиків ІБ. За задумом творців застосовуватися він може найрізноманітнішими різними структурними одиницями, починаючи з відділів і закінчуючи організаціями і навіть асоціаціями.

Під критично важливою інфраструктурою мається на увазі сукупність систем і активів, настільки життєво важливих для держави, що знищення таких систем і активів матиме згубні наслідки для національної безпеки. КІІ включає в себе державних і приватних власників, операторів та інших суб'єктів, що мають відношення до КІІ. Усі залучені до діяльності об'єкта несуть колективну відповідальність.

Загальні правила підвищення рівня захищеності не відрізняються від традиційного. Загалом увесь документ ділиться на 3 основні частини: Ядро - Профілі - Рівні реалізації.

Ядро являє собою набір інформативних посилань з інформаційної безпеки, спільних для деякого набору критичних ресурсів. Функції систематизують базові активності ІБ на найвищому рівні абстракції (ідентифікація, захист, реагування, відновлення високому рівні абстракції (ідентифікація, захист, виявлення, реагування, відновлення).

Функції ядра, що дають змогу підтримувати захищеність на заданому рівні, співвіднесені із заходами забезпечення безпеки (наприклад: управління активами, управління доступом), які, у свою чергу, мають детальний зміст, що забезпечує подальший поділ на організаційно-технічний захист інформації. Завершують ієрархію понять покажчики на стандарти - інформативні посилання, що вказують на конкретні розділи керівництв, практик і стандартів, які ілюструють методи виконання конкретних активностей (NIST 800-82 і 800-53, ISA/IEC-62443, ISO 27001/02, Стандарти ENISA, Стандарт Катару, Стандарт API, Рекомендації ICS-CERT, COBIT, Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)). Реалізація такого підходу дає змогу застосовувати найкращі практики та принципи управління ризиками для організацій, незалежно від їхнього статусу чи розміру.

Профіль рівня захищеності, розглядається як набір стандартів, практик і прийомів ядра. Такі профілі можуть бути використані для порівняння рівнів захищеності та визначення необхідного рівня при зміні зовнішнього/внутрішнього середовища організації. Застосування профілів дає змогу створити дорожню карту для зниження ризиків і підвищення рівня ІБ, враховуючи організаційні особливості об'єкта КІІ, юридичні/законодавчі вимоги, галузеві стандарти. З огляду на розмір і складності управління, на об'єкті КІІ може бути кілька рівнів профілів відповідно до їхніх індивідуальних потреб. На верхньому рівні займаються управлінням ризиками, нижній рівень створює профілі захисту і все це об'єднується на рівні управління процесами.

Профілі є інструментом, що дає змогу визначити послідовність усунення ризиків ІБ відповідно до завдань усієї КІІ та окремих її структурних елементів, враховуючи вимоги законодавства, регуляторів і найкращих практик, а також відображаючи пріоритети процесу управління безпекою. Профілі можуть бути використані для опису як поточного, так і цільового статусу ІБ, що дає можливість виявити недоліки для їх подальшого усунення. Цільовий профіль створюється для відображення вимог ІБ, що висуваються до КІІ, і може використовуватися під час взаємодії різних об'єктів КІІ.

Рівні реалізації показують, як на об'єкті КІІ здійснюється управління безпекою. Рівні описують суворість і складність застосовуваних практик управління ІБ і якою мірою управління безпекою інтегровано в загальний процес управління КІІ. Документ визначає 4 рівні захищеності КВО, перший рівень - найслабший, четвертий, відповідно, найзахищеніший.

У 2017 р. на обговорення було винесено нову версію цієї моделі [80]. Того ж року, після указу, підписаного президентом США, використання "Керівництва із захисту від кіберзагроз" стало обов'язковим для всіх федеральних структур. Для бізнес-спільноти та неурядових організацій застосування Cybersecurity Framework має добровільний характер. Але, згідно з дослідженням Gartner, через два роки після публікації першої версії цього керівництва, 30% відсотків компаній заявили про те, що дотримуються його правил. Як очікується, до 2023 р. цей показник досягне 50%.

Країни Західної Європи були першими, хто почав займатися проблематикою ідентифікації та захисту критичної інфраструктури. У 1999 р. у Великій Британії було відкрито Координаційний центр з безпеки національної інфраструктури (National Infrastructure Security Coordination Centre). Його завдання полягало в розвитку та координуванні діяльності із захисту та оборони критичної національної інфраструктури, в рамках яких було ідентифіковано системи, що відіграють важливу роль у забезпеченні функціонування держави. Порушення або відмова таких систем могли б призвести до заподіяння шкоди рівню життя населення та до серйозних негативних господарських і соціальних наслідків. До цих систем належали постачання енергій і пального, постачання води, продуктів харчування, кормів, забезпечення транспорту, всіх громадських служб, включно з охороною здоров'я, комунікаціями, банківською справою тощо[81].

У 2002 р. Північноатлантичний альянс у рамках Євроатлантичної ради партнерства (ЕАРС), визначив, що "критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих і необхідних видів

діяльності економіки та державного управління". Сюди включено передусім телекомунікаційні, енергетичні, банківські, фінансові, банківські, фінансові, водогосподарські системи та аварійні служби, як державні, так і приватні. У 2003 р. з'явилася ініціатива "European industrial potential in the field of security research", яка поставила перед собою завдання розвитку досліджень з безпеки. Її діяльність була спрямована, головним чином, на галузі інформаційних технологій, біотехнології, хімії та біохімії, аналіз і менеджмент ризиків. Згодом з нею було пов'язане дослідження з безпеки "European Security Research Programme (ESRP)" під захистом ЄС. Дослідження було спрямоване на потреби безпеки країн ЄС. Було розпочато дослідження під назвою "Research for Secure Europe" (Дослідження для безпечної Європи), яке здійснилося в період з 2007 р. по 2009 р. У всіх випадках було видно прагнення об'єднати підхід до створення заходів на випадок військового конфлікту та інших надзвичайних ситуацій.

Паралельно з цими заходами відбувається підготовка та здійснення проєкту із захисту критичної інфраструктури під назвою "European Programme for Critical Infrastrukture Protection" (EPCIP). Дискусія щодо цієї програми розпочалася ще у 2004 р. на рівні Європейської Ради та Європейської Комісії, але незважаючи на це, національна критична інфраструктура здебільшого залишається під відповідальністю та в юрисдикції відповідної держави-члена Європейського Союзу. У жовтні 2004 р. з'явився перший концепт цілісної критичної інфраструктури та її захисту й оборони: "Захист критичної інфраструктури у протидії тероризму"[82] , у якому було запропоновано напрями щодо поліпшення попередження, підготовки та здатності реагування на європейському рівні на терористичні акти, спрямовані на критичну інфраструктуру. Метою цього документа є створення оптимального рівня готовності та превенції. Критична інфраструктура визначена як "обладнання, служби та інформаційні системи, життєво важливі для держави, знищення або відмова яких призведе до ослаблення національного суспільства, національного господарства, громадського здоров'я, безпеки та ефективної роботи державної системи".

17 листопада 2005 р. Комісія ухвалила "Зелену книгу про Європейську програму із захисту критичної інфраструктури[83]. Цей стратегічний документ охопив усі політичні та професійні галузі з метою включення великої кількості суб'єктів і отримання від них конкретної інформації про політики, придатні для підготовлюваної Європейської критичної інфраструктури. Документ виходить з факту, що дієвий захист критичної інфраструктури вимагає зв'язку, координування і співпраці як на національному, так і на європейському рівнях, між усіма зацікавленими суб'єктами - власниками та користувачами інфраструктур, органами регулювання, професійними організаціями та

галузевими об'єднаннями, також як і всіх рівнів державного та громадського управління та громадськості. Особлива увага приділяється тим випадкам, коли існує ризик виникнення багатоступеневого поширення подій, генерованих одна одною ("ефект доміно"). В остаточній версії обговорювався проєкт Європейської програми із захисту критичної інфраструктури та її впровадження в практику. У тексті визначено цілу низку питань, відповіді на які стали основою для остаточної директиви, що стосується захисту критичної інфраструктури в Європі. Також тут наведені широкі фахові дискусії, запропоновані визначення основних понять з галузі безпеки інфраструктури та можлива структура планів, які будуть розроблені для забезпечення безпеки КІІ.

У 2008 р. вийшла Директива Ради 2008/114/ЄС від 8 грудня 2008 р., про визначення та позначення європейської критичної інфраструктури та про оцінку необхідності посилення її захисту[84]. Зазначена Директива визначає первинну та остаточну відповідальність за захист критичної інфраструктури Європейського масштабу. З неї також випливає обов'язок усіх держав-членів ЄС внести проблематику захисту критичної інфраструктури до свого законодавства. Цей документ можна розглядати як правову основу для всієї цієї галузі, що розглядається. Тут же вперше подано список передбачуваних областей, у яких знаходиться європейська і національна критична інфраструктура.

Разом із програмою EPCIP було створено "Попереджувальну інформаційну мережу критичної інфраструктури" (CIWIN). Це захищена інформаційна, комунікаційна та попереджувальна система для обміну інформацією між державами-членами ЄС про система для обміну інформацією між державами-членами ЄС щодо загальних загроз, уразливості та відповідні заходи та стратегії зниження ризику. Участь країн ЄС у мережі добровільна. У кожній державі створено контактне місце та одне місце безпосередньо в Комісії ЄС. CIWIN має дві функції:

- Електронний форум для обміну інформацією, що стосується КІІ;
- Функція своєчасного попередження, яка допоможе державам-учасницям і Комісії оприлюднювати оповіщення про безпосередні ризики та загрози для критичної інфраструктури.

Основні (постійні) галузі, на які спрямована робота CIWIN - це хімічна промисловість, енергетика, фінанси, продукти харчування, здоров'я, інформаційні та комунікаційні технології (ІСТ), галузі атомного, паливного циклу, дослідницькі інститути, космос, транспорт і вода. Наразі CIWIN працює, але деякі портали ще не заповнені.

У Директиві Ради 2008/114/ЄС встановлено відмінність національної та європейської критичної інфраструктури. Національна критична інфраструктура включає "засоби, системи та їх частини, що знаходяться в державі-члені ЄС, які є принциповими для збереження найважливіших суспільних функцій, здоров'я, безпеки, забезпечення або доброго господарювання. суспільних функцій, здоров'я, безпеки, забезпечення або хороших господарських чи соціальних умов для населення, порушення або знищення умов для населення, порушення або знищення яких мало б для членської держави серйозні наслідки внаслідок відмови таких функцій". Оскільки відомо, що деякі елементи інфраструктури можуть мати велике значення не тільки на національному рівні, а й на міжнародному, то визначено також і європейську критичну інфраструктуру. Вона складається з "критичної інфраструктури, що знаходиться в членських державах, порушення або знищення якої б принесло серйозні наслідки, принаймні, двом державам. Серйозність наслідків розглядається відповідно до з "наскрізними" (транскордонними) критеріями. Це стосується і наслідків, спричинених міжгалузевою залежністю від інших типів інфраструктури". Причому в той час як у США критична інфраструктура та основні джерела розділені на 18 секторів, у рамках Європи застосовуються "рівні областей" (секторів) і "рівні продуктів і послуг" (елементів). Як правило, їхня загальна кількість у різних європейських державах, коливається від 8 до 10.

Проведений огляд заходів щодо захисту КІІ в різних країнах і міждержавних союзах дає змогу дозволяє зробити низку зауважень щодо узагальнення отриманого ними досвіду для розуміння того, що відбувається в цій сфері та можливих напрямках її розвитку в Україні.

По-перше, різними країнами підкреслюється їхня безумовна залежність сучасної інфраструктури від КІІ та важливість захисту КІІ для забезпечення обороноздатності.

По-друге, у результаті розуміння проблеми не тільки формулюється загальне поняття КІІ як "обладнання, служб та інформаційних систем, що є життєво важливими для держави, знищення або відмова яких призведе до ослаблення національного суспільства, національного господарства, громадського здоров'я, безпеки та ефективної роботи державної системи", а й визначаються основні складові: телекомунікаційні, енергетичні, банківські, фінансові, водогосподарські системи та аварійні служби.

По-третє, стратегія забезпечення безпеки КІІ має системний характер і втілюється в життя за класичною схемою: навчання, попередження, оповіщення, ліквідація наслідків.

По-четверте, будь-які дії урядових установ із забезпечення безпеки КІІ , пов'язані з пошуком інформації в особистих комп'ютерах та електронних повідомленнях, повинні здійснюватися в суворій відповідності до законодавства, що забезпечує захист "громадянських свобод, особистих прав і особистих відомостей".

Російсько-українська кібервійна — складова протистояння між Росією та Україною, яке в 2014 році переросло у відкрите збройне протистояння — російсько-українську війну.

Перші атаки на інформаційні системи приватних підприємств та державні установи України фіксували під час масових протестів в 2013 році.

Російсько-українська кібервійна стала першим конфліктом в кіберпросторі, коли була здійснена успішна атака на енергосистему з виведенням її з ладу. На думку Адміністрації Президента США хакерські атаки на Україну з боку Росії в червні 2017 року із використанням вірусу NotPetya стала найбільшою відомою хакерською атакою.

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначав, що разом з військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну. Кібервійною називають російські атаки і українські експерти.
Кіберзагрози Український державі та суспільству умовно можна розділити на два ключових рівні. Перший - «класичні» кіберзлочини - як абсолютно оригінальні, так і вже звичайні, для своєї реалізації вони потребують лише сучасних інформаційних технологій.

Другі - злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодіння коштами громадян, так і з метою кібершпигунства.

Першим масованим випадком хактивізму, з яким зіткнулася Україна, були події довкола закриття файлообмінного сервісу ex.ua. Після спроб правоохоронних органів втрутитися в роботу файлообмінного сервісу було здійснено DDoS-атаки на понад 10 інтернет-сайтів органів державної влади, зокрема на сайт Президента України та сайт Міністерства внутрішніх справ України. Події довкола ex.ua вперше наочно продемонстрували, наскільки Українська держава не готова ані ідеологічно, ані технічно до подібних атак. Саме відсутність прямих економічних збитків стала причиною того, що реальних висновків тих подій так і не було зроблено, а країна виявилась непідготовленою до ефективного протистояння агресії Російської Федерації в кібернетичній сфері.

Наступна хвиля хактивізму сталась на тлі політичного протистояння в жовтні 2013 року — лютому 2014 року (події Революції гідності). Це протистояння активно відбувалось в соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток. Наприклад, у Twitter, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Також були використані механізми ускладнення традиційних комунікацій, **зокрема мобільного зв'язку** (через автоматичні дзвінки на телефони окремих активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі).

Після початку збройної агресії Російської Федерації проти України, компанії, що спеціалізувалися на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай, кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на полі бою. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти.

З початком російсько-української війни стали з'являтись загони антиукраїнських хактивістів, які йменують себе «Кіберберкутом» та проукраїнська «Кіберсотня Майдану», «Анонімусами» з російською або українською «пропискою» тощо. Попри складності у визначенні ступеню співпраці хакерських угрупувань з державними органами, спираючись на зібрані докази можна стверджувати, що

проросійські хакерські угрупування перебувають на території Росії, і що їхня діяльність відбувається на користь кремлівського режиму.

Можна стверджувати, що з початку Російсько-Української війни в середовищі дослідників кібербезпеки поліпшились можливості виявлення, відстеження, та захисту від угрупувань російських хакерів. Серед можливих пояснень можна навести те, що із загостренням протистояння, російським хакерам бракує часу на вчасне оновлення та вдосконалення тактики, технологій, та методів діяльності.

Дослідники компанії FireEye виокремили два угрупування російських хакерів, які активно проявили себе в Російсько-Українській кібервійні: так звана APT29 (також відома як Cozy Bear, Cozy Duke) та APT28 (також відома як Sofacy Group, Tsar Team, Pawn Storm, Fancy Bear).

В період між 2013 та 2014 роками деякі інформаційні системи урядових установ України були вражені комп'ютерним вірусом, відомим як Snake/Uroborus/Turla. Даний різновид шкідливого програмного забезпечення надзвичайно складний, стійкий до контрзаходів, та ймовірно створений в 2005 році.

Починаючи з 2013 року розпочалась «операція Армагедон» - російська кампанія систематичного кібершпигунства за інформаційними системами урядових установ, правоохоронних та оборонних структур. Здобута в такий спосіб інформація ймовірно могла сприяти Росії й на полі бою. Істотним відхиленням від цього правила стала кібердиверсія - атака на «Прикарпаттяобленерго».

3.2. Технічне забезпечення роботи об’єктів критичної інфраструктури

Технічне забезпечення на об’єктах критичної інфраструктури включає технології, механізми та засоби, що дозволяють реалізувати заданий рівень інформаційної безпеки кожної конкретної мережі, інформаційної системи, ресурсу, автоматизованого робочого місця, компонентів інформаційної інфраструктури шляхом виконання комплексу організаційно-технічних заходів.

При виконанні заходів щодо забезпечення ІБ повинні бути реалізовані вимоги ІБ до інформаційно-технологічних процесів обробки інформації з урахуванням специфіки конкретних інформаційних комплексів, до технології створення і застосування систем захисту об'єктів ІБ, а також вимоги ІБ до механізмів і засобів захисту.

Технологічні процеси обробки інформації, які потребують захисту мають бути однозначно визначені в нормативно-методичних документах відповідного об’єкта критичної інфраструктури.

Результати технологічних операцій з обробки інформації, що захищаються технологічними процесами, повинні бути контрольованими і засвідченими уповноваженими особами. Особи, які здійснюють обробку критичної інформації і контроль (перевірку) результатів обробки, мають бути незалежними один від одного.

На підставі технічних вимог для реалізації мінімального набору вимог ІБ щодо захисту інформації в інформаційних системах на об’єктах критичної інфраструктури, що містять відомості конфіденційного характеру, служби інформаційної безпеки повинні забезпечувати:

- розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів обробки (передачі) і захисту інформації;
- надійне зберігання традиційних і машинних носіїв інформації, ключів (ключової документації) і їх обіг, що виключає їх розкрадання, підміну і знищення;
- необхідне резервування технічних засобів і дублювання масивів і носіїв інформації;
- використання сертифікованих засобів захисту інформації при обробці конфіденційної інформації;
- використання технічних засобів, які відповідають вимогам стандартів з електромагнітної сумісності;
- фізичний захист приміщень і власне технічних засобів інформаційної системи за допомогою сил охорони і технічних засобів, що запобігають або істотно ускладнюють проникнення в будівлі, приміщення сторонніх осіб, розкрадання документів і інформаційних носіїв;
- криптографічне перетворення інформації, що обробляється і передається засобами обчислювальної техніки і зв'язку;

• запобігання впровадженню в автоматизовані системи програм-вірусів, програмних закладок;

• використання волокно-оптичних ліній зв'язку для передачі інформації з обмеженим доступом [85].

Розглянуті вимоги складають необхідний кваліфікаційний мінімум вимог технічного забезпечення при формуванні базового рівня будь-якої інформаційної системи і ресурсу, що містять відкриту і конфіденційну інформацію.

Основними засобами технічного забезпечення роботи на об’єктах КІ є:

• Апаратні засоби

• Програмні засоби

• Криптографічні засоби

• Фізичні засоби

До апаратних засобів захисту інформації відносяться різні за типом пристрої (електронні, електромеханічні, механічні та інші). Основними завданнями апаратних засобів є виявлення та протидія спробам промислового шпигунства. До них можна віднести генератори шуму, радіосканери й інші пристрої, що дозволяють виявити або перекрити різні канали витоку інформації. Пристрої такого роду мають дуже вузький спектр завдань і є дорогими. Конкретними прикладами таких пристроїв є: пригнічувачі (глушилки) диктофонів, пристрої пошуку жучків, генератори шумів, аналізатори провідних ліній, пристрої виявлення прихованих відеокамер і стільникових телефонів.

Програмні засоби захисту інформації є найпоширенішими. Вони включають програми для контролю користувачів, шифрування, системи контролю захисту та інші. Програмні засоби найчастіше володіють такими характеристиками як: гнучкість, простота налаштування, висока чутливість при будь-яких змінах, надійність і відносно невисока вартість. Класифікація програмних засобів захисту інформації представлена на рисунку 3.2.

Рис 3.2. Класифікація програмних засобів захисту інформації

Засоби захисту із запитом інформації вимагають для своєї роботи введення додаткової інформації з метою ідентифікації повноважень користувача.

Засоби пасивного захисту спрямовані на застереження, контроль, пошук доказів з метою створення обстановки невідворотного розкриття злочину.

Засоби власного захисту - це елементи захисту, які властиві самому програмному забезпеченню.

Засоби активного захисту ініціюються при виникненні особливих обставин: введення хибного пароля, вказівці неправильної дати, спроби доступу до інформації без дозволу.

Засоби захисту в складі обчислювальної системи – це засоби захисту апаратури і штатних пристроїв.

До програмного захисту інформації входять:

1. Засоби захисту інформації, вбудовані в системне програмне забезпечення:

- засоби аутентифікації;
- засоби контролю і управління доступом;
- засоби адміністрування;
- засоби аудиту;
- засоби файлової системи.

2. Засоби захисту інформації, вбудовані в прикладне програмне забезпечення (додатки):

- засоби аутентифікації;

• засоби захисту від модифікації.

3. Засоби електронного цифрового підпису та мандатного керування доступом.

4. Антивірусне програмне забезпечення.

5. Програмне забезпечення для захисту від спаму.

6. Програмне забезпечення для захисту від шпигунських програм.

7. Програмне забезпечення для шифрування і кодування інформації.

8. Програми архівування інформації.

9. Програмні сканери безпеки.

10. Програмні міжмережеві екрани [86].

Служби інформаційної безпеки на об’єктах критичної інфраструктури широко використовують у своїй діяльності криптографічні засоби захисту інформації, які поєднують апаратні і програмні засоби реалізації криптографічних перетворень інформації. Мета криптографічних засобів захисту інформації - математичне перетворення повідомлень таким чином, щоб навіть після перехоплення не було можливості їх дешифрування і отримання змісту повідомлення.

Переваги технічних засобів криптографічного захисту:

• забезпечують найвищу ступінь захисту телефонних переговорів;

• захист відбувається на всьому протязі лінії зв'язку;

• можуть бути використані як в кабельних, так і бездротових системах зв'язку.

Недоліки технічних засобів криптографічного захисту:

• необхідність установки однотипного обладнання на всіх абонентських пунктах;

• втрата часу, необхідного для синхронізації апаратури і обміну ключами на початку сеансу захищеного з'єднання.

Фізичні засоби захисту інформації, з якими працюють фахівці з ІБ, - це різні конструкції, пристрої, апарати, призначені для ускладнення дій зловмисника на шляху до носія конфіденційної інформації.

Інженерно-технічне забезпечення - сукупність засобів інженерно-технічного захисту територій і приміщень підприємства і засобів виявлення загроз та захисту інформації, організована спрямованість застосування яких полягає у створенні системи охорони та захисту інформації на об'єктах і в елементах інформаційної системи від погроз її розкрадання, модифікації або знищення.

Підсистема інженерно-технічного захисту територій і приміщень - це сукупність інженерно-технічних засобів фізичної системи захисту, що містить в своєму складі засоби, що перешкоджають фізичному проникненню (доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації, а також здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних дій.

Підсистема виявлення і захисту технічних каналів витоку інформації - це сукупність засобів, застосування яких забезпечує виявлення технічних каналів витоку інформації, захист інформації від витоків з технічних і матеріально-речових каналів, а також засоби захисту комп'ютерної інформації при несанкціонованому доступі до неї [87].

Важливим елементом технічного забезпечення діяльності фахівців з ІБ є система управління доступом - це програмно-апаратний комплекс, що включає в себе контролери СКУД (Система контролю управління доступом), керовані замки, зчитувачі, метало-детектори, перешкоди у вигляді дверей, воріт, турнікетів і шлюзових кабін, а також комп'ютери та програмне забезпечення верхнього рівня, що полегшує налаштування, моніторинг та оперативне управління правами доступу персоналу.

До основних засобів СКУД відносяться:

- контролер - електронний прилад (спеціалізований комп'ютер), в якому зберігається інформація про конфігурацію, режими роботи системи, перелік осіб, які мають право доступу на об'єкт, а також рівень їх повноважень;
- зчитувач - пристрій, що підключається до контролера і дозволяє витягувати з нього інформацію особистого ідентифікатора, як із «пропуску» користувача;

• перешкода, що одночасно є засобом пропуску персоналу або транспорту: двері, турнікет, шлюзова кабіна, шлагбаум;

• виконавчий механізм для підтримки перепони в закритому стані (нормальний стан - доступ заборонений): замок для дверей, що замикає пристрій турнікета, шлюзової кабіни, шлагбаума;

• засоби управління пристроєм запирання з модулем ідентифікації-контролер зі зчитувачем;

• ідентифікатори: електронні перепустки, картки.

Основні засоби системи відеоконтролю включають:

• передавальні телевізійні камери (відеокамери);

• пристрої відображення відеоінформації - монітори;

• пристрої обробки відеоінформації (комутатори, квадратори, мультиплексори);

• пристрої реєстрації інформації (відеопринтери, побутові та спеціальні відеомагнітофони);

• кабелі, що забезпечують електричний зв'язок елементів системи відеоспостереження.

Засобами, які використовуються для пошуку каналів витоку інформації за рахунок побічного електромагнітного випромінювання і наведень, можуть бути:

• селективні мікровольтметри;

• аналізатори спектру;

• спеціальні вимірювальні комплекси для проведення вимірювань рівнів електромагнітного випромінювання;

• виявлячі диктофонів.

Засоби виявлення радіовипромінювань закладних пристроїв:

• детекторні індикатори електромагнітного випромінювання;

• інтерсептори;

• побутові радіоприймачі;

• скануючі приймачі;

- спеціальні високошвидкісні пошукові приймачі;
- найпростіші типові пошукові програмно-апаратні комплекси;
- спеціалізовані пошукові програмно-апаратні комплекси.

Засоби виявлення невипромінюючих закладних пристроїв:

- спеціальні виявлячі пустот (тепловізори);
- нелінійні локатори;
- металодетектори;
- рентгенівські установки;
- пристрої контролю напруги ліній;
- пристрої аналізу несиметрії ліній;
- пристрої аналізу нелінійності параметрів ліній;
- пристрої аналізу неоднорідності телефонних ліній (кабельні радари).

Загроза кібератак на будь-якому рівні викликає занепокоєння, так само як і фізичні акти крадіжки та вандалізму в системах SCADA. Однак наслідки кібератак для критичних інфраструктур і командно-керованих систем SCADA можуть виявитися особливо руйнівними.

SCADA (Supervisory Control And Data Acquisition) - диспетчерське управління і збір даних[89]. SCADA це система автоматизації технологічних процесів, яка використовується для збору інформації від датчиків і віддалених вимірювальних приладів, передачі даних в операторську, їх відображення для контролю та управління. SCADA, як правило, система логічно або фізично ізольована, від інших мереж у системі критичної інфраструктури.

Системи SCADA можуть піддаватися таким фізичним загрозам, як виведення з ладу одного або декількох модулів, також і кіберзагрозам у вигляді атак дистанційно або зсередини. В обох випадках це може призвести до таких небажаних наслідків:

- Втрата життя
- Фінансова шкода
- Крадіжка/втрата інформації
- Збої та зупинка роботи об'єкта загалом
- Фізичне руйнування

- Відмова/обвал периферійної техніки
- Відмова/обвал Центру управління SCADA

Експерти, що спеціалізуються на індустріальних, стратегічних SCADA системах, проводять послідовні перевірки відповідно до кожного з наступних етапів експертизи:

- Аналіз і опис всіляких ризиків для Системи Безпеки.
- Аналіз системного захисту від проникнення.
- Інспекція внутрішніх протоколів.
- Аналіз топології системи і програмного забезпечення та рекомендації щодо оптимізації.
- Опція динамічного безпечного розширення системи, її аутентифікація та авторизація.
- Оцінка взятих до уваги ризиків.
- Аналіз Архітектури Системної Безпеки "АСБ"
- Аналіз наявного парольного захисту та рекомендації
- Аналіз вимог і можливостей "АСБ" відповідати цим вимогам.
- Тестування системи на вразливість через авторизований доступ до ресурсів.
- Виявлення вразливостей без жодної шкоди чи небезпеки для тестованих критичних систем, що тестуються.
- Рішення та рекомендації для зміцнення захисту.
- Рекомендація перевірених технічних рішень.
- Рекомендації в інтеграції нових технологій з існуючими модулями в системі.

Багаторічний досвід фахівців і новітні технології в галузі SCADA підказують, що єдино правильною стратегією кібербезпеки є паралельне рішення у двох площинах:

- Зовнішній захист, що виключає ймовірність дистанційних атак і виведення SCADA системи з ладу.

- Внутрішні захищені стільники, що забезпечують нормальне і незалежне функціонування кожного елемента АСУ при постійному зв'язку з іншими модулями системи SCADA.

Вирішення обох завдань можливе тільки за умови інтеграції міжмережевого розділового екрану, заснованого на принципі світлодіода, що дозволяє передачу інформації тільки за принципом "Зсередини назовні" і використання захисного модуля, що забезпечує Deep Inspection (Глибока Інспекція) всіх стандартних протоколів зв'язку SCADA системи.

Сервери SCADA часто контролюють чутливе обладнання і важливі державні інфраструктури, такі як атомні та інші електростанції, гідроелектричні дамби та міжнародні нафто- і газопроводи. Природно, це обладнання являє собою надзвичайно привабливу ціль для проведення операцій, пов'язаних з кібертероризмом.

Фізичний захист систем SCADA це сенсорні Блоки "СБ" - прокладаються вздовж трубопроводу, або безпосередній близькості SCADA модулів, автономних стратегічних об'єктів. "СБ" встановлюються на відстані приблизно 200м одна від одної (залежно від типу ґрунту) та умов навколишнього середовища (у міських умовах відстань скорочується до 100м). "СБ" закопуються вздовж лінії на глибині 30-80см зони до 10м у сторони від об'єкта, що охороняється. Технічні характеристики та опис системних блоків:

- Кожен "СБ" має свій ідентифікаційний номер, який визначає секцію, до якої він належить, і точні координати його залягання. Кожен "СБ" містить усі елементи, необхідні для функціонування і виробництва повного аналізу сейсмосигналу:
- Контейнер - герметичний і повністю корозійностійкий до важких умов навколишнього середовища.
- Цифровий Аналізатор Сигналу (DSP) - процесорний блок.
- 4-8 аналогових входів (входи для геофонів).
- Комунікаційний блок коротко-діапазонного радіозв'язку під час конфігурації системи з використанням бездротового зв'язку, або оптичну муфту і карту оптоволоконного зв'язку в разі дротової конфігурації.

- Акумуляторний блок з терміном роботи до 5 років у бездротовій конфігурації, або 20 років у дротовій конфігурації. Батареї забезпечують потреби електроживлення як процесорного, так і комунікаційного блоку.
- 4 геофони з'єднані з контейнером захищеними броньованими кабелями.
- У бездротовій конфігурації антена 20-30см заввишки, що розміщується в районі залягання СБ.

Оновлення програмного забезпечення проводиться з контрольного центру системою зв'язку за адресним принципом (для окремого блоку, для секції або для всього ланцюжка блоків). За розпорядженням оператора, системний блок може передати до центру вміст своєї флеш-пам'яті, головним чином з метою технічного обстеження або аналізу нових або незвичайних шумів.

3.3 Розробка рекомендацій для захисту об’єктів критичної інфраструктури від кібератак.

Заходи щодо забезпечення ІБ на об’єктах критичної інфраструктури можна розділити на три ключові види: технічні засоби, організаційні заходи та профілактичні перевірки рівня захищеності.

Організаційні заходи:

Підвищення обізнаності. Регулярні внутрішньо-корпоративні вебінари та навчання основам ІБ життєво необхідні для кожної компанії, а особливо для об’єктів критичної інфраструктури. Це дає змогу підвищити обізнаність співробітників і переконатися, що вони володіють навичками, необхідними для виявлення і протидії атакам.

Розмежування прав і ролей співробітників. Повний доступ кожного співробітника до всіх даних компанії має свої ризики - витік клієнтських баз, інсайдерська торгівля і розкриття інформації про інноваційну діяльність. Компаніям необхідно чітко розмежовувати права доступу користувачів до корпоративних систем, файлів і обладнання.

Профілактичні перевірки рівня захищеності:

Аудит інформаційної безпеки IT-інфраструктури - це незалежне оцінювання рівня захищеності компанії на відповідність визнаним практикам у сфері забезпечення ІБ, а також законодавчим вимогам та міжнародних стандартів.

До аудиту входять оцінювання ефективності та надійності наявних методів захисту, аналіз слабких місць і вразливостей, а також оцінювання їхньої критичності та розроблення рекомендацій щодо їхнього усунення. Аудит ІБ - найважливіший захід при розробці концепції захисту ІТ-ландшафту. Однак по-справжньому він ефективний тільки в тому разі, якщо здійснюється з певною періодичністю, а не як разова ініціатива.

PenTest. Це імітація реальної атаки із застосуванням технік і методів, які використовують зловмисники з метою виявлення вразливих точок в ІТ-інфраструктурі компанії. Проведення PenTest дає змогу отримати реальну оцінку і повноцінну картину рівня захищеності інфраструктури та всіх інформаційних систем, а також сформувати список дій і заходів, необхідних для підвищення рівня безпеки.

Аналіз ризиків. Рекомендується щорічно переглядати актуальні ризики ІБ, визначати актуальні вразливості інформаційних систем і відповідні їм загрози для кожного критичного інформаційного активу організації. Після перегляду ризиків вносять корективи у фінансування заходів ІБ, зокрема виділяють додаткові кошти на придбання або оновлення засобів захисту інформації та надання послуг з ІБ.

Обробка інцидентів. Для того, щоб зменшити ймовірність і кількість порушень у сфері інформаційної безпеки фахівці з ІБ на об’єктах критичної інфраструктури мають розробити регламент управління інцидентами і діяти відповідно до нього, зокрема впроваджувати заходи із запобігання, пом’якшення наслідків або уникнення деструктивних подій інформаційної безпеки.

Технічні засоби:

Контроль змінних носіїв. Зовнішні носії - це спосіб, який дозволяє занести шкідливий код в корпоративну мережу, а також відмінний канал витоку конфіденційних даних. Для контролю рекомендується використовувати спеціалізовані засоби.

WAF-комплекс. Це міжмережевий екран для веб-застосунків, основними функціями якого є виявлення і блокування атак. За допомогою WAF-комплексу можна не тільки виявляти шкідливий трафік, а й також визначати, які атаки були спрямовані на бізнес-критичні системи. Впровадження цього інструменту дає змогу критично важливим об’єктам захиститися від атак .

Міжмережеві екрани (FW). Міжмережеві екрани є цифровим захисним бар'єром навколо ІТ-інфраструктури, який захищає мережу і запобігає несанкціонованому доступу. Міжмережеві екрани забезпечують безпеку мережі шляхом фільтрації вхідного та вихідного мережевого трафіку на основі набору

правил. Загалом, завдання міжмережевих екранів полягає в тому, щоб зменшити або унеможливити виникнення небажаних мережевих під'єднань, даючи водночас змогу вільно протікати всім законним комунікаціям.

Антивірус. Антивірус - це програма, яка виявляє зараження і виконує дії з його усунення: лікує або видаляє заражені файли. Антивірусне ПЗ працює і як профілактичний засіб: воно не тільки бореться, а й запобігає зараженню комп'ютера в майбутньому. Антивірусне програмне забезпечення дає змогу захиститися від шпигунського ПЗ, шкідливих програм, фішингових атак, спам-атак та інших кіберзагроз.

DLP - це набір інструментів і процесів, які застосовуються для запобігання втрати та нелегітимного використання конфіденційних даних. DLP-система відстежує весь трафік у захищеній корпоративній мережі та дає змогу виявляти порушення політик, несанкціонований доступ до даних з боку неавторизованих користувачів і блокувати спроби несанкціонованого передавання критично важливих даних.

Поштовий захист. Основна лінія захисту корпоративної пошти - це безпечний шлюз. Він фільтрує шкідливі повідомлення і відправляє їх у карантин. Безпечний шлюз електронної пошти може блокувати до 99,99% спаму, виявляти і видаляти листи, що містять шкідливі посилання або вкладення.

SIEM-системи. Такі системи збирають і об'єднують дані з усієї IT-інфраструктури: від хост-систем і застосунків до пристроїв безпеки. Після відбувається класифікація та аналіз інцидентів і подій. SIEM-системи на основі правил кореляції одержуваних подій виявляють потенційні інциденти ІБ і повідомляють про це адміністратора безпеки.

Висновки до третього розділу

1.Проведений огляд заходів щодо захисту КІІ в різних країнах і міждержавних союзах дає змогу зробити низку зауважень щодо узагальнення отриманого ними досвіду для розуміння діяльності, яка відбувається в цій сфері, і можливих напрямів її розвитку в Україні. По-перше, різні країни підкреслюють їхню безумовну залежність сучасної інфраструктури від КІІ і важливість захисту КІІ для забезпечення обороноздатності. По-друге, в результаті розуміння проблеми не тільки формулюється загальне поняття КІІ як "обладнання, служб та інформаційних систем, життєво важливі для держави, знищення або відмова яких призведе до ослаблення національного суспільства, національного господарства, громадського здоров'я, безпеки та ефективної роботи державної системи", а й визначаються основні складові: телекомунікаційні, енергетичні, банківські,

фінансові, водогосподарські системи та аварійні служби. По-третє, стратегія забезпечення безпеки КІІ має системний характер і втілюється в життя за класичною схемою: навчання, попередження, оповіщення, ліквідація наслідків. По-четверте, будь-які дії урядових установ із забезпечення безпеки КІІ, пов'язані з пошуком інформації в особистих комп'ютерах та електронних повідомленнях, мають здійснюватися в суворій відповідності до законодавства, що забезпечує захист "громадянських свобод, особистих прав та особистих відомостей".

2. Технічне забезпечення на об’єктах критичної інфраструктури включає технології, механізми та засоби, що дозволяють реалізувати заданий рівень інформаційної безпеки кожної конкретної мережі, інформаційної системи, ресурсу, автоматизованого робочого місця, компонентів інформаційної інфраструктури шляхом виконання комплексу організаційно-технічних заходів. Основними засобами технічного забезпечення роботи на об’єктах КІ є:апаратні засоби, програмні засоби, криптографічні засоби, фізичні засоби. Служби інформаційної безпеки на об’єктах критичної інфраструктури широко використовують у своїй діяльності криптографічні засоби захисту інформації, які поєднують апаратні і програмні засоби реалізації криптографічних перетворень інформації.

3. Заходи щодо забезпечення ІБ на об’єктах критичної інфраструктури можна розділити на три ключові види: технічні засоби, організаційні заходи та профілактичні перевірки рівня захищеності. До яких входять : підвищення обізнаності персоналу, розмежування прав та ролей співробітників, аудит ІБ, PenTest, аналіз ризиків, обробка інцидентів, контроль змінних носіїв та багато технічних засобів.

ВИСНОВКИ

У кваліфікаційній роботі досліджено питання системи захисту інформації критичних інфраструктур, проблеми нашої та інших країн. Ця тема грає велику роль у концепції сталого розвитку підприємства. Розробка, впровадження та використання мережних інформаційних систем виявлення атак є головною задачею в сфері інформаційного забезпечення установ. Під час написання кваліфікаційній роботі було вивчено та представлено:

- Структура обчислювальної мережі підприємства;

- Аналіз потоків інформації (як у внутрішній мережі, так і між

підрозділами підприємства);

- Алгоритм передачі та збереження інформації (схема процесу

документообігу).

Ця тема грає велику роль у концепції сталого розвитку підприємства. У

кваліфікаційній роботі надані перелік додаткових заходів щодо захисту інформації, розробка архітектурної системи захисту безпеки й обмеження доступу в корпоративну інформаційну мережу підприємства:

- мережний периметр вузлів та каналів передачі даних;

- брандмауери та маршрутизатори з фільтрацією пакетів;

- транслятори мережних адрес;

- транслятори адрес основних та альтернативних портів;

- підсистема захисту від розподілених мережних атак;

- псевдосервіси з явними вразливостями ("медові пастки");

- мережні псевдосервіси з вразливостями (мережні "медові пастки").

Під час написання кваліфікаційної роботи було вивчено та представлено:

- Структура обчислювальної мережі підприємства;

- Аналіз потоків інформації (як у внутрішній мережі, так і між підрозділами підприємства);

- Алгоритм передачі та збереження інформації (схема процесу документообігу).

Основним рішення щодо запобігання розподілених атак на комп'ютерні мережі та системи підприємства було обрано теорію конфлікту та адаптації степенів уразливості до поведінки атакуючого об'єкту, а саме:

- агресивна поведінка – демонстрація спокою;

- нейтральна поведінка – демонстрація впевненості;

- втрата інтересу – демонстрація розгубленості

Дані зміни концепцій взаємодії системи захисту з атакуючим суб'єктом надають можливість утримувати його у постійній напрузі і виключає підозри в тому, що суб'єкт потрапив у медову пастку.

З метою охорони анонімної інформації, якою обмінюються філії підприємства, використана технологія віртуальної корпоративної мережі підприємства, що створює умови для реалізації захисту каналу передачі даних від перехоплення і підміни інформації. Для збереження внутрішньої схеми побудови комп'ютерної інфраструктури підприємства використані антивірусні рішення.

Проксі-сервіси використовуються для наступних цілей:

- Доступ з локальної комп'ютерної мережі в Інтернет.

- Кешування даних: при регулярному зверненні до одних і тих самих зовнішніх ресурсів, можна отримати їх копію на проксі-сервері і видавати за запитом. До того ж це допомагає знизити навантаження на канал обміну інформації у зовнішню мережу і прискорює отримання клієнтом потрібної інформації.

- Стиснення даних: завантажуючи інформацію з Інтернету, проксі-сервер передає її у стисненому вигляді. Так проксі-сервери працюють з метою економії зовнішнього трафіку.

- Захист мережі від зовнішнього доступу: параметри налаштування проксі-серверу дозволяють зробити можливим звертання до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звернутися до термінальних вузлів взагалі (вони можуть №бачити» тільки проксі-сервер).

- Обмеження доступу з корпоративної мережі до зовнішньої: проксісервер дозволяє заборону доступу до певних ресурсів, обмеження використання інтернету певним локальним користувачам, встановлення квоти на трафік чи

смугу пропускання, фільтрування рекламного контенту та підозрілі трафіки чи віруси.

- Конфіденційність доступу до різних ресурсів. Проксі-сервер приховує інформацію про джерело запиту або користувача. Тобто зовнішній сервер «бачить» лише дані проксі-серверу (наприклад, IP-адресу), але визначити дійсне джерело запиту – неможливо. Також бувають спотворюючі проксісервери, що передають сторонньому серверу «фейкову» інформацію про існуючого користувача.

Для управління використовується інтерфейс, що має широкий набір параметрів та інструментів з управління доступом користувачів по протоколам HTTP та FTP. Також є можливість проаналізувати та сформувати статистичні дані, такі, як часто відвідувані вузли, кількість «спійманих» вірусів та ін.

При потребі взаємодії підрозділу з центральним офісом через VPN-канал використовується термінал-сервер. Термінальний клієнт після встановлення зв’язку з термінальним сервером пересилає на останній та вводить дані (натискання клавіш, переміщення миші) і далі, можливо, дозволяє доступ до локальних ресурсів (наприклад, принтер, дискові ресурси, пристрій читання смарт-карт, локальні порти (COM / LPT)). Термінальний сервер створює середовище для роботи (термінальна сесія). Як результат роботи серверу передаються зображення монітору чи звук (при його присутності). До переваги схеми використання термінального серверу можемо віднести забезпечення безпеки та зниження навантаження на канал зв’язку. Отже, завдання дипломного проектування виконані. Отриманні знання та інформація надалі можуть бути використані для захисту корпоративної інформації в комп’ютерних мережах чи системах підприємств чи установ, не залежно від масштабу, територіального розміщення чи призначення.

Встановлено, що під критичною інфраструктурою слід розуміти сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може спричинити втрату управління або завдати істотної шкоди на загальнодержавному, регіональному, місцевому або об'єктовому рівні. об'єктовому рівні. Атомні та гідроелектростанції, що входять до її складу, хімічні та нафтохімічні комбінати, металургійні заводи і безліч інших державних підприємств і приватних установ стратегічного призначення належать до потенційно-небезпечних і критично важливих об'єктів. Таким чином, під критичною інформаційною інфраструктурою розуміють сукупність автоматизованих систем управління виробничими та технологічними процесами потенційно-небезпечних, критично важливих та інших об'єктів критичної

інфраструктури, інформаційно-телекомунікаційні системи та мережі зв'язку, що забезпечують їхню взаємодію. Її головними вразливими місцями є провідні та бездротові лінії зв'язку й апаратно-програмні пристрої, що розташовуються за межами периметра, що охороняється.

Історія кібератак, що відбулися у світі, показує, що на кожному об'єкті критичної інфраструктури є інформаційно-управлінська складова, так звана критична інформаційна інфраструктура, виведення з ладу якої може не тільки зупинити виробничий процес підприємства, а й призвести до масштабних аварій і катастроф.

Проведений аналіз та дослідження нормативних документів дають можливість визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завданням із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту

Визначено, що обмеженість ресурсів вимагає визначення пріоритетів на основі економічної ефективності заходів безпеки, а не сліпого прийняття всеохоплюючого підходу. У більшості випадків потреба в безпеці має бути збалансована з продуктивністю, оскільки різні варіанти можуть бути громіздкими і заважати функціонуванню системи та організації. Більшість практик управління кіберризиками для захисту інфраструктури можна розділити на три групи: структурні, процедурні та реагування. Основна складова ризику залежить від характеру організації та управління її персоналом і підрядниками.

Технологічні рішення не вирішують всіх проблем кібербезпеки, , а модель управління кібербезпекою об'єктів критичної інфраструктури має вдосконалюватися разом з оперативним реагуванням на кібератаки інфраструктури, повинна вдосконалюватися разом із швидким розвитком технологій, правових аспектів. Кібератака часто розвивається в п'ять різних етапів: пошук вразливості системи, отримання контролю над системою або її частиною, впровадження шкідливого програмного забезпечення в систему, зараження інших компонентів системи та здійснення атаки на всю систему або на окрему її частину. Головним аспектом кібербезпеки є те, що кібербезпека має бути наріжним каменем при розробці нових IT-рішень та систем, а не, як це часто

буває, згадуватися лише наприкінці проекту, як це сталося з архітектурою Інтернету, яка була розроблена для сприяння зв'язку, а не безпеці. Модель управління кібербезпекою складається з шести основних розділів: правове регулювання, ефективне управління, управління ризиками, культура безпеки, управління технологіями, управління інцидентами.

Безпека критичної інформаційної інфраструктури - стан захищеності критичної інформаційної інфраструктури, що забезпечує її стійке функціонування під час проведення щодо неї комп'ютерних атак. Суб'єкти критичної інформаційної інфраструктури схильні до кібератак з різних причин, в основному, через свою значущість. Також ясно, що фізичні або кібератаки ніколи не припиняться. Тому кожна країна повинна повсюдно застосовувати найдоступніші та найнадійніші заходи щодо забезпечення інформаційної безпеки для цих інфраструктур. Кібератаки на критично важливі інфраструктури можуть завдати серйозної шкоди. Кількість кібератак на ядерні об'єкти, енергосистеми, греблі та інші найважливіші об'єкти зростає з кожним днем. Зростаюча кількість підключених до інтернету смарт-пристроїв створює серйозні вразливості для безпеки мереж. Отже, якщо не буде вжито дуже важливих кроків для розв'язання проблем безпеки, то очевидно, що шкода, яку завдають кібератаки на суб'єкти критичної інформаційної інфраструктури, призведе до катастрофічних наслідків для держав і організацій. Додатки Інтернет Речей є найбільш важливими структурами з точки зору підвищення ефективності роботи та взаємодії суб'єктів критичної інформаційної інфраструктури. Однак усі атаки, які можуть статися в мережі Інтернет, можуть бути виконані і в середовищі Інтернет Речей. У роботі було представлено найпоширеніші методи, які використовуються при кібератаках на суб'єкти критичної інформаційної інфраструктури. Обговорено різні сучасні способи пом'якшення наслідків кібератак з точки зору кібербезпеки. Особливо важливим аспектом кібербезпеки є використання відповідних методів ідентифікації, оскільки це допомагає заздалегідь вживати контрзаходів, а також дає змогу розробити прогнозуючу та попереджувальну стратегію кібербезпеки для суб'єктів критичної інформаційної інфраструктури з технологіями Інтернет Речей.

Проведений огляд заходів щодо захисту КІІ в різних країнах і міждержавних союзах дає змогу зробити низку зауважень щодо узагальнення отриманого ними досвіду для розуміння діяльності, яка відбувається в цій сфері, і можливих напрямів її розвитку в Україні. По-перше, різні країни підкреслюють їхню безумовну залежність сучасної інфраструктури від КІІ і важливість захисту КІІ для забезпечення обороноздатності. По-друге, в результаті розуміння проблеми не тільки формулюється загальне поняття КІІ як "обладнання, служб та

інформаційних систем, життєво важливі для держави, знищення або відмова яких призведе до ослаблення національного суспільства, національного господарства, громадського здоров'я, безпеки та ефективної роботи державної системи", а й визначаються основні складові: телекомунікаційні, енергетичні, банківські, фінансові, водогосподарські системи та аварійні служби. По-третє, стратегія забезпечення безпеки КІІ має системний характер і втілюється в життя за класичною схемою: навчання, попередження, оповіщення, ліквідація наслідків. По-четверте, будь-які дії урядових установ із забезпечення безпеки КІІ, пов'язані з пошуком інформації в особистих комп'ютерах та електронних повідомленнях, мають здійснюватися в суворій відповідності до законодавства, що забезпечує захист "громадянських свобод, особистих прав та особистих відомостей".

Технічне забезпечення на об’єктах критичної інфраструктури включає технології, механізми та засоби, що дозволяють реалізувати заданий рівень інформаційної безпеки кожної конкретної мережі, інформаційної системи, ресурсу, автоматизованого робочого місця, компонентів інформаційної інфраструктури шляхом виконання комплексу організаційно-технічних заходів. Основними засобами технічного забезпечення роботи на об’єктах КІ є:апаратні засоби, програмні засоби, криптографічні засоби, фізичні засоби. Служби інформаційної безпеки на об’єктах критичної інфраструктури широко використовують у своїй діяльності криптографічні засоби захисту інформації, які поєднують апаратні і програмні засоби реалізації криптографічних перетворень інформації.

Заходи щодо забезпечення ІБ на об’єктах критичної інфраструктури можна розділити на три ключові види: технічні засоби, організаційні заходи та профілактичні перевірки рівня захищеності. До яких входять : підвищення обізнаності персоналу, розмежування прав та ролей співробітників, аудит ІБ, PenTest, аналіз ризиків, обробка інцидентів, контроль змінних носіїв та багато технічних засобів.

Список використаних джерел

1. **Наталія Гончаренко**

ЗАСТОСУВАННЯ МЕХАНІЗМІВ DARK WEB ДЛЯ ЗАБЕЗПЕЧЕННЯ НОВОГО РІВНЯ ЗАХИСТУ ІОТ

2. **Еліна Пяташова, Наталія Лукова-Чуйко**

ТЕХНОЛОГІЯ БЛОКЧЕЙН. ОСНОВИ КІБЕРБЕЗПЕКИ ПРИ ВИКОРИСТАННІ КРИПТОВАЛЮТИ

3. **Віталій Чубаєвський, Валентина Макоєдова**

ЗАСТОСУВАННЯ БАГАТОРІВНЕВОГО ПІДХОДУ ЯК ЗАСІБ ПРОТИДІЇ

КІБЕРЗАГРОЗАМ

4. **Яніна Шестак, Максим Скрипник**

ОСНОВНІ ВИМОГИ ДО БЕЗПЕЧНИХ ХМАРНИХ СИСТЕМ УПРАВЛІННЯ

ВІДНОСИН З КЛІЄНТАМИ

5. **Лариса Крючкова, Іван Цмоканич**

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИСОКОЧАСТОТНОГО НАВ’ЯЗУВАННЯ НА

ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

6. **Лариса Крючкова, Максим Вовк**

МЕТОД БЛОКУВАННЯ КАНАЛІВ АКТИВНИХ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ

7. **Іван Данилів, Тарас Матіїв**

ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ ПРИ РОЗРОБЦІ ВЕБ СЕРВІСІВ

8. **Вікторія Клочко, Наталія Лукова-Чуйко**

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЛОКАЛЬНИХ МЕРЕЖ НА ПІДПРИЄМСТВІ

9. **Чумаченко Богдан, Заблоцький Костянтин, Малик Святослав, Одарченко Роман**

ДОСЛІДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОНІТОРИНГУ МЕРЕЖ

10. **Тетяна Бабенко, Романюк Валентин**

ФІШИНГОВІ АТАКИ З ВИКОРИСТАННЯМ HTM(HTML) ФАЙЛІВ, ЩО КОПІЮЮТЬ ЛЕГІТИМНІ СЕРВІСИ. МЕХАНІЗМ ДІЇ, СПОСОБИ ПРОТИДІЇ.

11. The Great IDS Debate: Signature Analysis Versus Protocol Analysis by Matt Tanase, Feb. 5, 2003p

12. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b4c1f4bd-4199-4d9eb61b486b3df2d76c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

13. CompTIA Security+ SY0-501 Cert Guide, Academic Edition, 2nd Edition By David L. Prowse - 560 ст.

14. Kurose J.F. Computer Networking: A Top-Down Approach, 7th Ed / James F. Kurose, Keith W. Ross. - Pearson Education, Inc., 2017. - 864 ст. Stallings W. Computer Organization and Architecture, 10th Ed. / Pearson Education, Inc., Hoboken, NJ, 2016. - 864 ст. Ng C.K. Honeypot Frameworks and their Applications: A New Framework /Chee Keong Ng, Lei Pan, Yang Xiang. - Springer Nature Singapore Pte Ltd., 2018. - 81 ст.

15. https://www.projecthoneypot.org/

16. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, 2002. – 480 ст.

17. http://www.iso27000.ru/standarty/bsi-it-baseline-protection-manual

18. Barabosch T. Bee Master: Detecting Host-Based Code Injection Attacks//Thomas Barabosch, Sebastian Eschweiler, and Elmar Gerhards-Padilla. - in Proceedings of 11th International Conference, DIMVA 2014, Egham, UK, July 10-11, 2014/

19. Diogenes Y. Cybersecurity - Attack and Defense Strategies / Yuri Diogenes, Erdal Ozkaya. - Packt Publishing Ltd., Livery Place,35 Livery Street, Birmingham,

B3 2PB, UK, 2018. - 354 ст.

20. Cybersecurity Best Practices Guide For IIROC Dealer Members - Investment Industry Regulatory Organization of Canada, 2015. - 53 ст.

21. Joseph Migga Kizza J.M. Guide to Computer Network Security, Fourth Edition. - Springer International Publishing AG 2017. - 569 ст.

22. Crimes R.A. Honeypots for Windows. - APRESS, 2005. - 392 ст.

23. Joshi R.C. Honeypots A New Paradigm to Information Security / R.C. Joshi, Anjali Sardana. - Science Publishers, P.O. Box 699, Enfi eld, NH 03748, USA, 2001. - 323 ст.

24. Park J.H. Future Information Technology / James J. (Jong Hyuk) Park, Yi Pan, Cheon-Shik Kim, Yun Yang. - Springer-Verlag Berlin Heidelberg 2014. – 936 ст.

25. Graham R. COMMUNICATIONS, RADAR AND ELECTRONIC WARFARE. - John Wiley and Sons, Ltd., The Atnum. Southern Gate, Chiche;ter, We;t Sussex, PO 19 8SQ, United Kmgdom. 2011. - 378 ст.

26. Mesarovic M.D. General Systems Theory: Mathematical Foundations. /

M.D. Mesarovic, Yasuhico Takahara. - Academic Press, New York, 1975, xii+268 ст.

27. Marchau V.A.W.J. Decision Making under Deep Uncertainty: From Theory to Practice / Vincent A. W. J. Marchau, Warren E. Walker,Pieter J. T. M. Bloemen, Steven W. Popper - Springer Nature Switzerland AG, Gewerbestrasse 11, 6330 Cham, Switzerland, 2019. - 405 ст.

28. Myers G.J. The Art of Software Testing 3rd Ed. / Glenford J. Myers, Corey Sandler, Tom Badgett. - John Wiley & Sons, Inc., 2012. - 256 ст.

29. Saaty T. L. The analytic hierarchy process / T. L. Saaty. - McGraw Hill, N.- Y., 1980, 288 ст.

30. Bonaventure O. Computer Networking : Principles, Protocols and Practice. - Release Sep 07, 2018. - 272 ст.

31. Benslama M. Ad Hoc Networks Telecommunications and Game Theory / Malek Benslama Mohamed Lamine Boucenna Hadj Batatia. - John Wiley & Sons, Inc., 2015. – 141 ст.

32. Bendat J. Random Data: Analysis and Measurement Procedures. Fourth Edition / Julius S. Bendat, Allan G. Piersol. - John Wiley & Sons, Inc., Hoboken, New Jersey, 2010. - 640 ст.

33. Наталія Гончаренко

ЗАСТОСУВАННЯ МЕХАНІЗМІВ DARK WEB ДЛЯ ЗАБЕЗПЕЧЕННЯ НОВОГО РІВНЯ ЗАХИСТУ ІОТ