Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *«Розробка концепції розгортання кіберполігону»*

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Демчишин М.М.
підпис (прізвище та ініціали)

Керівник *Александер Марек Б.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» __червня__ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Демчишину Максиму Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка концепції розгортання кіберполігону

Керівник роботи Александер Марек Богуслав, д.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи Вимоги до кіберполігону

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз вимог до розгортання кіберполігону
Аналіз інфраструктури кіберполігону
Аналіз сучасних загроз в складових безпеки інформації
Принципи формування задач, вихідної інфраструктури до відпрацювання у кіберполігоні
Розгортання елементів інфраструктури кіберполігону університету
Розробка рекомендацій задач, які відпрацьовуються у кіберполігоні
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець.М.І., проф. кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.01 – 19.01	*Виконано*
2.	Підбір джерел про методи та принципи побудови кіберполігонів	20.01 – 05.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	06.02 – 22.02	*Виконано*
4.	Розгортання кіберполігону	23.02 – 20.03	*Виконано*
5.	Розробка рекомендацій задач, які відпрацьовуються у кіберполігоні	21.03-05.04	*Виконано*
6.	Оформлення розділу «Аналіз вимог до розгортання кіберполігону»	06.03 – 17.04	*Виконано*
7.	Оформлення розділу «Розробка концепції розгортання кіберполігону»	18.04 – 29.04	*Виконано*
8.	Оформлення розділу «Розгортання кіберполігону в університеті»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 11.06	*Виконано*
12.	Перевірка на плагіат	12.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	23.06.2023	

Студент _____ *Демчишин М.М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Александер Марек Б.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка концепції розгортання кіберполігону // Кваліфікаційна робота ОР «Бакалавр» // Демчишин Максим Миколайович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. __ , рис. – __, табл. – __, кресл. – , додат. –

Ключові слова: КІБЕРПОЛІГОН, BLOCKCHAIN, СУЧАСНІ ЗАГРОЗИ, PROXMOX VE, KVM, LXC, КЛАСТЕР ВІРТУАЛІЗАЦІЇ, СЕРВЕР, ЗАХИСТ ІНФОРМАЦІЇ, РОЗУМНИЙ ДІМ, МЕРЕЖЕВА АРХІТЕКТУРА, CPS, CCIS, МОДЕЛЬ OSI.

Метою роботи є огляд та опис архітектури та принципів розгортання кіберполігону на базі кластеру віртуалізації, формування завдань для відпрацювання у кіберполігоні, а також розбір сучасних загроз, котрі будуть розглянуті на практиці у кіберполігоні.

Об'єктом дослідження є процес розгортання кіберполігону.

Предметом дослідження є розробка концепції розгортання кіберполігону.

Результатами дослідження є засоби, методи, заходи що до збільшення кваліфікації студентів, фахівців, експертів та керівників в сфері інформаційних технологій, інформаційної безпеки та систем промислової автоматизації.

Отримані результати можуть бути впроваджені в нормативну базу університету з метою покращення рівня його рейтингу.

Проведено аналіз інфраструктури кіберполігону на базі кластеру віртуалізації за технологією Proxmox VE, функціональні можливості технології Proxmox VE. Проведена оцінка загроз інформаційній безпеці і наведені заходи по забезпечення безпеки інформаційної системи університету, а також проведена оцінка економічної складової заходів забезпечення інформаційної безпеки.

ABSTRACT

Development of a concept for deploying a cyber range // Thesis of educational level "Bachelor" // Denchyshyn Maksym Mykolaiovych// Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБс-41 group // Ternopil, 2023 // P. ___ , fig. -____, table. - __ , chair. - ___ , added. -___.

Keywords: CYBER POLYGON, BLOCKCHAIN, MODERN THREATS, PROXMOX VE, KVM, LXC, VIRTUALIZATION CLUSTER, SERVER, INFORMATION PROTECTION, SMART HOUSE, NETWORK ARCHITECTURE, CPS, CCIS, OSI MODEL.

The purpose of the master’s thesis is to review and describe the architecture and principles of cyber polygon deployment based on the virtualization cluster, the formation of tasks for practice in cyberpolygon, as well as analysis of current threats that will be considered in practice in cyber polygon.

The object of study is the process of deploying a cyber polygon.

The subject of research is the development of the concept of cyber polygon.

The results of the study are tools, methods, measures to improve the skills of students, professionals, experts and managers in the field of information technology, information security and industrial automation systems.

Obtained results can be incorporated into the university's regulatory framework in order to improve its rating.

The analysis of the cyberpolygon infrastructure on the basis of the virtualization cluster according to Proxmox VE technology, the functionality of Proxmox VE technology is carried out. Research of assessment of threats to information security and measures to ensure the security of the information system of the university, as well as assessment of the economic component of measures to ensure information security.

ЗМІСТ

ВСТУП

У сучасних реаліях злам зловмисниками корпоративної мережі починається з компрометації корпоративного сайту компанії або облікового запису електронної пошти, форма авторизації якої часто знаходиться в межах сайту або на піддомену. Отримання доступу до вебсайту компанії дозволяє зловмисникам проводити подальші атаки всередину мережі організації або вже на цьому етапі отримувати фінансову вигоду [4–14].

Злам корпоративного сайту – проблема безпеки, що найчастіше зустрічається. Як ми й писали раніше, на одному з перших місць стоїть слабка парольна політика – багато хто звикли ставити прості паролі в особистому житті та переносять цю практику в корпоративний сектор. На другому місці – вразливість вебдодатків. Як показує практика, зловмисники атакують абсолютно будь-які сайти, попри їх приналежність та рівень захисту. Це виникає через те, що більшість «спеціалістів» найчастіше не мають повноцінного і коректно налаштованого моніторингу, із-за чого це може призвести до неможливості розслідування інциденту.

Інтенсивне впровадження передових інформаційних технологій у державну сферу та стійка тенденція до формування нового середовища віртуального протистояння – кіберпростору, спонукає до пошуку дієвих механізмів та інструментів забезпечення його безпеки. Кіберполігон - це сукупність спеціалізованих програмно-апаратних комплексів, що об’єднані провідними й безпровідними комунікаціями, інтегрованими у мережу Інтернет, які застосовуються для здійснення моніторингу, впливу на системи управління об’єктів, що становлять інтерес, а також захисту власних систем управління від аналогічних дій протиборчої сторони [6]. Таким чином його розгортання в університетах, де навчаються за спеціальністю 125 “Кібербезпека” є актуальним завданням.

РОЗДІЛ 1. АНАЛІЗ ВИМОГ ДО РОЗГОРТАННЯ КІБЕРПОЛІГОНУ

1.1 Аналіз принципів розгортання кіберполігону

Більшість державних структур та компаній не готові до кібератак. Ще 10 років тому хакери атакували, в основному, ті організації, звідки вони могли швидко вивести гроші. Для промисловості ця загроза була менш релевантною. Предметом їх інтересу стають і інфраструктури державних організацій, енергетичних, промислових підприємств. Тут ми частіше маємо справу зі спробами шпигунства, крадіжки даних в різних цілях (конкурентна розвідка, шантаж), а також отриманням точок присутності в інфраструктурі для подальшого продажу їх зацікавленим товаришам. Середній час виявлення інциденту становить 100 днів. Причиною цього є недостатньо навичок для оперативного реагування, тому що не проводиться регулярних тренувань на протидію атакам, відображає актуальні тенденції в області кібербезпеки. Найчастіше відсутність повноцінного і коректно налаштованого моніторингу призводить до неможливості розслідування інциденту. З іншого боку, моніторинг може бути “забитий” шумом, що призводить до неможливості швидкого і коректного реагування. Саме для покращення даної ситуації, було створено кіберполігон.

Кіберполігон представляє собою сукупність спеціалізованих програмно-апаратних комплексів, що об’єднані провідними й безпровідними комунікаціями, інтегрованими у мережу Інтернет, які застосовуються для здійснення моніторингу, впливу на системи управління об’єктів, що становлять інтерес, а також захисту власних систем управління від аналогічних дій протиборчої сторони [6].

Це реальна можливість для студентів, кадетів або інших спеціалістів різних компаній “потренуватись з кішками”, відпрацювати практичні навички без ризиків, що щось може піти не за планом та кібернавчання нанесуть збиток діяльності реального підприємства. Типова схема мережевих інфраструктур наприклад підприємства або корпорації – це доволі стандартний набір серверів, робочих комп’ютерів та різноманітних мережевих пристроїв з типовим набором

корпоративного ПЗ та систем інформаційної безпеки. Розглянемо галузевий кіберполігон Міністерства оборони – це все теж саме, але більш серйозна специфіка, різко ускладнює віртуальну модель. Комплекс дозволяє розгорнути та використовувати понад 1500 віртуальних машин і створювати більш як 70 незалежних дослідницьких лабораторій. Інфраструктура дозволяє перерозподілити потужності між ділянками відповідно до потреб. Високопродуктивна мережа передачі даних, підключена до захищених мереж (мережі зв'язку спеціального призначення), дозволить структурам МО (міністерство оборони) використовувати лабораторії віддалено. Система резервування відновлення даних забезпечує найвищу ступінь відмово стійкості комплексу [6–8].

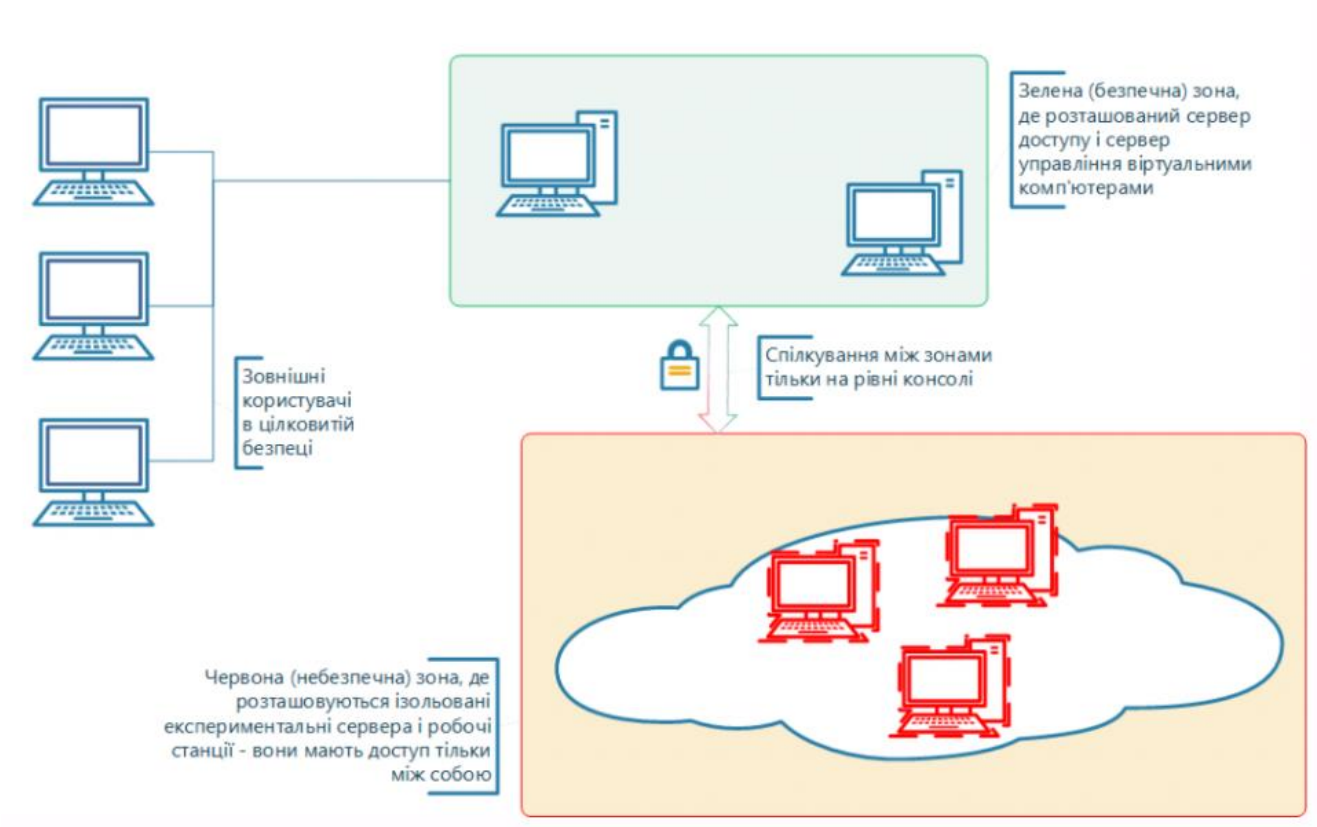


Рисунок 1.1 – Віртуальна лабораторія "Кіберполігон" – концептуальна схема

1.2 Оцінка основних функцій кіберполігону

У теперішній час дуже активно використовують персональні комп'ютери. Це призводить до потреби створювати захист для важливих даних. Зазвичай різні установи не мають своїх фахівців, які вирішують задачі по захисту інформації. Але

це триває до певного часу, а потім звертаються до ІТ-спеціалістів, адміністративним менеджерам або пускають все на самоплив, але доки ваш програмний код, інформація або продукт не розпочнуть заробляти гроші на інших сайтах. На привеликий жаль немає одного алгоритму, якиц підійте для всіх. Кожна організація потребує індивідуальний підхід.

Можна назвати декілька вид загроз кібербезпеки, які варті уваги [4–14]:

- соціальна інженерія і фішинг;
- вірусне програмне забезпечення;
- використання неактуальних версій програмного забезпечення;
- інсайдерські загрози.

Якщо переглянути основні задачі системи Кіберполігону, то можна виділити те, що загалом вони забезпечують рішення:

- розроблення та практична апробація спеціалізованого програмного забезпечення для забезпечення кібербезпеки;

- розроблення лабораторії, щоб проводити необхідні дослідження різноманітних методів захисту та проведення дослідів в галузі технічних та програмних засобів кіберзахисту об’єктів критичної кібернетичної інфраструктури;

- розроблення способів нейтралізації кіберзагроз, врахувавши наявні сили та засобів;

- моделювання процесів кібернападу та кіберзахисту на об’єкти з критичною кібернетичної інфраструктури, тощо.

Але як саме зможуть підготувати спеціалістів до різноманітних атак, що насправді повинен знати та вміти кожен з державних спеціалістів або з великої компанії.

Проаналізувавши основні з методики тренування під час тестування продукту, можна виділити [4–14]:

- аналіз коду програмних продуктів (використовуючи, наприклад методи зворотної інженерії);
- аналіз функціональності програмно-апаратних комплексів;

- виявлення вразливостей в автоматизованих системах управління;
- навантажувальне тестування систем управління і захисту інформації;
- перевірка оновлень ПЗ перед застосуванням;
- перевірка захищеності мереж зв’язку;
- можливість віддаленого використання центру для навчання фахівців;
- співробітники центру зможуть перевірити засвоєні знання на практиці.

За всіма аналізами можна зробити висновок, що розвиток обчислювальних ресурсів та технологій “G” визначили стрімке зростання Інтернет-речей на основі синтезу фізичних систем та інтернет-технологій. З урахуванням того, що відсутнє єдине загальноприйняте визначення кіберфізичних систем, дається досить загальне визначення кіберфізичної системи як системи, яка використовується для моніторингу та управління об'єктами фізичної природи (фізичного світу). Ці системи сприймаються як нове покоління вбудованих систем керування. Крім того, системи, в які вбудовані мережі датчиків та виконавчих механізмів, також вважаються кіберфізичними системами.

Через залежність від ІТ-систем кіберфізичні системи можна визначити, як ІТ-системи, які інтегровані у додатки фізичного світу. Ця інтеграція є результатом досягнень у галузі інформаційних та комунікаційних технологій (ІКТ) для покращення взаємодії з фізичними процесами. Всі ці визначення підкреслюють постійну та інтенсивну взаємодію між кібер- та фізичним світом [5]. Однак їх розвиток визначив і новий напрямок у розвитку та/або модифікації старих загроз, що не тільки проявляється у можливості злому та несанкціонованого доступу до конфіденційної (персональної) інформації користувачів, а й можливістю проведення “енергетичного апокаліпсиса”. Це дає кіберзлочинцям використовувати кіберфізичні системи для отримання синергетичного ефекту від реалізації загроз у кіберпросторі загалом.

Під час створення систем класифікацій та розробки відповідних класифікаторів кіберфізичним системам, слід розглядати дані аналізу та класифікації загроз інформаційним ресурсам державного рівня як дорожню карту для цілей цього дослідження. Використання даного підходу можна аргументувати

тим, що між інформаційними ресурсами традиційних IT-систем та ресурсами кіберфізичних систем існують суттєві відмінності, що унеможливлює використання методологічних основ, орієнтованих на традиційні IT-системи, у сферу кіберфізичних систем. Проведення іспитів, котрі були, присвячені розробці методологічних основ побудови класифікаторів загроз кіберфізичних систем, теоретично розділяємо на три групи.

Перша група об’єднує дані іспитів, що описують різні кіберфізичні системи та їх особливості та характеристики, які роблять їх уразливими для різноманітних загроз. Друга група включає дані, присвячені різноманітним загрозам та атакам, спрямованим безпосередньо на кіберфізичні системи. Дані третьої групи описують різні підходи до побудови таксономії та класифікації, які, зрештою, призводять до побудови класифікаторів загроз для кіберфізичних систем. Найбільш показовою роботою першої групи є, в якій зібрано та систематизовано в рамках єдиної структури наявного дослідження з безпеки кіберфізичних систем (CPS – cyber-physical systems). Запропонована структура є тривимірною системою ортогональних координат. Перша вісь відповідає відомим класифікаціям (таксономіям) загроз, вразливостей, атак та засобів контролю з погляду безпеки. Друга вісь відповідає компонентам та підсистемам з точки зору їх природи, а саме – кібернетичної (комп'ютерно-інформаційної), фізичної та кіберфізичної. Остання проявляє синергетичні властивості, якими не мали елементи або підсистеми перших двох. І нарешті, третя вісь відповідає зображенню інтегральних (синергетичних) функцій кіберфізичних систем, а також прояву їх у різних типових кіберфізичних системах (наприклад, інтелектуальних мережах, медичних CPS та інтелектуальних машинах та механізмах). На рис. 1.2 пропонується взаємозв'язок запропонованої структури з інформаційно-критичними кібернетичними системами (critical cybernetic information systems, CCIS), з прикладу організацій банківського сектора [5–10].

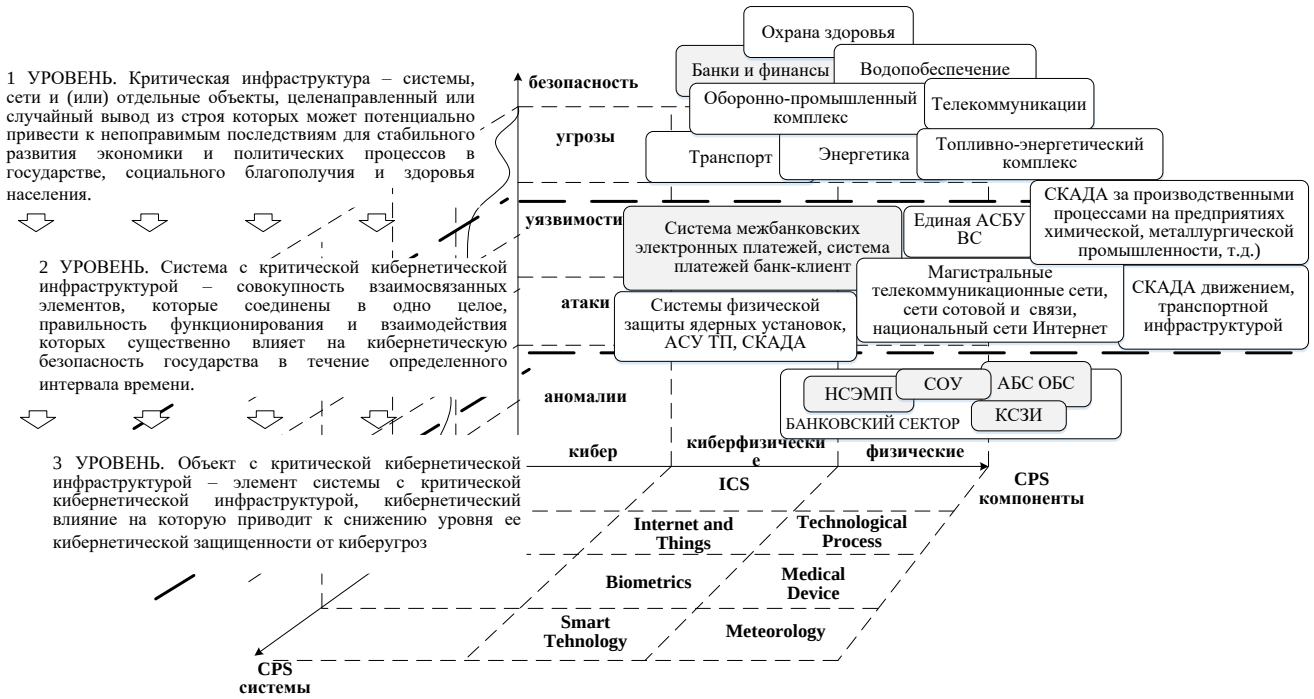


Рисунок 1.2 – Взаємозв’язок ІККС із CPS

Зазначається, що проектована модель CPS (кіберфізичної системи, cyberphysical system) може бути як абстрактною, щоб показати загальні взаємодії програми CPS, так і специфічною, щоб фіксувати будь-які деталі, коли це необхідно. Таке уявлення дозволяє побудувати модель, досить абстрактну, щоб її можна було застосовувати в різних гетерогенних CPS-додатках, з одного боку, і отримати модульне уявлення тісно пов'язаних та взаємодіючих компонентів CPS, що забезпечує формування та прояв у процесі функціонування синергетичних властивостей. Такий абстрактний поділ дозволяє сформувати систематичне розуміння безпеки CPS та виділити потенційні джерела атак та способи захисту. У результатах проведеного аналізу стверджується, що виявлення відмінностей між традиційними IT-системами та кіберфізичними системами є ключовим у розумінні проблем безпеки CPS і подальшій побудові класифікаторів загроз таким системам.

Спеціально розглядаються 4 конкретні кіберфізичні системи, а саме мережі енергопостачання, медичні системи, інтелектуальні автомобілі та системи управління промисловими об'єктами. Для цих систем докладно розглядаються питання зв’язку у цих системах та їх безпека. Наголошується, що контроль безпеки зазвичай пов'язаний з такими механізмами, як криптографія, контроль доступу,

виявлення вторгнень та багато інших рішень, які зазвичай використовуються в IT-системах. Ці механізми є дуже важливими для захисту інфраструктури інформаційних та комунікаційних технологій. Зазначається, що для забезпечення безпеки необхідні рішення, що враховують кіберфізичні аспекти, і вони можуть бути доповнені рішеннями IT-безпеки [5–14].

Забезпечення безпеки CPS пов'язане з різними проблемами, однією з яких є розуміння потенційних загроз. Знання того, від кого від чого ми захищаємо CPS, однаково важливо для розуміння існуючих вразливостей та механізмів атаки. Загроза безпеки визначається як "набір обставин, які можуть призвести до втрати або заподіяння шкоди". Визначаються п'ять чинників кожної загрози: джерело, мета, мотив, вектор атаки та потенційні наслідки. Джерелом загрози є ініціатор атаки. Джерела загроз поділяються на три типи: протиборчі загрози, які є намірами окремих осіб, групових організацій або держав/націй; випадкові загрози – це загрози, викликані випадково або через законні компоненти CPS; екологічні загрози, у тому числі стихійні лиха (повені, землетруси), техногенні катастрофи (пожежі, вибухи) та зброї допоміжної інфраструктури (перебої у подачі електроенергії або втрата зв'язку).

Цілі – це програми CPS, їх компоненти або користувачі. У зловмисників CPS зазвичай є одна або кілька причин для початку атаки: злочинна, шпигунська, терористична, політична чи кібервійна. Загроза може виконувати один або кілька із чотирьох механізмів успішної атаки: перехоплення, переривання, модифікація чи фабрикація. Наслідками атаки можуть бути порушення конфіденційності, цілісності, доступності, конфіденційності або безпеки CPS. Для обраних чотирьох додатків кіберфізичних систем досліджуються потенційні загрози та вразливість. Дані проведеного аналізу містять зведені таблиці, що відбивають вплив кожного з п'яти зазначених чинників той чи інший тип кіберфізичної системи, і навіть перелік характерних атак, вжитих проти таких систем. Все це може розглядатися як фундамент для побудови класифікатора загроз кіберфізичним системам, які враховують синергетичні ефекти таких систем [5–8].

Якщо розглянути внесок даних від згаданих аналізів у проблемі побудови класифікаторів загроз CPS можна сформулювати так:

1. Запропоновано систему безпеки CPS, яка призначена для розрізнення кіберфізичних та фізичних компонентів у даній системі.

2. Досліджено потенційні джерела загроз та їх мотиви.

3. Подано існуючі вразливості та виділено суттєві причини їх виникнення на реальних прикладах.

4. Проведено огляд зафіксованих атак на CPS з метою виявлення основних вразливостей та компонентів, що зазнають впливу загроз.

5. Проведено порівняльний аналіз існуючих механізмів контролю та визначено невирішені проблеми та проблеми у різних додатках CPS. Обговорюються три ключові проблеми для захисту кіберфізичних систем: розуміння загроз і можливих наслідків атак, виявлення унікальних властивостей кіберфізичних систем та їх відмінностей від традиційної IT-безпеки, та обговорення механізмів безпеки застосовується до кіберфізичних систем. Зокрема, аналізуються механізми безпеки для: запобігання, виявлення та відновлення, стійкості та стримування атак. Відмінною рисою іспиту є розробка моделі супротивника як спосіб зрозуміти масштаби проблеми та оцінити ризики. У звіті дослідження, наведено опис деяких потенційних зловмисників, їх мотиви та ресурси, а також аналіз поведінкових аспектів зловмисників [5–10]. Кіберзлочинці, метою яких є компрометація комп’ютерів скрізь, де їх можна виявити (навіть у системах управління). Атаки кіберзлочинців не обов’язково можуть бути цільовими (тобто кіберзлочинці можуть не мати наміру завдавати шкоди системам контролю), але можуть викликати негативні побічні ефекти: системи управління, заражені шкідливим програмним забезпеченням, можуть працювати неналежним чином.

Інсайдери нині є основним джерелом цілеспрямованих комп'ютерних атак системи управління. Ці атаки важливі з точки зору безпеки, тому що вони викликані особами з авторизованим доступом до комп’ютерів та мереж, які використовуються системами керування; тому, навіть якщо мережі керування

будуть повністю ізольовані від загальнодоступних мереж (і Інтернету), атаки з боку інсайдерів будуть можливі. Оскільки незадоволені співробітники, як правило, діють поодинці, потенційні наслідки їх атак можуть бути не такими руйнівними, як потенційна шкода, яку завдають більші організовані групи.

Терористи, активісти та організовані злочинні групи є ще однією потенційною загрозою для систем контролю. Атаки на системи управління з метою вимагання не є новими. Кібератаки є природним розвитком фізичних атак: вони дешевші, менш небезпечні для зловмисника, не обмежені відстанню, їх легше копіювати та координувати.

Держави можуть бути потенційною загрозою для систем управління. Загалом не дивно, що більшість військових держав вивчають технології майбутніх атак, включаючи кібератаки проти фізичної інфраструктури інших країн.

За результатами дослідження [5–8] підкреслюється, що основним завданням є виявлення та класифікація атак нового типу, які можливі в системах управління, та вивчення їх можливих наслідків. Так, наприклад, зловмисники можуть запускати унікальні атаки на системи управління (тобто атаки, які неможливі у традиційних IT-системах). Одним із можливих прикладів можуть бути резонансні атаки. У резонансній атаці зловмисник, який скомпрометував деякі датчики чи контролери, змусить фізичну систему вагатися зі своєю резонансною частотою. У, виходячи з визначення кіберфізичної системи, як розподіленої системи управління зі строгими тимчасовими обмеженнями, що складається з фізичних та кіберкомпонентів, сформульовані відмінності між IT-системою та кіберфізичною системою. Фізичний інтерфейс: Наявність фізичного інтерфейсу – це те, що робить безпеку CPS особливо складною. На відміну від окремої IT-системи порушення безпеки в системі CPS призводить до катастрофічних наслідків. Зловмисник може використовувати фізичний інтерфейс, щоб підірвати безпеку CPS без порушення механізму контролю доступу. У традиційній IT-безпеці це може статися тільки якщо дані передаються через відкриту мережу [5].

Система керування: CPS виконується на основі однієї або декількох базових мереж керування, які часто інтегровані з фізичним датчиком/виконавчим

механізмом, що помітно відрізняється від традиційної безпеки IT. Системи диспетчерського контролю та збору даних (SCADA) є невід'ємною частиною сучасної промислової інфраструктури. Не дивно, що вразливості у цій мережі управління залишаються привабливим місцем для кібератак, які продовжують зростати через підключені до Інтернету системи SCADA. Особливістю аналізу є не лише класифікація атак, а й зв'язок її зі стандартами безпеки. Крім цього, сучасні гібридні атаки на комп'ютерні системи державного рівня не просто ушкоджують ізольовану машину чи порушують роботу єдиної корпоративної системи.

Натомість нові атаки націлені на інфраструктуру, яка є невід’ємною частиною економіки, національної оборони та повсякденного життя. Дослідження кіберфізичних систем змістили акцент із розробки завдання оптимізації цих обчислювальних компонентів на залучену взаємодію між фізичними середовищами та обчислювальними елементами, з якими вони взаємодіють.

Запропоновано класифікацію, що складається з чотирьох вимірів, що дозволяє одночасно розглядати питання як функціонування мережі, так і питання, пов'язані з комп'ютерними атаками. Перший вимір класифікації охоплює вектор атаки та основний сценарій проведення атаки. Другий вимір класифікації ідентифікує атаку з її основної мети. Вразливості класифікуються у третьому вимірі класифікації, а корисні навантаження – у четвертій таксономії. Аналогічно, автори представляють методологію аналізу ризиків інформаційної безпеки, яка пов'язує активи, уразливості, загрози та елементи управління організації. Підхід використовує послідовність матриць, які відбивають кореляцію різних елементів під час аналізу ризику. Дані агрегуються та каскадуються за матрицями, щоб співвідносити активи з елементами управління таким чином, щоб отримати пріоритетне ранжування елементів управління на основі активів організації.

Крім того, обговорювалися і класифікувалися кіберфізичні інциденти на основі секторів, джерел та впливу інцидентів. У цьому документі наведено приклад того, як організація процесу збору інформації про кіберінциденти може бути використана жертвами кібератак. Крім того, описана спроба допомогти в розумінні загрози кіберінцидентів для різних цілей, що може бути корисним для підвищення

організаційної спрямованості з погляду кіберінциденту. У запропонованій класифікації етапи інцидентів були досліджені з урахуванням додаткових розширень, що зображають різні категорії сутності, що беруть участь в атаках та взаємозв'язках атак. Так, авторами виділені такі класи сутностей – це зловмисник, вразливість, інструмент, ціль, дію, цілі та несанкціонований результат. Зловмисники використовують інструменти для виконання дій, які використовують вразливість мети [5–8].

Наведено моделі серед віртуальних систем управління (VCSE), що ілюструє відповідні частини CPS та їх загрози. Вони призначені для аналізу впливу фізичних факторів. Моделі були побудовані з реальних, змодельованих та емульованих компонентів, які були вразливими для фактичних, змодельованих шкідливих та інших ворожих дій. Крім динамічної основи кібертероризму було запропоновано структуру, що описує основні компоненти кібертероризму. Кібертероризм було визначено структурою, що відбиває шість точок зору: мотивацію, мета, метод атаки, предметну область, дії злочинця і вплив атаки.

Класифікація механізмів кібератак та захисту для мереж управління у надзвичайних ситуаціях націлена на підтримку загального уявлення про пов'язані механізми кібератак та захисту. Механізми атак класифікуються за трьома аспектами, мережею, за функціями, що атакуються, і факторами атаки, у той час, як механізм захисту визначається за типом захисту, ступенем розподілу та організаційними елементами [5–11]. Крім того, проблеми кібербезпеки в управлінні надзвичайними ситуаціями поділені на три групи, які визначаються критичністю за часом (належить до надзвичайних ситуацій), коли рішення мають бути прийняті та швидко передані. Національний інститут стандартів та технологій (NIST) представив структуру, сфокусовану на використанні драйверів бізнесу для керівництва діяльністю кібербезпеки та розгляді ризиків кібербезпеки як частини процесів управління ризиками організації. Структура класифікації представлена трьома частинами: ядром структури, профілем структури та рівнями реалізації структури. Ядром структури є комплекс заходів щодо кібербезпеки, підсумки та інформаційні довідники, які є спільними для секторів критичної інфраструктури,

забезпечуючи докладний посібник для розробки організаційних профілів особистості. Використовуючи профіль, структура покликана допомогти організації привести свою діяльність у галузі кібербезпеки у відповідність до вимог бізнесу, допустимих ризиків та ресурсів. Рівні надають методику для організацій, щоб зрозуміти та розглянути характеристики підходу до управління ризиком кібербезпеки. Крім того, представлена математична кількісна структура, засновану на загрозах, яка використовується для оцінки та проєктування безпеки CPS [5–8].

Для протистояння кожному елементу загрози пропонується керуватися такими трьома принципами [6]:

Принцип 1: фокусування на критичній системі має включати лише основні функції.

Принцип 2: переміщення ключових елементів активів, необхідних для місії, та контроль безпеки, який зловмиснику важко досягти фізично та логічно (для зменшення доступності).

Принцип 3: реагування, виявлення, адаптація та введення в оману зловмисників шляхом впровадження елементів системи з технологіями динамічного реагування (для протидії можливостям зловмисника).

Після досліджень [5–11] були представлені результати аналізу сучасного забезпечення захисту державних інформаційних ресурсів (ДІР) в інформаційно-телекомунікаційних системах, при цьому акцент під час аналізу, котрий було проведено на нормативно-правовому забезпеченні захисту ДІР, докладно розкрито правові аспекти формування системи ДІР, а також введено нові терміни та визначення проблематики їх захисту. Істотним недоліком є відсутність зв’язку загроз з моделлю OSI, яка дозволяє визначити критичні точки проникнення.

За результати аналізу [5] пропонується удосконалений варіант класифікатора загроз на банківську інформацію, на рис. 1.3 наведено структурну схему запропонованого рішення.

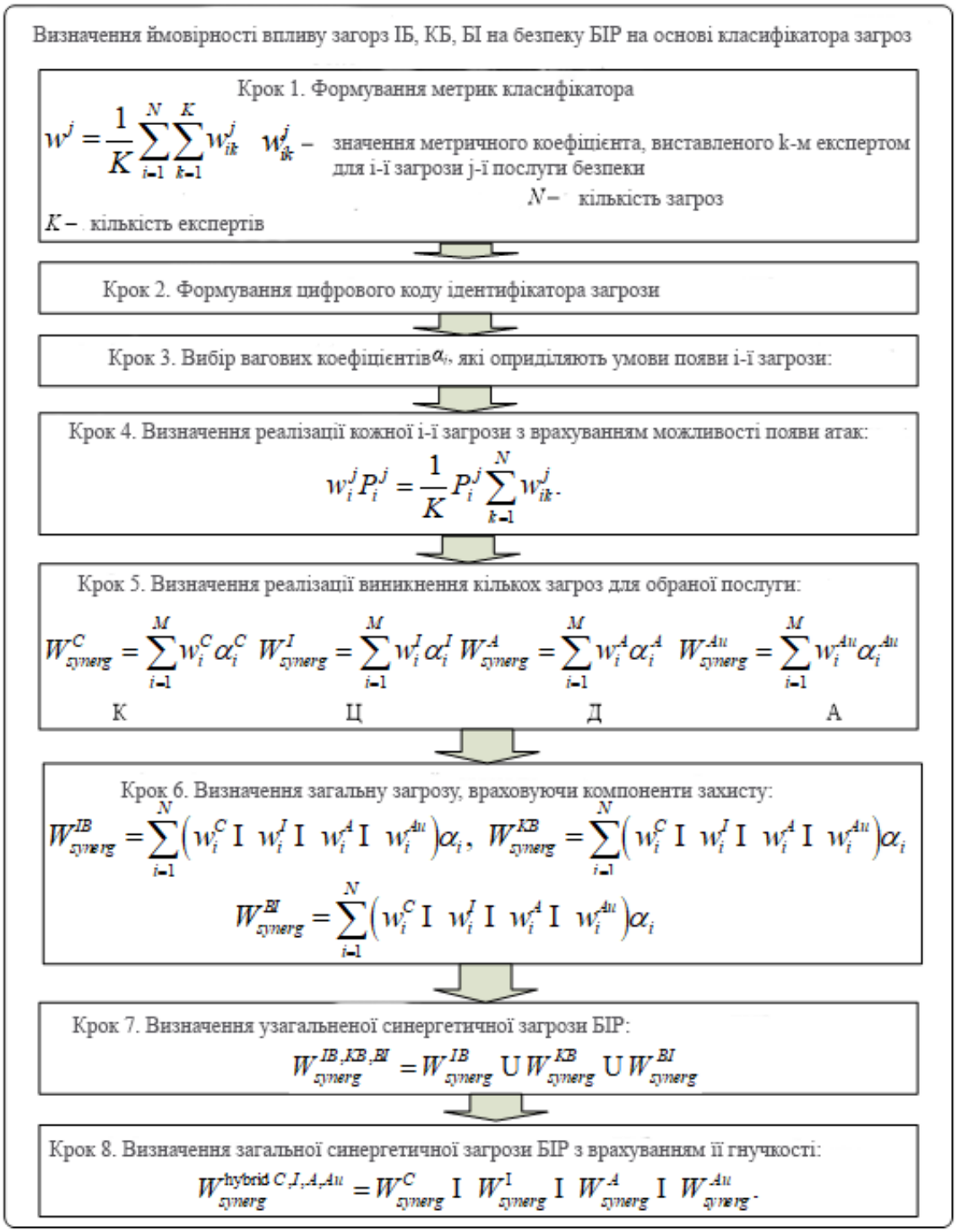


Рисунок 1.3 – Визначення ймовірності загроз на основі синергетичної моделі загроз

Відповідно до стандарту ISO/IEC 27001:2013 загрози поділяються на навмисні, випадкові та/або екологічні. Типовими прикладами можуть бути технічні зброї, несанкціоновані дії, втручання у програмне забезпечення, фізичні збитки, компрометація функцій тощо [5].

1.3 Основні технічні вимоги до апаратного обладнання, програмних застосунків

До складу структурної схеми кіберполігону, на прикладі МО, який наведений на рис. 1.5 входять два комплекти спеціалізованих програмно-апаратних комплексів [6–11]:

- комплект сил кібероборони;
- комплект сил тестування на кіберзахищеність.

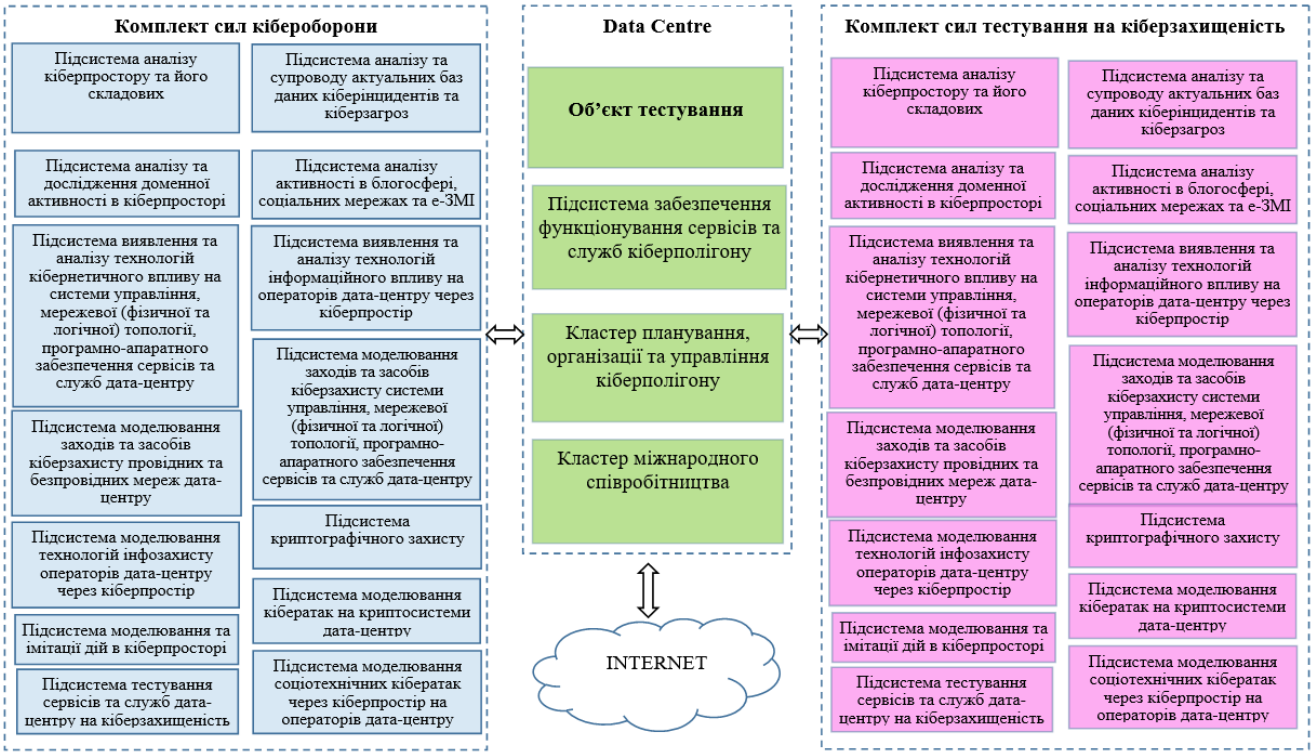


Рисунок 1.4 – Структурна схема кіберполігону

Комплект сил кібероборони застосовується для захисту сервісів, а також служб дата-центру кіберполігону.

Комплект сил тестування застосовується для тестування на кіберзахищеність сервісів та служб дата-центру кіберполігону.[6–8].

В основу мережевої топології кіберполігону покладено комплекти, об'єкти, компоненти, кластери та підсистеми кіберполігону визначені згідно зі структурною схемою (див. рис. 1.6) [6].

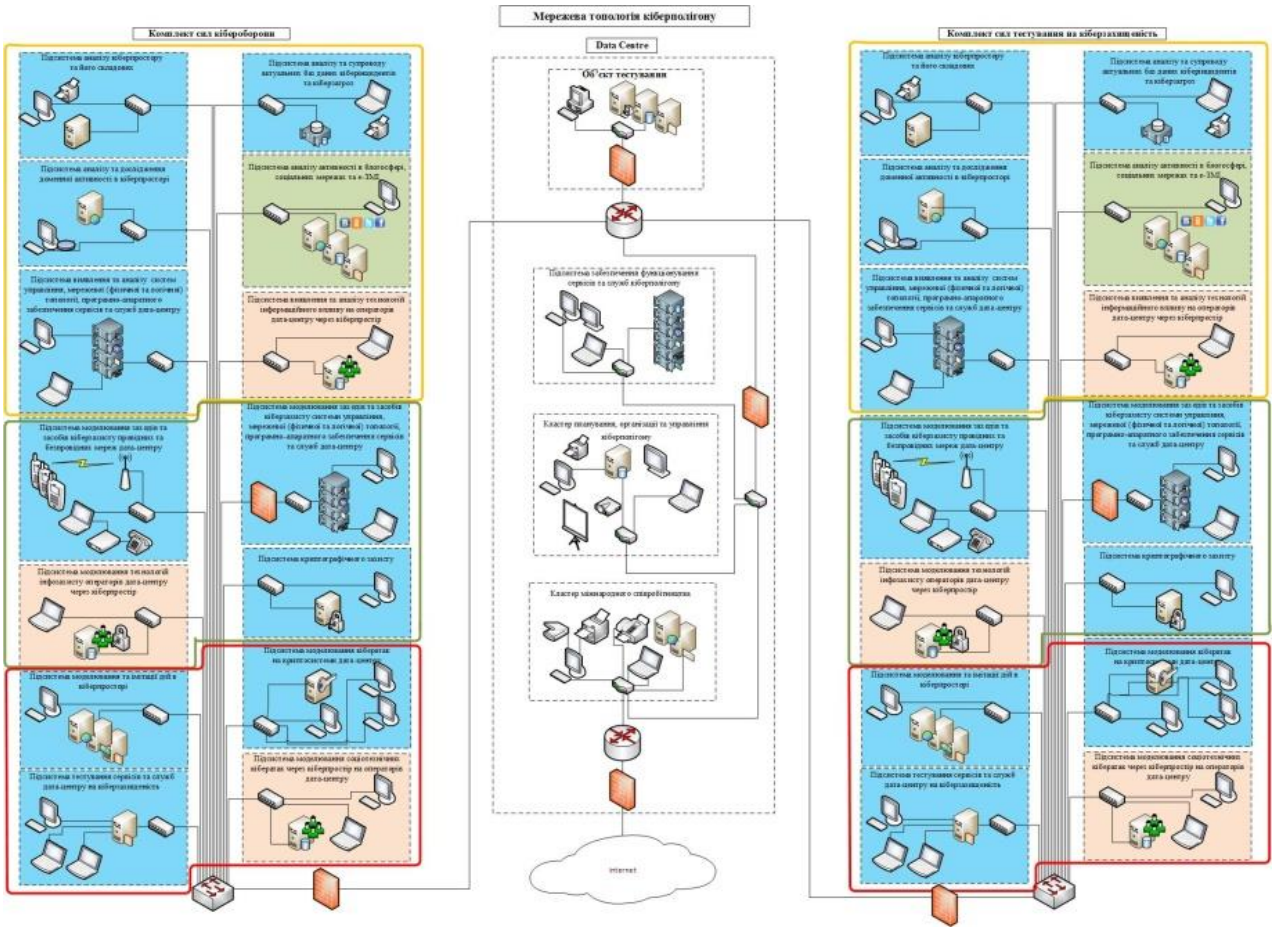


Рисунок 1.5 – Мережева топологія кіберполігону

1.4 Висновки до розділу 1

З кожним роком кіберзлочинці удосконалюють тактики та техніки для проведення атак. Вони використовують поділ праці, залучаючи для різних етапів атаки спеціалізовані команди хакерів або купуючи “доступ як послугу” у професійних зломщиків. У хід йдуть уразливості нульового дня та витончена соціальна інженерія.

“Кіберполігон” містить множину регулярно поновлюваних машин з логічними вразливостями, щоб ви завжди знаходилися на піку форми. Вони призначені для всіх, хто цікавиться навичками пошуку та експлуатації вразливостей, розробки експлойтів, виявлення та запобігання атакам.

На відміну від теоретичних занять і тренінгів, в процесі експлуатації Кіберполігону фахівці глибоко зрозуміють методи, які використовуються

передовими групами хакерів і навчаться їм протистояти на практиці. Проводиться реальна демонстрація та навчання протистоянню атакам із самого початку: проникнення в периметр ззовні, потім просування через мережу та підвищення привілеїв.

РОЗДІЛ 2. РОЗРОБКА КОНЦЕПЦІЇ РОЗГОРТАННЯ КІБЕРПОЛІГОНУ

2.1 Аналіз інфраструктури кіберполігону

Концептуально інфраструктура кіберполігону повторює в собі підприємств різних галузей, що повторюють типові інфраструктури. Типова схема мережевої інфраструктури умовного великого підприємства чи корпорації – це досить стандартний набір серверів, робочих комп'ютерів та різних мережевих пристроїв з типовим набором корпоративного ПЗ та систем інформаційної безпеки. Галузевий кіберполігон – це все те саме плюс серйозна специфіка, що різко ускладнює віртуальну модель. Але важливим моментом є те, що при створенні концепції індустріальної частини кіберполігону потрібно детально проаналізувати та вирішити який з обраних методів моделювання складної кіберфізичної системи. Основними можна назвати три підходи моделювання [6–8, 15]:

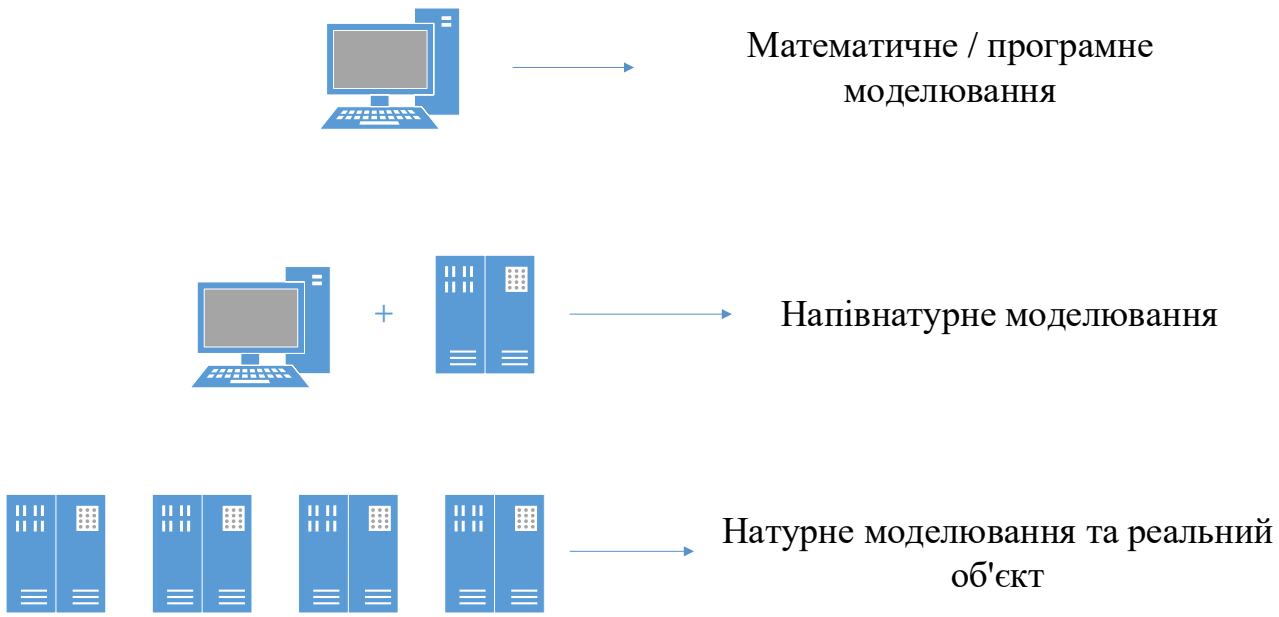


Рисунок 2.1 – Методи моделювання індустріальної інфраструктури кіберполігону

Кожен з цих підходів має свої переваги та недоліки. У різних випадках, залежно від кінцевої мети та наявних обмежень, можуть застосовуватися всі три

зазначені вище способи моделювання. Для того, щоб визначити який з методів може підійти найбільше, пропонується такий алгоритм [6, 8, 15]:

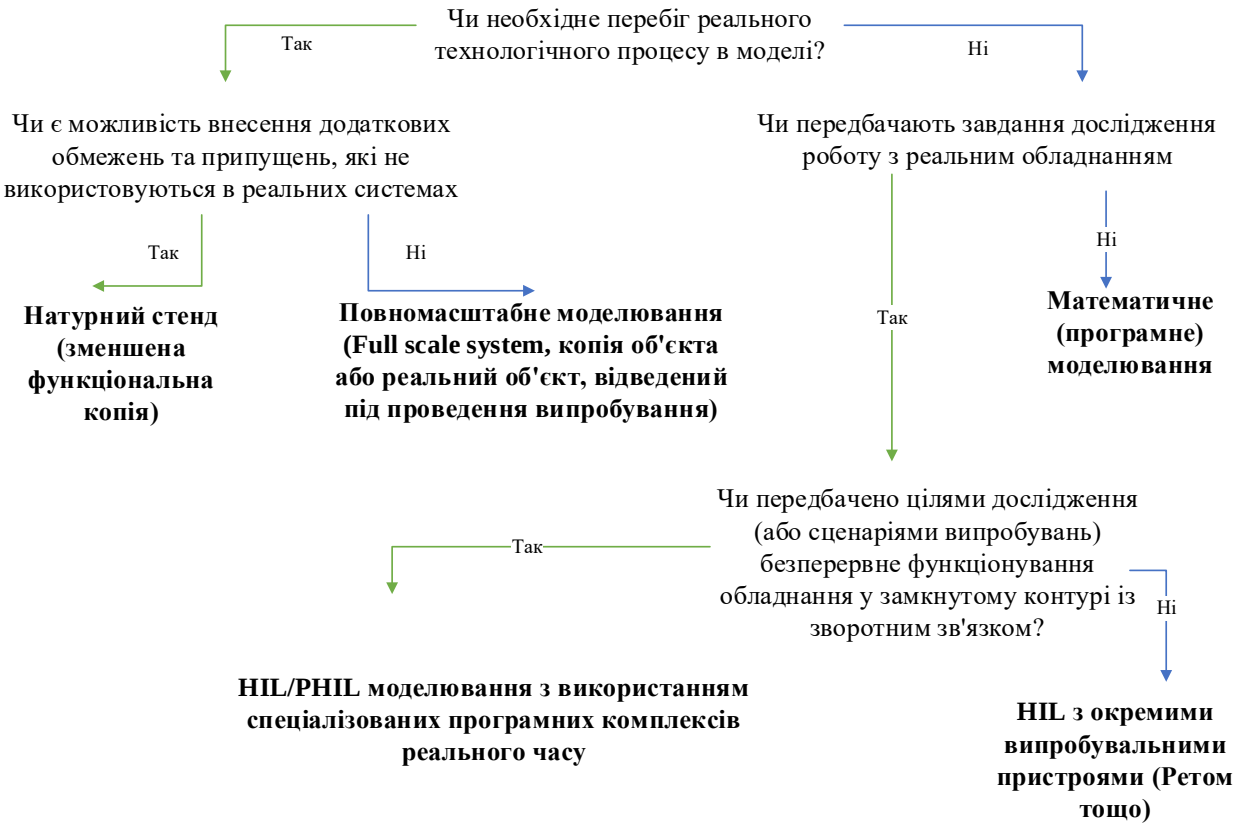


Рисунок 2.2 – Алгоритм формування методів моделювання інфраструктури кіберполігону

При формуванні потрібно обрати пріоритет направлення. Якщо це охоплення областей дослідження, тоді найкраще за все підійдуть Математичні моделі, ПО. Але якщо потрібно більш точне моделювання та ступінь співвідношення моделі реальної системи, то краще за все підійде «Натурний стенд» або «Реальний об’єкт». Проте є третій варіант, коли потрібно обрати дві області одразу. Таким чином, оптимальним за співвідношенням точності та гнучкості моделювання є так зване напівнатурне моделювання (hardware-in-the-loop, HIL).

У межах такого підходу кіберфізична система частково моделюється з допомогою реального устаткування, а частково – з допомогою математичних моделей. Наприклад, електрична підстанція може буде представлена реальними

комплексами пристроїв, призначених для швидкого, автоматичного виявлення та відокремлення від електроенергетичної системи пошкоджених елементів, також серверами автоматизованих систем управління та іншим вторинним обладнанням, але самі фізичні події, які виконуються в самій електричній мережі – реалізовані за допомогою комп'ютерної моделі. Попри все це, це лише перший і найнижчий рівень, до якого відноситься так зване "первинне обладнання" – це оптоволокно, електрична мережа чи ще щось – залежно від галузі. Воно обмінюється даними та управляється спеціалізованими промисловими контролерами, а ті, своєю чергою, SCADA-системами. Звичайно, на початку створення першого рівня неможливо реалізувати через натурне моделювання з використанням реальних об'єктів. Тому найкращим варіантом буде використання математичної моделі [14–15].

Ця модель включає все силове обладнання підстанцій – лінії електропередачі, трансформатори й так далі, і виконується в спеціальному програмному комплексі RSCAD. За підсумком «жива» ділянка електроенергетичної системи, що функціонує за всіма законами фізики й навіть реагує на зовнішні впливи (наприклад, спрацювання терміналів релейного захисту та автоматики, відключення вимикачів тощо). Взаємодії із зовнішніми пристроями вдалося домогтися за допомогою спеціалізованих інтерфейсів зв'язку, що налаштовуються, що дозволяють математичній моделі взаємодіяти з рівнем контролерів і рівнем автоматизованих систем.

А ось вже самі рівні контролерів та автоматизованих систем управління енергооб'єкту можна створювати за допомогою реального промислового обладнання (хоча, за потреби, ми можемо також використовувати віртуальні моделі). На двох даних рівнях розташовуються, відповідно, контролери та засоби автоматизації (РЗА, PMU, УСПД, лічильники) та автоматизовані системи управління (SCADA, ОВК, АІІСКУЕ). Натурне моделювання дозволяє значно підвищити реалістичність моделі і, відповідно, самих кібернавчань, оскільки команди взаємодіятимуть із реальним промисловим обладнанням, яке має свої особливості, баги та вразливості [15].

Та на третьому етапі об’єднати взаємодію математичної та фізичної частин моделі за допомогою спеціалізованих апаратних та програмних інтерфейсів та підсилювачів сигналу.

Якщо зібрати опис усіх трьох рівні, тоді інфраструктура матиме такий вигляд [15]:

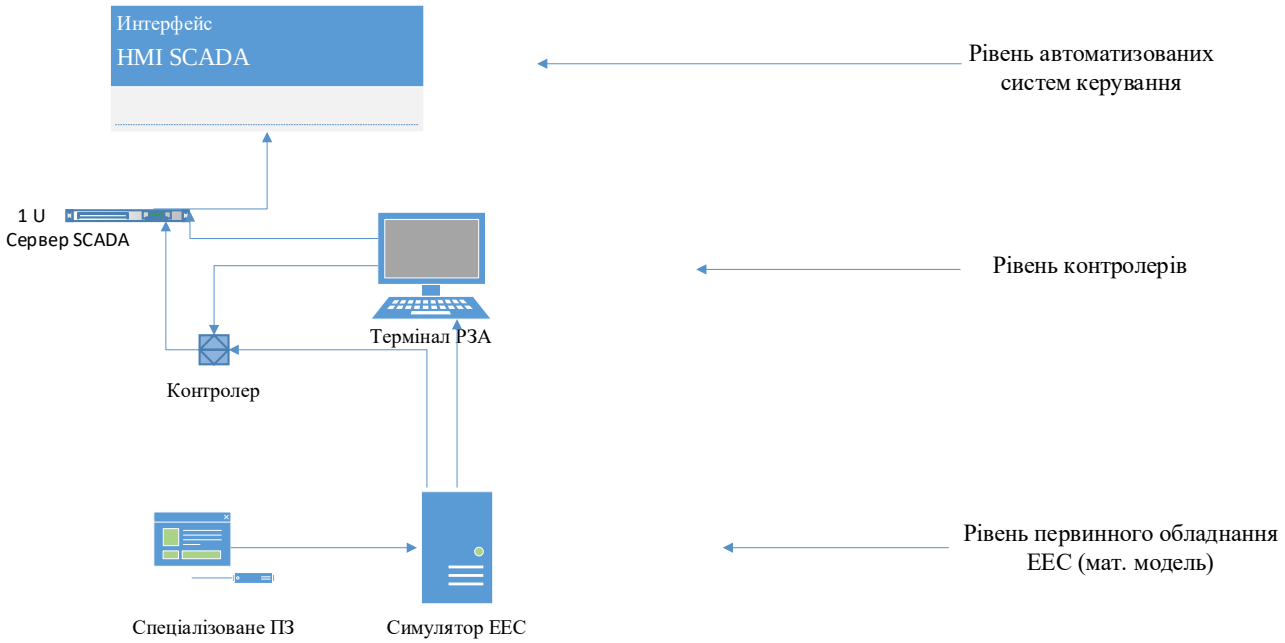


Рисунок 2.3 – Рівні формування інфраструктури кіберполігону

Усі обладнання полігону взаємодіє між собою так само як і у реальній кіберфізичні системі. Якщо розглянути це більш предметно, то під час створення даної моделі можна використати наступні обладнання та обчислювальні засоби [14–15]:

1. Обчислювальний комплекс RTDS щодо розрахунку «в реальному часі»;
2. Автоматизоване робоче місце (АРМ) оператора із встановленим програмним забезпеченням для моделювання технологічного процесу та первинного обладнання електричних підстанцій;
3. Шафи з обладнанням зв’язку, терміналами РЗА та обладнанням АСУ ТП;
4. Шафи підсилювачів, призначені для посилення аналогових сигналів із плати цифро-аналогового перетворювача симулятора RTDS. Кожна шафа

підсилювачів містить різний набір блоків посилення, що використовуються для формування вхідних сигналів струму та напруги для досліджуваних терміналів РЗА. Вхідні сигнали посилюються рівня, необхідного для нормальної роботи терміналів РЗА.

Даний варіант не є єдиним рішенням, але це один з оптимальних для проведення кібернавчання, оскільки відбиває реальну архітектуру абсолютної більшості сучасних підстанцій, і навіть її можна кастомізувати те, щоб максимально точно відтворити якісь особливості конкретного об'єкта.

2.2 Аналіз сучасних загроз в складових безпеки інформації

В умовах стрімкого зростання обчислювальних ресурсів та розширення спектру цифрових послуг у сучасних кіберполігонах повинні відпрацьовуватись завдання, пов'язані з загрозами на об'єкти критичної інфраструктури, системи Інтернет-речей та інтегровані в кіберфізичні системи їх елементи.

У табл. 2.1 наведені порівняльні результати співвідношення секторів держави до КІ [6].

Таблиця 2.1 – Порівняльна таблиця критичних інфраструктур

ДЕРЖАВА / СЕКТОР КРИТИЧНОЇ ІНФРАСТРУКТУРИ	Велика Вісімка															
	США	Японія	Німеччина	Великобританія	Франція	Італія	Канада	Російська федерація	Австралія	Австрія	Нідерланди	Нова Зеландія	Норвегія	Польща	Фінляндія	Швеція
Банки і фінанси	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Водопостачання	■	■	■	■	■	■	■		■	■	■		■	■	■	
Дамби	■															
Енергетика	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Комунальні мережі			■						■	■			■		■	
Національні символи	■						■			■						
Небезпечні матеріали (Х, Б, Р, Я)	■	■		■			■							■		
Оборонно-промисловий комплекс	■	■			■		■	■	■						■	
Органи виконавчої влади	■		■	■			■		■		■	■	■	■		■
Органи судової влади	■															
Охорона здоров'я	■	■	■	■	■	■	■		■	■	■		■	■		■
Паливно-енергетичний комплекс	■	■	■	■	■	■	■	■	■		■	■	■	■		
Поштові служби	■									■						
Сільське господарство	■	■	■	■			■		■		■			■	■	
Система управління повітряним рухом																■
Служби охорони громадського руху				■	■	■	■	■	■	■	■		■			
Служби екстреної допомоги та реагування на НС	■	■	■	■		■	■		■	■		■	■			
Телекомунікації	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Транспорт	■	■		■	■	■	■	■	■	■	■	■	■	■	■	
Управління відходами		■		■		■	■		■				■			

Проведений аналіз табл. 2.1 показав, що для великої кількості держав найвразливішими об'єктами критичної інфраструктури є енергетика, перекомунікації об'єкти фінансової сфери. На основі результатів аналізу [16] пропонується ієрархічна структура критичної інфраструктури метасистеми держави, яка наведена на рис. 2.4.

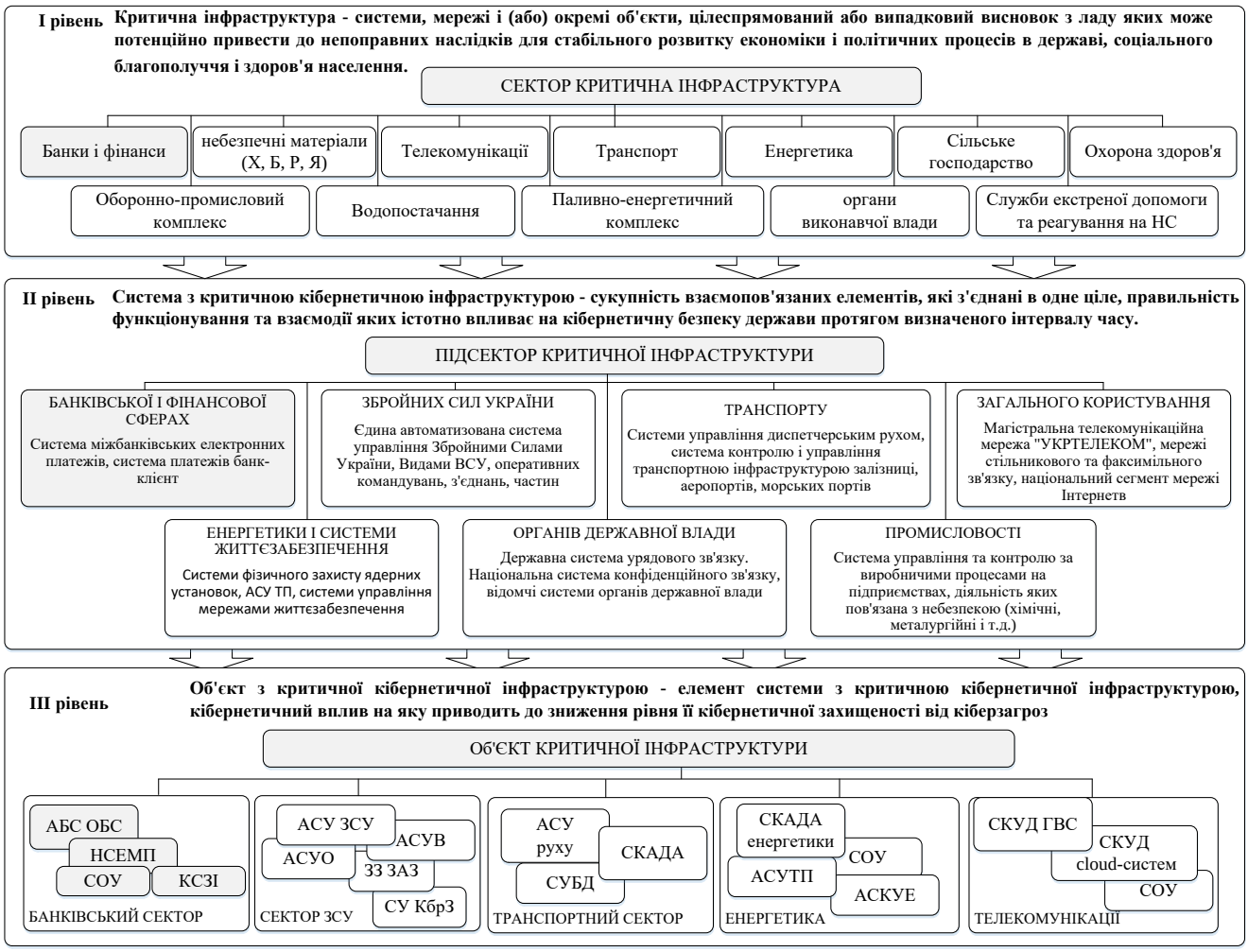
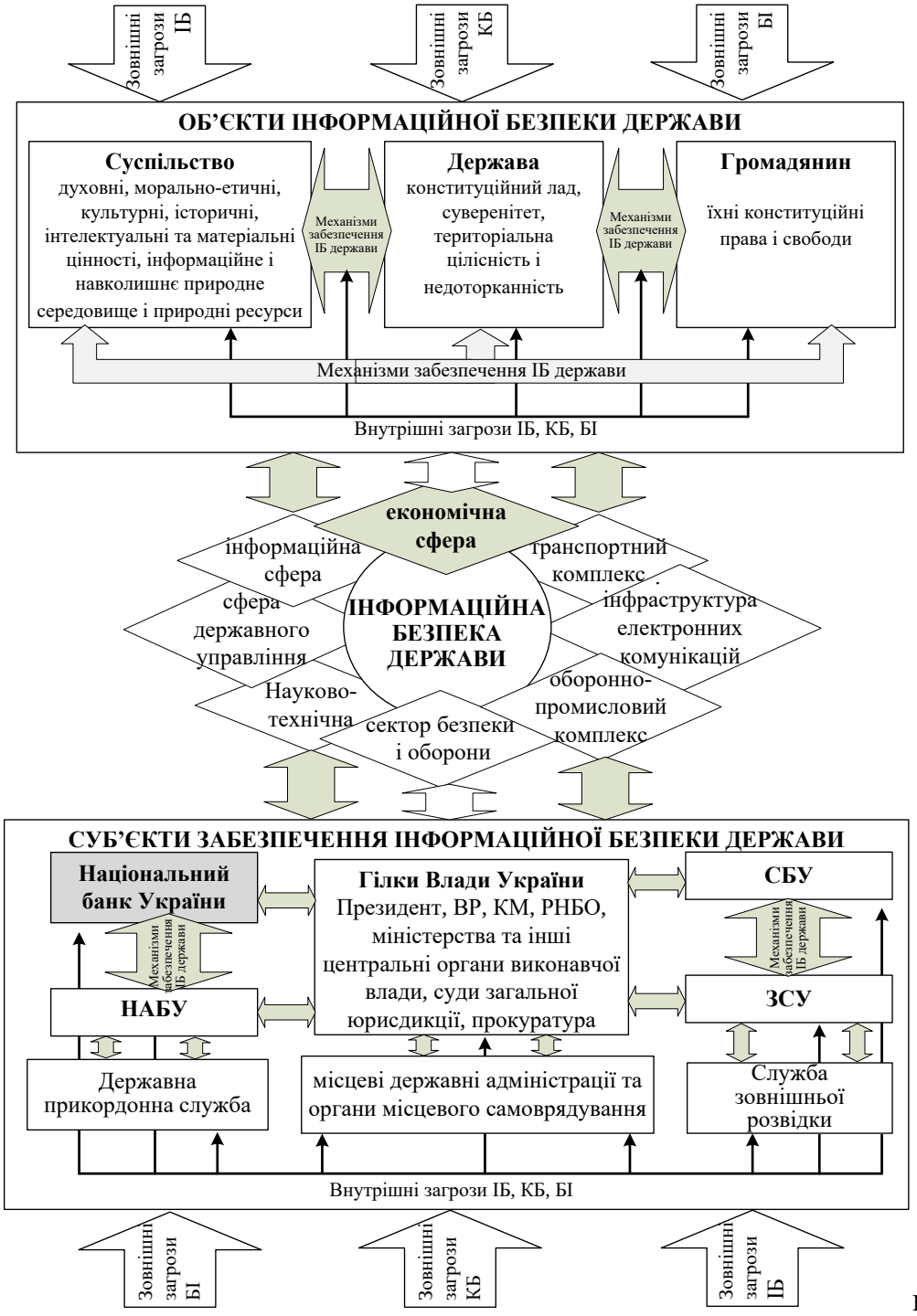


Рисунок 2.4 – Ієрархічна структура критичної інфраструктури метасистеми держави

На рис. 2.5 наведений взаємозв’язок між основними складовими інформаційної безпеки (ІБ) держави.



и.

Рисунок 2.5 – Взаємозв'язок основних складових інформаційної безпеки держави

Основні загрози безпеці інформації БІР у банківській сфері, описано так [17]:

1. Порушення конфіденційності: несанкціоноване введення даних та передача конфіденційних даних, неправильні твердження про платіжну документацію, моніторинг трафіку, щоб знайти протоколи обміну, фальсифікація платіжних

документів, претекстінг, фішинг, скрімінг, фармінг - методи соціальної інженерії для отримання конфіденційних даних, тощо.

Порушення цілісності даних можуть включати такі дії: несанкціоноване копіювання інформації з магнітних носіїв; використання робочого терміналу, який залишений без нагляду, для доступу і копіювання даних; зміна даних та програми на різноманітних носіях інформації, для того щоб підробити фінансові документи в неробочий час, підміна, знищення обладнання або інформації.

Існують ще зовнішні і внутрішні загрози в інформаційній безпеці БІР, а це в свою чергу впливає як на банк так і на працюючий персонал і обслуговуючих клієнтів. Взалежності від різноманітної діяльності окремих об’єктів та суб’єктів, зовнішні і внутрішні загрози також поділяються на інтелектуальні, економічні, та фізичні [18–19].

До економічних загроз відносять шахрайство, корупційні схеми, недобросовісна конкуренція, і т.д. Ці всі дії призводять до збитків банківським системам, а також втрати прибутків.

Щодо фізичних загроз, то це стосується пограбування, привласнення чужих коштів банків, виведення з ладу обладнання банків. При реалізації цих і похожих їм загроз банки зазнають величезних збитків: втрата власності та додаткові затрачання коштів, для того щоб відновити різноманітні матеріальні засоби.

Тепер розглянемо інтелектуальні загрози. Це дискредитація банку на ринку банківських послуг, розголошення банківської інформації, а також її неправомірне використання, соціальні конфлікти. Врезультаті виникає соціальна або психологічна напруженість в колективах установ, а також навколо самих банків, погіршуючи їх імідж, а це призводить до збитків.

Кібербезпека включає в себе захист персональних даних, що пересікається з мережевою безпекою, Інтернет-безпекою та безпекою критичних інформаційних інфраструктур (рис. 2.6).

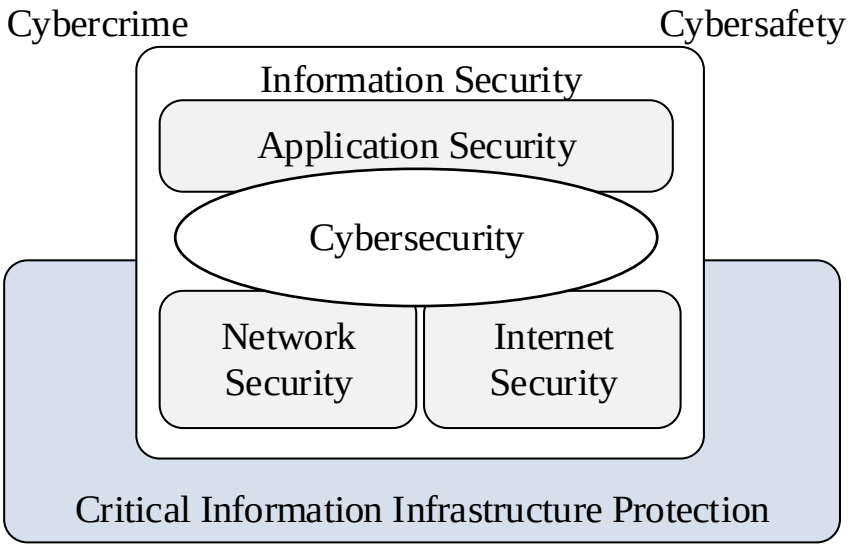


Рисунок 2.6 – Логічні взаємозв’язки кібербезпеки та інших доменів безпеки згідно зі стандартом ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

Аналізуючи результати оцінки кількості кібератак, а також враховуючи співвідношення рівнів складності програмного забезпечення та технічної кваліфікації зловмисників, отриманих від компаній, таких як "Arbor Networks" [20], CISCO [21] можна зробити висновок, що чим швидше буде рости кіберзлочинність тим швидше відбудеться зростання складних кібератак на периферійне мережеве обладнання.

Підводячи висновки з результатів досліджень [6, 20–34] можна об'єднати кібератаки в чотири основні класи. Їх суть відображається на рис. 2.7.

Рисунок 2.7 – Класифікація кібератак на АБС з прив’язкою до моделі OSI

Дана класифікація показує, що кібератаки різних класів виконують конкретні завдання впливу на БІР, але при цьому незалежать від функціонального призначення і можуть знаходитись на різних рівнях моделі взаємодії відкритих систем OSI.

Аналізуючи описані загрози, для покращення ефективності систем безпеки БІР, педставляю новішу модель загроз безпеці БІР, як отримала назву - синергетична модель (рис. 2.8).

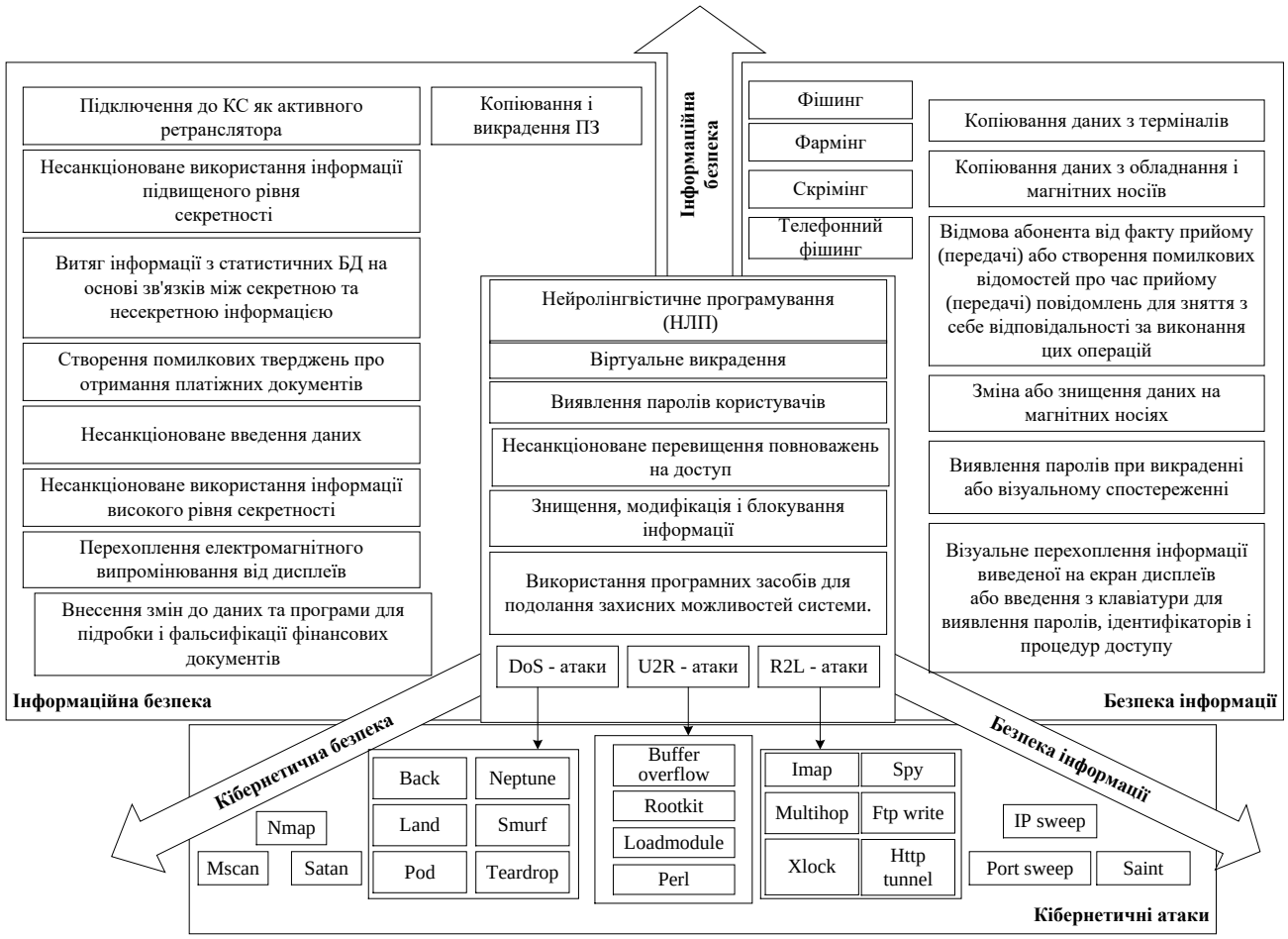


Рисунок 2.8 – Синергетична модель загроз безпеці БІР

Переваги синергетичної моделі, яка представлена на рис.2.8, є наявність логічних зв'язків, які виникають між загрозами на різних рівнях безпеки. Тому ця модель забезпечує важливо необхібні умови, що успішно розробити новий методологічний базис, гарантуватиме безпеку як для державних так і для приватних систем захисту банків.

Основні загрози систем Інтернет-речей та елементів інфраструктури кіберфізичних систем представлені на рис. 2.9.

Відповідно до стандарту ISO/IEC 27001:2013 загрози поділяються на навмисні, випадкові та/або екологічні.

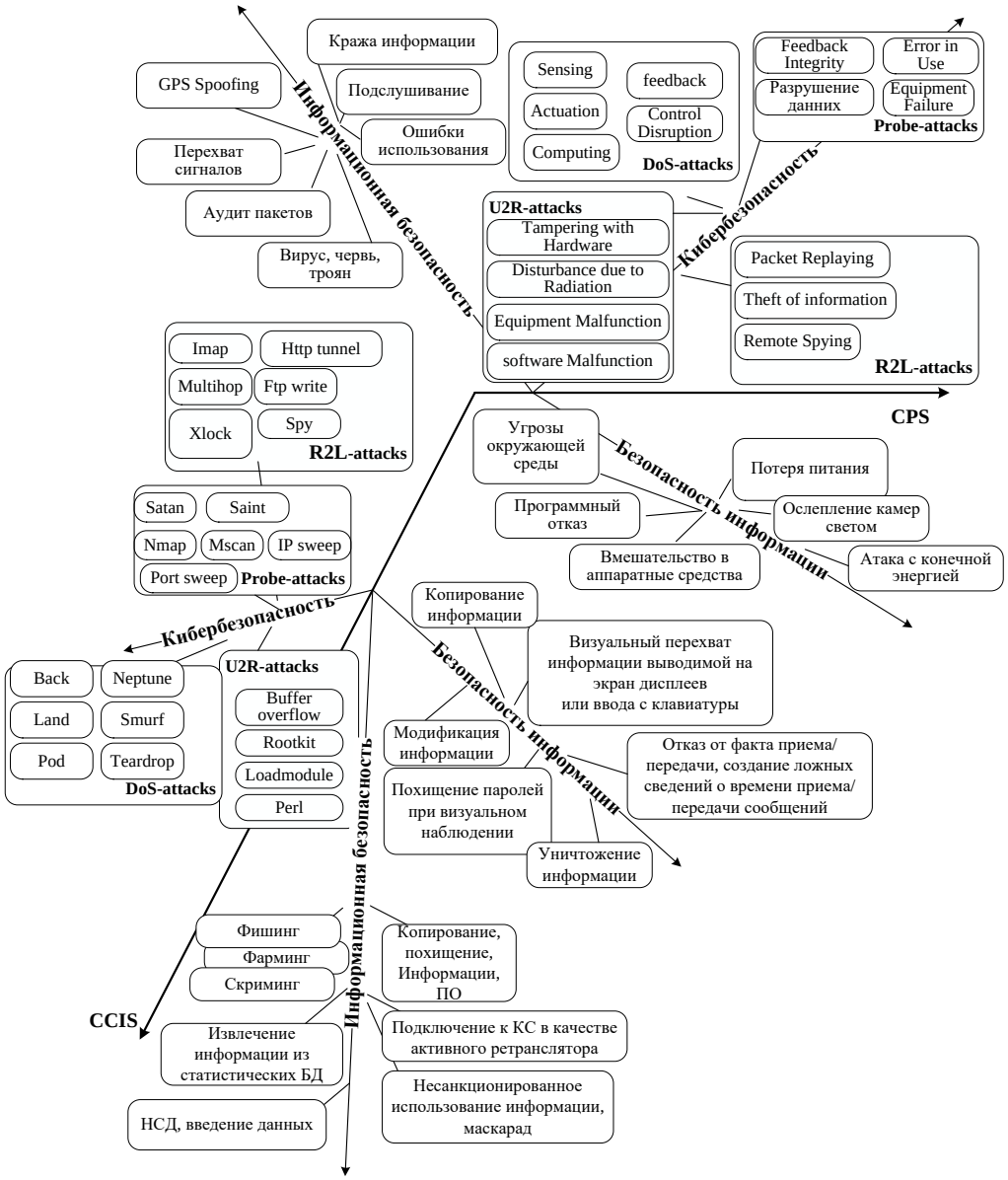


Рисунок 2.9 – Структурна схема синергетичної моделі загроз синтезу на CCIS та CFS

Таким чином, типовими прикладами можуть бути технічні зброї, несанкціоновані дії, втручання в програмне забезпечення, фізичні збитки, компрометація функцій тощо. Однак, стандарт, як і інші нормативні міжнародні акти, не розглядає синергію та гібридність сучасних загроз, їх комплексування з методами соціальної інженерії, що суттєво підвищує ризик реалізації загрози.

2.3 Принципи формування задач, вихідної інфраструктури до відпрацювання у кіберполігоні

Підготовку фахівців з ІБ у сучасних умовах відрізняють два пов'язані між собою фактори [32]:

1. Конвергенція цілей ІБ від протистояння загрозам створення систем, які забезпечують збереження повномасштабного функціонування інформаційних систем за умов постійно діючих комп’ютерних атак. Необхідність докладного вивчення механізмів реалізації загроз, вразливостей, тестування проникнення тощо.

2. Ігровий характер протистояння засобів захисту та загроз у кіберпросторі, що піддається моделюванню з використанням технологій віртуалізації та мережевих полігонів. Технології віртуалізації дозволяють за відносно невеликих витрат створювати адекватні макети реальних систем і здійснювати моделювання кіберпротиборства.

При цьому загальнотеоретична підготовка фахівців з ІБ повинна базуватися на таких галузях знань:

- управління інформаційною безпекою: методи організації адаптивної динамічної системи зі стохастичними характеристиками, адаптивне керування з використанням штучного інтелекту;
- криптографічний захист: гомоморфна криптографія, розподілені постквантові криптоалгоритми, криптографічний захист у децентралізованих розподілених самоорганізованих мережах, блокчейн;
- безпека великих даних: принципи роботи з великими даними, захищені системи інтелектуального збору та перед обробки неструктурованих даних, аналіз даних у хмарних системах та на гетерогенному обчислювальному кластері, застосування гомоморфної криптографії для обробки великих та надвеликих масивів даних, методи динамічного керування навантаженням;
- кіберстійкість систем управління цифровим виробництвом: методи забезпечення глобальної довіри та кіберстійкості, методи глибокого навчання для

виявлення вразливостей у програмному забезпеченні, аналізу шкідливих програм, розпізнавання мережевих атак, виявлення бот-мереж та кібершахрайства.

Такий підхід забезпечує формування основних завдань, які мають вирішуватись у класах кіберполігону [12]:

- лабораторна база для передачі, відпрацювання та закріплення навичок дії;
- проведення фундаментальних, прикладних та пошуково-експериментальних досліджень у галузях захисту інформації, кібербезпеки та кіберстійкості;
- оцінка ефективності систем з урахуванням вимог їх функціональності, стабільності та захищеності;
- організація у режимі реального часу моніторингу стану технічного та інших видів забезпечення розроблюваних чи наявних систем з можливістю прийняття рішень щодо усунення виявлених негативних ситуацій;
- організація та забезпечення функціонування систем комплексного захисту на основі технічних, програмних, організаційних та інших методів захисту для забезпечення необхідного рівня стійкості та функціональності;
- реалізація методів та методик інтелектуальної підтримки прийняття рішень в умовах нечіткості та слабкої структурованості;
- забезпечення оптимізації, оперативного управління, моніторингу та контролю, прогнозування та оцінки запропонованих рішень при формуванні керуючих впливів у ході функціонування захищених систем та ПЗ.

Виходячи із завдань, визначимо основні принципи формування завдань та вихідних даних [12]:

- формування завдань у сфері електроенергетики. Необхідність підключення кіберполігону до промислового сегмента дозволить створити єдину інфраструктуру, що імітуватиме типовий пристрій організацій паливно-енергетичного комплексу;
- інтеграція істотно розширить технологічні можливості та дозволить проводити більш масштабні навчання з максимальною реалістичністю досліджуваних процесів. Об’єднання сценаріїв атак та їх показ на єдиному

майданчику сформує перелік загроз, з якими можуть зіткнутися промислові підприємства. Такий досвід буде корисним для посилення інформаційної безпеки окремих компаній та розширення загальної бази кіберполігону;

- формування завдань для кібернавчань, що охоплюють відпрацювання всіх ключових процесів служб інформаційної безпеки – від аналізу захищеності та вибудовування системи комплексної безпеки інфраструктури до виявлення та відбиття хакерських атак;

- створення кіберполігону реалізується з використанням хмарних технологій, що дозволяє його використання не лише для навчання та тренування студентів, а й спеціалістів/експертів різного профілю, керівників у галузі інформаційної безпеки та інформаційних технологій сучасним практикам забезпечення безпеки.

Кібернавчання – це чудова можливість об'єктивно оцінити рівень своїх компетенцій та відпрацювати практичні навички реагування на інциденти інформаційної безпеки, а формат змагання додав до них елемент азарту [6]. Важливо, що під час заходу відпрацьовувалися сценарії, близькі до життя, релевантні для промислових підприємств. Кібернавчання можна формувати та проводити за окремими сценаріями. Наприклад, у перший день кібернавчань команди мали провести максимально повну інвентаризацію інфраструктури, спеціально створеної на базі промислового сегмента кіберполігону.

Потім їм необхідно було виконати пошук вразливостей у ній та налаштувати джерела подій у SIEM-системі. На даному етапі оцінюється повнота та точність даних від кожної команди. На другий день команди протистоять цілеспрямованим атакам, і на цьому етапі ключовим показником може стати швидкість виявлення інциденту та реагування на нього. За підсумками кожної атаки команди повинні подати звіти з описом як ланцюжка кроків зловмисника, так і заходів, необхідних для того, щоб уникнути повторення інциденту.

В останній день кібернавчань підбиваються загальні підсумки, а також проводиться детальний аналіз сценаріїв навчальних кібератак і дій команд.

Таким чином, такий підхід дозволяє забезпечити формування національного (інтегрованого) центру проведення не лише відпрацювання окремих завдань, а й комплексних навчань, спрямованих на підвищення рівня кібер- та інформаційної безпеки персоналу та студентів спеціальності.

2.4 Висновки до розділу 2

Проведений аналіз загроз дозволяє сформувати необхідні вихідні данні щодо визначення основних напрямів відпрацювання превентивних заходів щодо протидії сучасним комплексованим загрозам з ознаками синергізму та гібридності.

Такій підхід дозволяє сформувати не тільки основні напрямки загроз, а також забезпечити навчання реальними сценаріями нападу на об’єкти критичної інфраструктури, що дозволяє не тільки визначити їх структуру та класифікацію, цільові атаки на їх елементи інфраструктури, а також забезпечити виконання вимог міжнародних та національних регуляторів, щодо формування відповідних елементів системи захисту інформації.

РОЗДІЛ 3. РОЗГОРТАННЯ КІБЕРПОЛІГОНУ В УНІВЕРСИТЕТІ

3.1 Розгортання елементів інфраструктури кіберполігону університету

При розгортанні кіберполігону в університеті, можна залучитись до його побудови на базі кластеру віртуалізації за технологією Proxmox Virtual Environment з використанням некомерційної ліцензії, котра цілком задовольняє навчальні потреби ВНЗ. Proxmox VE розроблено на базі Debian Linux, котрий являє собою вебінтерфейс до кластера віртуалізації. Використовуючи даний кластер ми одразу отримуємо можливість масштабування, а також дозволяє розгорнути сервери й побудувати віртуальну мережеву архітектуру на основі Linux-контейнерів LXC та віртуальних машин, які керуються гіпервізором KVM (інфраструктура Linux та Windows).

На цей час використовуючи у середовищі LXC є можливість лише тільки Linux машини будь-який дистрибутив, але він являється швидкою системою віртуалізації. Головною ідеєю LXC являється запуск ізольованих контейнерів, котра сильно впливає на безпеку самої віртуальної машини. Теоретично можливість того, що на одній віртуальній машині хакер скомпрометує систему віртуалізації та зможе отримати доступ до інших машин є, але на цей час тяжких фізичних вразливостей не було реалізовано на базі відповідних систем віртуалізації. Тому застосування систем віртуалізації є гарною практикою, тому що має такі переваги фактичної економії застосування комп’ютерних ресурсів, а також зручність керування IT інфраструктурою.

Інша технологія це віртуалізація Kernel-based Virtual Machine (KVM), котра застосовує рівень ядра ОС Linux, тому вона також має гарну швидкість на цій системі, одна KVM це повна віртуалізація яка дає змогу застосовувати у якості “гостьових” ОС будь-яку систему, наприклад на x64 платформі Intel сумісна, тому є можливість запускати Windows.

Нижче представлено приклад зовнішнього вигляду панелі управління Proxmox VE:

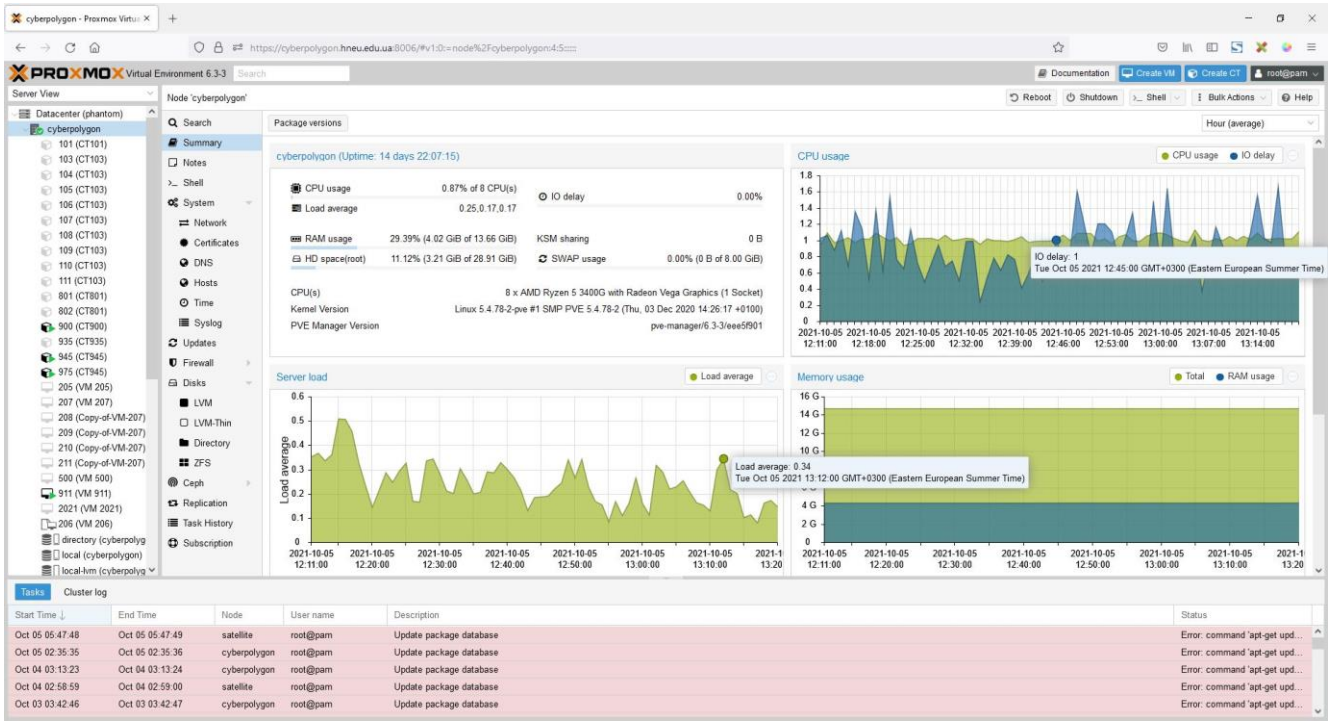


Рисунок 3.1 – Зовнішній вигляд панелі управління Proxmox VE

Під час використання Proxmox VE є можливість отримати доступ до інформації завантаження серверу та оперативної пам’яті. Також отримати безпосередньо доступ до командної строки ОС, а також налаштування, в котрому буде зображено підтримку фактично налаштування інфраструктури віртуального data-centre. Це значить, що в даній системі є можливість створення безліч віртуальних мережевих інтерфейсів та віртуальних мостів, наприклад Linux Bridge. На базі цих мереж є можливість побудови взаємодії між віртуальними машинами, що були запущені. Так само в панелі управління можна побачити яким чином застосуються ресурси відповідного серверу:

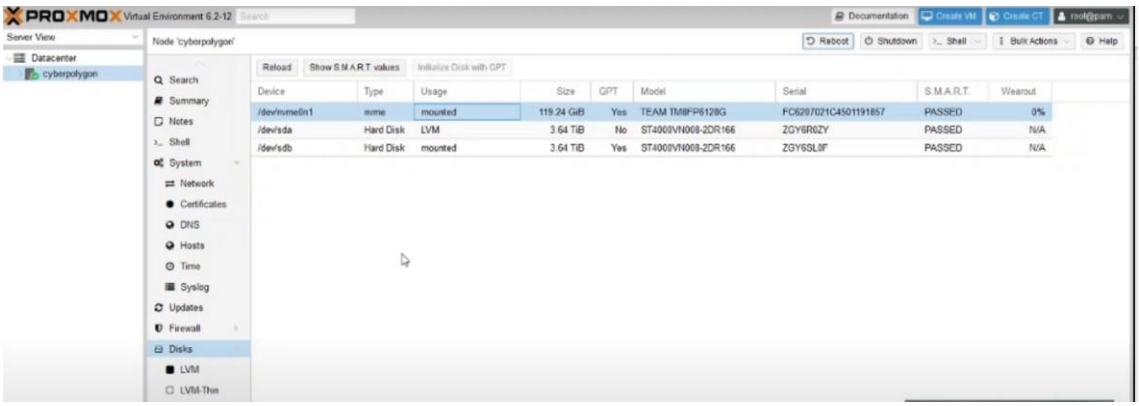


Рисунок 3.2 – Інформація в панелі управл. про завантаженість ресурсів серверу

Також завдяки тому, що сервер має два фізичних інтерфейси отримати доступ до ресурсів навчального класу, в якому також розгорнуті на базі технології віртуалізації VirtualBox, котрий допоможе з роботою як з операційними системами родини Windows, так і з ОС Linux.

Апаратну платформу кіберполігону побудовано на основі двох потужних серверів: ASUSTeK: TUF B450M-PLUS, 8 x AMD Ryzen 5, 16 GB RAM, 2 x 4TB HDD + 120 GB SSD; Supermicro: X9DRi-LN4+, 24 x Intel Xeon E5-2620 (2 Socket), 32 GB RAM, 4TB HDD + 2 TB Raid 1. Для організації гнучкої інфраструктури віртуальних мереж кіберполігону залучені: 24-портовий комутатор, який керується; маршрутизатор з бездротовою точкою доступу (Wi-Fi) та програмні рішення рівня мережевого маршрутизатора, що розгорнуто, як звичайні віртуальні машини. Апаратну складову кіберполігону фізично побудовано на базі 19"-стойки, під'єднано до системи резервування живлення та загальної мережі ЗВО та Інтернет.

Серверна інфраструктура є доступною з зовні мережі кампуса та дозволяє виконувати лабораторний практикум віддалено. Завдяки гнучкої побудови мережевих комунікацій віртуальні сервери можуть бути ізольовані від загальної мережі ЗВО. Також до складу кіберполігону входить комп’ютерний клас, який складається з 12 сучасних робочих станцій рівня Intel i5, 8GB RAM, 2 TB HDD. Комп’ютерний клас, поруч із кластером віртуалізації дозволяє побудувати різноманітні практичні завдання лабораторного практикуму та сприяє ефективному виконанню наукових досліджень за напрямом спеціальності 125 – Кібербезпека.

В результаті підключення усіх апаратних та системних технологій, можна отримати дану схему:

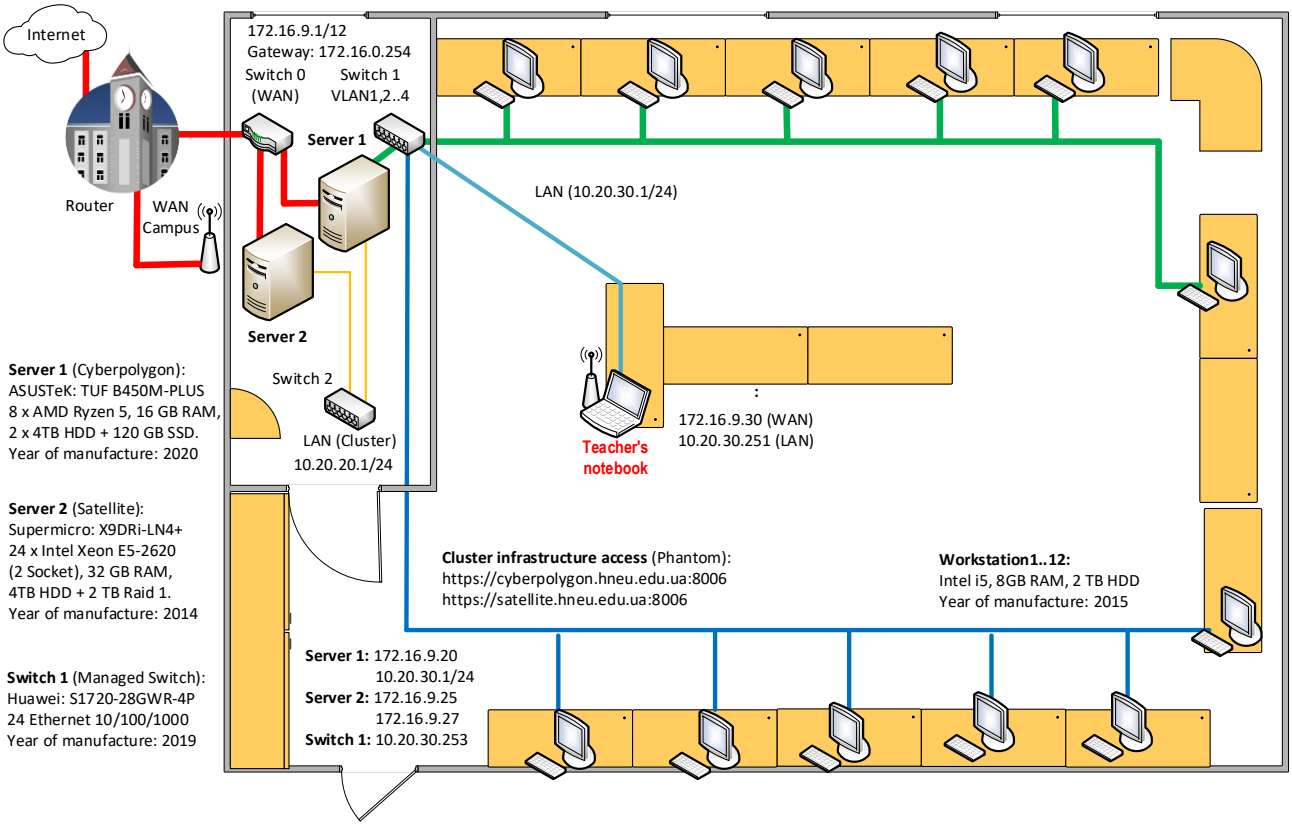


Рисунок 3.3 – Схема підключення апаратної платформи кіберполігону

3.2 Розробка рекомендацій задач, які відпрацьовуються у кіберполігоні

Перш за все кіберполігон являє собою сукупність спеціалізованих програмно-апаратних комплексі, що об’єднані провідними й безпровідними комунікаціями, інтегрованими у мережу Інтернет, які застосовуються для здійснення моніторингу, впливу на системи управління об’єктів, що становлять інтерес, а також захисту власних систем управління від аналогічних дій протиборчої сторони, підвищення рівня підготовки спеціалістів у виявленні кібератак та інцидентів ІБ. При формуванні:

Оволодіння теоретичної та практичної бази навичок у сфері кібер-фізичних систем

Практичні завдання за темою Інтернет-речей, та який вплив має в сучасному світі технологія Blockchain

Об’єкти критичних інфраструктур на державному рівні

Перше, це кіберфізичні системи. Поняття доволі комплексне, котре містить взаємодію між обчислювальними процесами та процесами фізичними, тому можна. сказати,. що кібер-фізична система об'єднує в собі різні елементи, завдячи чому на постійній основі одержує інформацію навколишнього середовища, яка на далі оприміzовує управлінські процеси. Важливо відзначити, що кібер-фізичні системи схожі по архітектурі з інтернетом речей і можуть використовувати його елементи для зв'язку або отримання даних, але по суті вони набагато складніше, тому ставити знак рівності тут було б некоректно [38].

Для прикладу, та компанія, як Toshiba у своєму проєкті віртуальної електростанції взяла за основу принцип кібер-фізичних систем. Також завдяки технології інтернету речей контрулює роботу розподілених джерел енергії (вітрової, сонячної, та водневої енергії), що споживають її електротранспортних систем та зберігання/накопичення енергії [38].

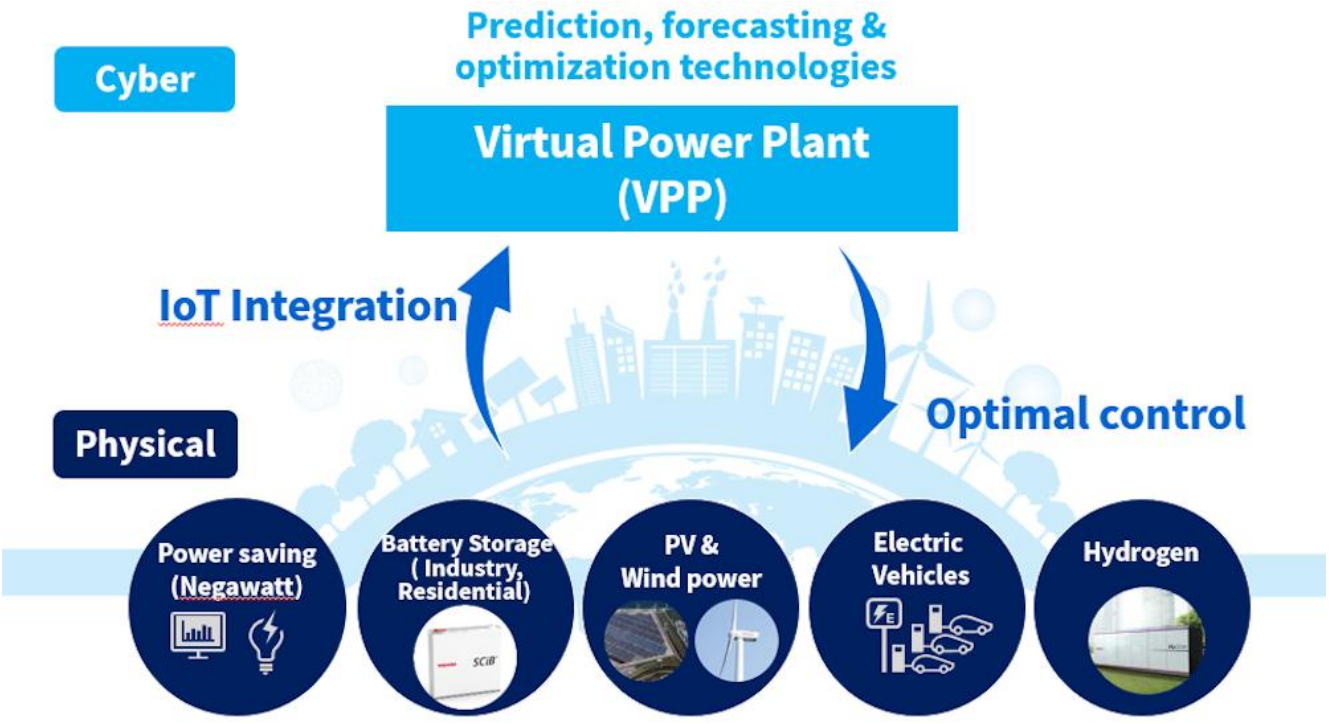


Рисунок 3.4 – Схема віртуальної електростанції Toshiba

Якщо існують кіберфізичні-системи, тоді на них є кіберфізичні атаки, котрі становлять особливу категорію кібератак, які навмисно чи ні також негативно впливають на фізичний простір, націлюючись на обчислювальну та комунікаційну інфраструктуру, що дозволяє людям та системам контролювати та контролювати датчики та виконавчі механізми. Кіберфізичні атаки зазвичай розглядаються у зв'язку з кіберфізичними системами та вразливістю їх обчислювальних та комунікаційних елементів. Наприклад, зловмисник, який взяв під контроль обчислювальні або комунікаційні компоненти водяних насосів, медичних імплантатів автомобілів і клапанів газопроводів, може використовувати їх для впливу на фізичний простір, завдаючи шкоди майну або навколишньому середовищу та наражаючи на ризик життя людей. У результаті безпека повсюдно сприймається як одне з найважливіших завдань під час проєктування надійних кіберфізичних-систем. Надалі мета полягає в тому, щоб отримати більш глибоке розуміння загроз, з якими стикається інфраструктура кіберфізичних систем, а також визначити ймовірність і наслідки загроз для кіберфізичних систем [38].

Найбільш часто обговорюваними загрозами для промислових систем управління таких систем і пов'язаних з загрозами безпеки (перший розділ, SCADA-системи), найголовніше реальний приклад на сьогодні (Наступний розділ, “Стакснет”), і цільовий, який повсюдно розглядається як Святий Грааль, спонсоровані державою напади (в останньому розділі, електричної мережі). Ранні системи SCADA відрізнялися провідними панелями з лічильниками та кнопками, але по суті мали більшу частину функціональності, що спостерігається в сучасних системах, включаючи інтерфейс між людиною оператором та машиною, механізм зображення тенденцій у зібраних даних, набір сигналів тривоги, що вказують різні умови, та двосторонній зв’язок з RTU [38].

У минулому обробка, необхідна для більшості з них, виконувалася централізовано на одній головній станції, підключеної до RTU по виділених лініях, так званої монолітної (перше покоління, рисунок 3.5(1)). З того часу системи SCADA прийняли розподілену архітектуру (друге покоління, рисунок 3.5(2)), що включає кілька серверів, кожен із яких відповідає за свій аспект системи. Перехід

від пропрієтарних протоколів конкретних виробників до відкритих протоколів, які дозволяють використовувати компоненти COTS (готові апаратні та програмні технології відкритого типу), сприяє зміні архітектури (третє покоління, рисунок 3.5(3)). Зв'язок системи за допомогою локальних мереж дозволило працювати на великих географічних територіях та різноманітних мережевих інфраструктурах, включаючи глобальні мережі та Інтернет. У четвертому поколінні (рисунок 3.5(4)) систем SCADA наголошується на взаємопов'язаності та взаємодії різних технологій. Для контролю відображається повноцінне мережеве середовище пристроїв, що надсилають звіти безпосередньо через Інтернет і без необхідності в RTU та людино-машинних інтерфейсах (HMI), які не обмежені центральним місцем, але доступні з будь-якого місця через мобільні пристрої [38].

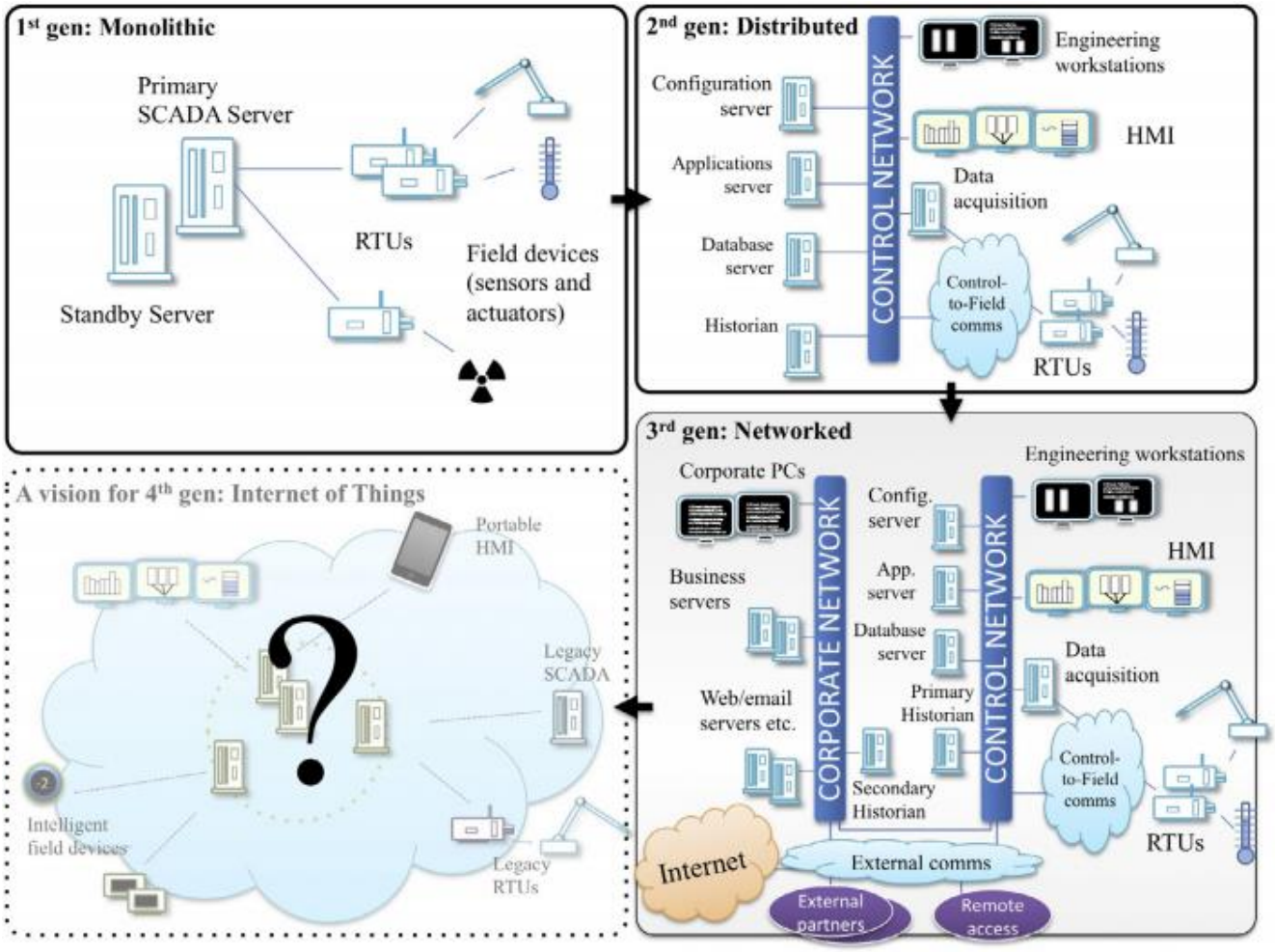


Рисунок 3.5 – Покоління SCADA та їх архітектура

З отриманих даних можна створити таблицю точок входу для атак на різні системи [38]:

Таблиця 3.1 – Точки входу для атак систем SCADA

Опис точки входу	Ймовірні атаки
Радіозв'язок між RTU/PLC та датчики/виконавчі механізми	Глушення зв'язку, подача команд, введення неправдивих даних
RTU/PLC та зв'язок з серверами SCADA	Впровадження коду / модифікація прошивки, зараження шкідливим програмним забезпеченням, відмова в обслуговуванні, глушіння, повторна атака, впровадження команди, введення неправдивих даних, чорна діра / сіра діра, ізоляція мережі, шахрайський вузол
Мережа управління, включаючи сервери SCADA та робочі місця інженерів	Зараження шкідливим програмним забезпеченням, відмова в обслуговуванні, посередник
Комунікаційний шлюз/канал між системою управління та корпоративною мережею (наприклад, з'єднання між первинним та вторинним архіватором)	Відмова в обслуговуванні, введення неправдивих даних (на основі бази даних)
Корпоративна мережа	Зараження шкідливим програмним забезпеченням, соціальна інженерія
Інтернет та мережі партнерів	Веб-атаки (шкідливе ПЗ, SQL-ін'єкції тощо), Соціальна інженерія

А також точки входу для атак на системи розумного дому [38]:

Таблиця 3.2 - Точки входу для атак на систему разумного дому

Опис точки входу	Ймовірні атаки
Мережа Wi-Fi та маршрутизатор Wi-Fi	Зламування паролів для Wi-Fi роутера, зніффінг пакетів, відмова в обслуговуванні, шахрайський вузол, глушення зв'язку
Додаток для смартфона або ПК для керування через Інтернет	Зламування паролів додатків для смартфонів або ПК, шкідливе ПЗ на смартфоні або ПК

Наступним класом являється вивчення систем інтернет-речей та технологій блокчейн. Інтернет-речі або як ще це називають *IoT-сегмент* – це тематично значуща частина Інтернету речей, яка виділена цільовим чином та пов'язана із заданою предметною областю. Для IoT-сегменту важливими є не тільки базові технології IoT, а й додаткові технології (методи та інструменти), які найкраще реалізують обрану тематику. Поняття IoT-сегменту стає важливим для конкретного бізнесу, який реалізує свою стратегію та орієнтований на конкретний сегмент ринку. Саме адаптація під цільові потреби клієнтів та способи задоволення таких потреб формують особливості, можливості та обмеження для предметної реалізації моделей бізнесу у рамках IoT-технологій. Поряд із досить широкими загальноприйнятими IoT-сегментами, кожен бізнес має право виділяти й позначати собі вужчі цільові сегменти. Однак, при цьому він має аналізувати тенденції та технології суміжних, пов'язаних чи залежних предметних напрямків Інтернету речей, які підтримуються та розвиваються лідерами ринку, галузевими бізнес-спільнотами, приватними та державними фондами та регуляторами. Розвиток бази та спектру сегментів Інтернету речей – це не поле для індивідуальної гри, а інформаційно-економічний простір, в рамках якого кожен із гравців ринку займає та реалізує вигідну позицію на основі активних конкурентних переваг, а не за допомогою пасивної монополізації даних, технологій, ресурсів і т.п.

Якщо у першому випадку вигоду від IoT отримує індивідуальний клієнт, то у другому випадку – група клієнтів, бізнес, спільнота, галузь загалом. Частково ґрунтуючись на цьому, ряд експертів прямо поділяє Інтернет речей на «споживчий» та “індустріальний”, позначаючи два незалежні напрямки. Однак, вибір між IoT для персонального споживання та для ділового (соціального) використання є штучним і незаслужено обмежує його цілісне розуміння та розвиток. Такий поділ, швидше за все, дозволяє усунути деякі сперечання конкретних компаній у спробі запропонувати на особливий ринок IoT, що розвивається, власні поточні продукти, які недостатньо під нього адаптовані.

Якщо підходити чесно, то повноцінне рішення (проєкт) для IoT лежить у споживчому та індустріальному полі одночасно [37].

Більш того, ключовою особливістю Інтернету речей є «розмиття кордонів» між персональним та громадським, між споживчим та промисловим. Коли технологія IoT забезпечує персональне рішення, вона безсумнівно з меншим успіхом може використовуватися й у вирішення ділових, економічних, соціальних завдань, мають значення для групи, однак пов'язаних, осіб. Підтвердження цієї тези спостерігається під час детального вивчення кожного з глобальних або спеціалізованих сегментів IoT. Тому оцінюючи особливості конкретного сегмента Інтернету речей та позиції бізнесу щодо нього завжди розумно досліджувати, розробляти та формувати конкурентні переваги як у частині споживчих (клієнтських) можливостей, так і в частині суспільних (індустріальних, галузевих) рішень [37].

Проблема безпеки Інтернету речей стоїть на одному з перших місць та викликає цілком обґрунтовані побоювання. Вплив мережевих технологій, особливо тих, які вторгаються в особистий та суспільний простір, від яких залежить життя та здоров’я людей, має бути не лише пасивно безпечним, а й запобіжно захищаючим. Неможливо допускати поширення технологій здатних викликати суттєвий негативний або навіть катастрофічний вплив на споживчі або промислові системи, якщо вони належним чином не застраховані від ризиків, якщо не вжито всіх заходів щодо моніторингу їхньої безпечної роботи та не передбачено способів мінімізації та усунення наслідків несприятливих подій.

У технічно складних системах, особливо тих, що залучають безліч окремих пристроїв, алгоритмів та інформації, виключити виникнення ризикованих ситуацій не було і не буде можливим. Горезвісний «людський фактор» також не виключений і вельми ймовірний. Потрібно створення системи захисту від широкого спектра ризиків: технічних, методичних, інформаційних, кон'юнктурних, подійних, ресурсних та багатьох інших.

З іншого боку, комплексний якісний захист від несприятливих подій, а також їх ліквідацію та компенсацію їх наслідків зможе забезпечити лише спеціалізований, професійний методичний та інструментальний, незалежний (стійкий) бізнес. Юридично це може бути незалежна особа чи виділений підрозділ (одиниця)

великого бізнесу. В останньому випадку важливо забезпечити його стабільність і стійкість у період дії несприятливої події, оскільки не лягає повний тягар відповідальності з підтримки бізнесу в критичних ситуаціях.

Таким чином, для активного та безпечного розвитку Інтернету речей знадобиться формування спеціальних висококваліфікованих центрів управління ризиками, які зможуть [36]:

- аналізувати та прогнозувати ризики;
- запобігати ризиковим подіям;
- керувати перебігом ризикових подій;
- ліквідувати наслідки несприятливих подій;
- відновлювати нормальний стан після ризикових подій.

У системах реалізованих на основі IoT-технологій недостатньо просто розробити “чарівні” протоколи та алгоритми дотримання та контролю безпеки. Необхідна повноцінна інтенсивна робота з моніторингу подій у сегментах Інтернету речей та управління ризиками як з точки зору технічної їх стійкості, так і з точки зору інформаційно-економічної самостійності та життєздатності.

Інтернет речей залучає у взаємодію не лише мобільні та стаціонарні пристрої, не лише фізичні речі та алгоритми, а й звичайних людей, соціальні групи, виробництва, бізнеси. Збій в ланцюзі трансакцій на будь-якому етапі та на будь-якому суб'єкті може призвести до несподіваних наслідків. Тому потрібно особливого виду та інформаційного рівня ризик-менеджмент[36].

Крім того, буде розглянуто та розгорнуто описано про технологію блокчейну, бо ця технологія вважається однією з передових технологій найближчого часу, яка може істотно змінити модель економіки. Блокчейн можна сприймати як свого роду суперкомп'ютер, який би кілька вузлів. Всі ваші дані зберігаються на ньому в цілості та безпеці. Що найцінніше – втратити такі дані неможливо. Вони зберігаються назавжди, причому реплікуючись у кожний вузол системи. Дані у блокчейні перебувають не лише у своєму фінальному стані, а й у всіх попередніх. Хакерам практично неможливо зламати це сховище, тому що кожен наступний

блок пов'язаний ланцюжком із попереднім, і так далі. Цей ланцюжок працює на численних комп'ютерах. Зламування блокчейну – це практично спроба обману глобальної комп’ютерної мережі, що з поточним розвитком техніки є малореальним.

Більшість користувачів мережі термін «блокчейн» однозначно асоціюється з Bitcoin. Ці два поняття – далеко не одне й те саме, хоч і нерозривно пов'язані: технологія блокчейн була розроблена для підтримки Bitcoin. Як відомо, цю криптовалюту створив у 2008 році хтось під псевдонімом Сатосі Накамото, тим самим випустивши з лампи джина технологій. Сьогодні за ці загадкові гроші в інтернеті можна купити все, що забажаєте. Ніхто не здатний контролювати їхній оборот, а відкрити биткоин-гаманець набагато простіше, ніж рахунок у банку. Користувачами мережі дуже високо цінуються такі якості цієї криптовалюти, як анонімність та прозорість. Переваги технології роблять її затребуваною для використання у таких сферах життя, як банківські операції, медицина, логістика, юриспруденція, музика. Візьмемо, наприклад, музикантів. На жаль, за традиційної схеми видання музики основна частина доходів йде лейблам, а творцям дістаються крихти. Застосування блокчейну в музичному бізнесі могло б дозволити автору пісні розмістити її для безплатного прослуховування, при цьому оформлюючи через програму окремі контракти на використання у приватних цілях, наприклад, у серіалі [36].

Та останнім класом являється вивчення безпеки об’єктів критичних інфраструктур. Бажано зазначити, що під об'єктами критичної інфраструктури ми розуміли не лише атомні електростанції. Підприємства, опитувані в ході дослідження, підбиралися з галузей, які мають таке значення для національної економіки або для суспільства, що у разі успішних атак та пошкодження їх комп'ютерних мереж виникне загроза національній безпеці – це охорона здоров'я, екстрені служби та, наприклад, телеком [36].

3.3 Розробка Концепції розгортання кіберполігону в університеті

Загальні відомості

Кіберполігон є спеціалізованою мережею, яка повністю ізольована від внутрішньої корпоративної інформаційно-освітньої мережі університету. При цьому кіберполігон, являє собою комплекс високопродуктивних лабораторій, які забезпечують основні напрямки розвитку цифрових послуг, підвищення рівня практичної підготовки у виявленні комп'ютерних атак, розслідування інцидентів інформаційної безпеки, взаємодії між підрозділами, впровадженні превентивних заходів щодо попередження комп'ютерних атак у учнів, фахівців, експертів та керівників в сфері інформаційних технологій, інформаційної безпеки та систем промислової автоматизації, проведення кібер-навчань, змагань і практичних тренувань з інформаційної безпеки для учнів, фахівців, експертів та керівників в сфері інформаційних технологій, інформаційної безпеки та систем промислової автоматизації, тестування програмного забезпечення, обладнання, елементів автоматизованих систем і систем промислової автоматизації на реалізацію функцій інформаційної безпеки.

Пропонується кіберполігон сформувати з трьох основних напрямків:

1 клас - вивчення кіберфізичних систем;

2 клас - вивчення систем Інтернет-речей, технології блокчейн;

3 клас - вивчення безпеки об'єктів критичних інфраструктур.

Лабораторії кіберфізичних систем мають виконувати такі функції:

- застосування на практиці пошуку та попередження витоків важливої інформації;

- знаходження та блокування використання закладок;

- визначення на скільки стійкими можуть бути криптографічні алгоритми.

Пропонується розглядати створення трьох комплексованих лабораторій, які дозволять сформувати єдиний комплекс.

Комплекс призначений для вирішення наступних завдань:

“Навички інформаційної безпеки” – інфраструктура включає в себе платформу для тестування і підготовки працівників практичним навичкам дотримання правил інформаційної безпеки, включаючи імітацію фішингових атак;

“Захист від несанкціонованого доступу” – інфраструктура включає в себе технології і продукти не менше двох виробників засобів розмежування доступу кожного типу: програмних систем захисту інформації для комерційних операційних систем, апаратно-програмних модулів довіреного завантаження (електронних замків), захищених операційних систем вітчизняного (не менше двох різнотипних операційних систем) та іноземного виробництва, засобів антивірусного захисту інформації (не менше двох вітчизняних різних антивірусних засобів захисту);

“Мережева безпека” – інфраструктура включає технології і продукти не менше двох виробників міжмережевих екранів, не менше двох виробників системи виявлення атак;

“Захист веб-додатків” – інфраструктура включає технології та продукти не менше двох виробників міжмережевих екранів рівня веб-додатків;

“Моніторинг та аналіз інцидентів інформаційної безпеки” – інфраструктура включає технології та продукти не менше двох виробників систем виявлення і аналізу інцидентів;

“Реагування на комп'ютерні інциденти та комп'ютерна форензіка” – інфраструктура включає в себе не менше двох виробників засобів пошуку, відновлення та аналізу цифрових доказів, включаючи приховану і технологічну системну інформацію.

При формуванні практичних завдань передбачається використовувати практичні та лабораторні завдання курсів Академії CISCO в спеціалізованих курсах CCNA Cybersecurity Operations, Network Security, IoT Fundamentals: IoT Security Course Resources.

Вимоги безпеки

Віртуалізована система резервування та відновлення даних забезпечує найвищу ступінь відмовостійкості комплексу. Можливість віддаленого використання кіберполігону дозволить проводити заняття зі студентами з урахуванням, як офлайн, так і онлайн навчання, використовувати потужності кіберполігону у віддаленому доступі для виконання практичних та лабораторних завдань. Програмні та технічні засоби кіберполігону повинні пріоритетно вибиратися з урахуванням можливості нарощування обчислювальної потужності і масштабування його компонентів і підсистем, у тому числі, з використанням хмарних технологій. Кіберполігон не повинен бути призначений для обробки інформації, що становить державну таємницю. В процесі обслуговуванні Кіберполігону повинні дотримуватися норми електричної та протипожежної безпеки, встановлені на об'єкті проведення робіт.

Вимоги до захисту від впливу зовнішніх впливів

Програмно-технічні і технічні засоби Кіберполігону повинні бути встановлені в спеціально обладнаних приміщеннях, в яких забезпечується необхідна ступінь кліматичного захисту від впливу зовнішнього середовища.

Приміщення, в яких розміщуються програмні та технічні засоби Кіберполігону, повинні бути обладнані засобами контролю та управління доступом, пожежної безпеки, вентиляції та кондиціонування.

Приміщення та обладнання Кіберполігону повинні виключати можливість безконтрольного доступу сторонніх осіб.

Вимоги до ергономіки та технічної естетики

Компоненти технічної частини Кіберполігону повинні мати можливість установки в монтажні стійки (шафи) в наявних серверних приміщеннях.

Технічне забезпечення уніфікованих робочих місць повинно надавати можливість використання інфраструктуру Кіберполігону для участі в кібернавчаннях та проведення тестування програмного забезпечення

Вимоги щодо збереження інформації при аваріях

При аваріях повинна бути забезпечена збереженність такої інформації:

- параметри конфігураційних налаштувань систем Кіберполігону;

- параметри налаштувань засобів ідентифікації, аутентифікації і авторизації систем Кіберполігону;

- дані журналів подій.

Збереження інформації повинна забезпечуватися при наступних аварійних ситуаціях:

- порушення електроживлення;

- збій загального або спеціального програмного забезпечення компонентів Кіберполігону;

- проведення внутрішніх та зовнішніх атак на інфраструктуру Кіберполігону.

Вимоги до захисту від впливу зовнішніх впливів

Програмно-технічні та технічні засоби Кіберполігону повинні бути встановлені в спеціально обладнаних приміщеннях, в яких забезпечується необхідна ступінь кліматичного захисту від впливу зовнішнього середовища.

Приміщення, в яких розміщуються програмні та технічні засоби Кіберполігону, повинні бути обладнані засобами контролю і управління доступом, пожежної безпеки, вентиляції та кондиціонування.

Приміщення та обладнання Кіберполігону повинні виключати можливість безконтрольного доступу сторонніх осіб.

3.4. Висновки до розділу 3

Запропонований функціонал завдань кіберполігону дозволяє створювати на відпрацьовувати завдання, які пов’язані з сучасними векторами комплексованих загроз. Розроблені принципи к формуванню та розгортанню кіберполігону в університеті дозволяють визначити узагальнений підхід щодо основних напрямків завдань (функціональності) лабораторій кіберполігону, вимог безпеки, ергономіки та технічної естетики, збереження інформації при аваріях.

Такій підхід дозволяє гарантувати можливість масштабування, розширювання спектру завдань та функціональності.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Організація служби охорони праці на підприємстві

Закон України «Про охорону праці» передбачає, що роботодавець зобов'язаний створити на робочому місці умови праці та забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці. З цією метою роботодавець забезпечує функціонування системи управління охороною праці та несе безпосередню відповідальність за порушення вимог з охорони праці на підприємстві.

На підприємстві з кількістю працюючих менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають виробничий стаж не менше трьох років і пройшли навчання з охорони праці.

На підприємстві з кількістю працюючих 50 і більше осіб роботодавець створює службу охорони праці відповідно до типового положення, що затверджується центральним органом виконавчої влади, що забезпечує формування державної політики у сфері охорони праці.

На підприємстві з кількістю працюючих менше 20 осіб для виконання функцій служби охорони праці можуть залучатися сторонні спеціалісти на договірних засадах, які мають відповідну підготовку.

Служба охорони праці підпорядковується безпосередньо роботодавцю. Керівники та спеціалісти служби охорони праці за своєю посадою і заробітною платою прирівнюються до керівників і спеціалістів основних виробничо-технічних служб.

Спеціалісти служби охорони праці мають право:

- видавати керівникам структурних підрозділів підприємства обов'язкові для виконання приписи щодо усунення наявних недоліків, одержувати від них необхідні відомості, документацію і пояснення з питань охорони праці;
- вимагати відсторонення від роботи осіб, які не пройшли передбачених законодавством медичного огляду, навчання, інструктажу, перевірки знань і не мають

допуску до відповідних робіт або не виконують вимог нормативно-правових актів з охорони праці;

- зупиняти роботу виробництва, дільниці, машин, механізмів, устаткування та інших засобів виробництва у разі порушень, які створюють загрозу життю або здоров'ю працюючих;
- надсилати роботодавцю подання про притягнення до відповідальності працівників, які порушують вимоги щодо охорони праці;
- за поліпшення стану безпеки праці вносити пропозиції про заохочення працівників за активну працю.

Припис спеціаліста з охорони праці може скасувати лише роботодавець. Ліквідація служби охорони праці допускається тільки у разі ліквідації підприємства чи припинення використання найманої праці фізичною особою.

Фінансування охорони праці здійснюється роботодавцем. Фінансування профілактичних заходів з охорони праці, виконання загальнодержавної, галузевих та регіональних програм поліпшення стану безпеки, гігієни праці та виробничого середовища, інших державних програм, спрямованих на запобігання нещасним випадкам та професійним захворюванням, передбачається, поряд з іншими джерелами фінансування, визначеними законодавством, у державному і місцевих бюджетах.

Для підприємств, незалежно від форм власності, або фізичних осіб, які відповідно до законодавства використовують найману працю, витрати на охорону праці становлять не менше 0,5 відсотка від фонду оплати праці за попередній рік.

На підприємствах, що утримуються за рахунок бюджету, розмір витрат на охорону праці встановлюється у колективному договорі з урахуванням фінансових можливостей підприємства, установи, організації.

Суми витрат з охорони праці, що належать до валових витрат юридичної чи фізичної особи, яка відповідно до законодавства використовує найману працю, визначаються згідно з переліком заходів та засобів з охорони праці, що затверджується Кабінетом Міністрів України.

Роботодавець зобов’язаний інформувати працівників або осіб, уповноважених на здійснення громадського контролю за дотриманням вимог нормативно-правових актів з охорони праці, та Фонд соціального страхування України про стан охорони праці, причину аварій, нещасних випадків і професійних захворювань і про заходи, яких вжито для їх усунення та для забезпечення на підприємстві умов і безпеки праці на рівні нормативних вимог.

Працівникам забезпечується доступ до інформації та документів, що містять результати атестації робочих місць, заплановані роботодавцем профілактичні заходи, результати розслідування, обліку та аналізу нещасних випадків і професійних захворювань і звіти з цих питань, а також до повідомлень, подань та приписів органів державного нагляду за охороною праці.

Органи державного управління охороною праці у встановленому порядку інформують населення України, працівників про реалізацію державної політики з охорони праці, виконання загальнодержавної, галузевих чи регіональних програм з цих питань, про рівень і причини аварійності, виробничого травматизму і професійних захворювань, про виконання своїх рішень щодо охорони життя та здоров’я працівників.

4.2 Психофізіологічне розвантаження для працівників

При проведенні сеансів психофізіологічного розвантаження рекомендується використовувати деякі елементи методу аутогенного тренування, який ґрунтується на свідомому застосуванні комплексу взаємопов’язаних прийомів психічної саморегуляції й виконанні нескладних фізичних вправ із словесним самонавіюванням. Головна увага при цьому приділяється набуванню й закріпленню навичок м’язового розслаблення (релаксації). У рекомендованому сеансі, який має проводитися в кімнаті психофізіологічного розвантаження з відповідним інтер’єром та кольоровим оформленням, виділяються три періоди, що відповідають фазам відновлювального процесу. Перший період – абстрагування працівників від виробничої обстановки – відповідає фазі залишкового збудження.

Лунають повільна мелодійна музика, пташиний спів. Обравши зручну позу, працівники адаптуються і психологічно готуються до наступних періодів. Другий – заспокоєння – відповідає фазі відновлювального гальмування. Пропонується показ фотослайдів із зображеннями квітучого лугу, березового гаю, гладенької поверхні ставка тощо. Через навушники транслюється спокійна музика, а на її фоні негучно, повільно висловлюються заспокійливі формули аутогенного тренування. Як функціональне освітлення застосовують зелене світло. Яскравість світла має поступово знижуватись протягом періоду, а наприкінці його світло вимикається зовсім на 1-2 хвилини. Екран теж гасне. Третій період – активізація – відповідає фазі підвищеної збудженості. На початку періоду світло вимкнене, через певний час на екрані з'являється червона пляма, розміри і яскравість якої поступово збільшуються. Наприкінці періоду лунає бадьора музика. Тричі вимовляються мобілізуючі формули аутогенного тренування, яким мають передувати глибоке вдихання та довге глибоке видихання

Сеанси психологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний:

- повне розслаблення;

- активізація працездатності.

У разі потреби, на фоні музичних програм можуть вимовлятися окремі фрази навіювання відпочинку, гарного самопочуття і, на заключному етапі, бадьорості.

Після сеансів психофізіологічного розвантаження у працівників зменшується відчуття втоми, з’являються бадьорість, гарний настрій. Загальний стан відчутно поліпшується.

ВИСНОВКИ

1. Проведений аналіз сучасного стану загроз дозволяє сформулювати основні направленості сучасних загроз, їх ефективність, та можливість модифікації. В умовах диджиталізації та розвитку цифрових послуг в кіберпросторі вимагає забезпечення безпеки за складовими: кібербезпека, інформаційна безпека, та безпека інформації. Тому практична складова відпрацювання відомих цільових атак, реалізація превентивних заходів дозволяє створювати системи захисту інформації, які спроможні протидіяти цім атакам.

2. При відпрацюванні сучасних загроз необхідно мати не тільки відповідне обладнання, яке дозволяє створювати ту, чи іншу інфраструктуру, забезпечувати необхідні обчислювальні ресурси щодо реалізації атак, а також забезпечити безпеку проведення практичних занять, щодо корпоративної інформаційно-освітньої мережі університету. Для реалізації цих завдань необхідно створення захищеного середовища – кіберполігон, який дозволяє не тільки забезпечити відпрацювання завдань з нападу та захисту, а також забезпечити безпеку до фізичної мережі закладу вищої освіти.

3. Запропонована Концепція розгортання кіберполігону є універсальним підходом, який відповідає сучасним міжнародним вимогам щодо створення кіберполігону, дозволяє масштабувати та розширювати не тільки спектр функціональності, а також напрямки відповідно до зміни векторів кіберзагроз, розвитку обчислювальної техніки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наскрізна програма практики для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронний ресурс] / уклад. С. П. Євсеєв, О. В. Мілов, О. Г. Король. – Харків : ХНЕУ ім. С. Кузнеця, 2021. – 32 с.

2. Методичні рекомендації до виконання дипломних проєктів (робіт) для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронний ресурс] / уклад. С. П. Євсеєв, О. Г. Король, А. А. Гаврилова, О. В. Мілов. – Харків : ХНЕУ ім. С. Кузнеця, 2021. – 47 с.

3. Вимоги до оформлення курсових і дипломних проектів : методичні рекомендації для студентів галузі знань 12 "Інформаційні технології" / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 50 с.

4. Диогенес Ю. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, О. Эрдаль., 2016. – 326 с.

5. Yevseiev and other. Development of conception for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies. 2021. 3/9 (111). P. 63–83.

6. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

7. Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014.

8. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, *“Політика інформаційної безпеки”*, ПВП «Задруга»,. 2014.

9. Ю. Г. Даник та ін., “*Основи захисту інформації*” навч. пос., Житомир : ЖВІ ДУТ, 2015.

10. О. К. Юдін “*Інформаційна безпека. Нормативно-правове забезпечення*”, К. : НАУ, 2011.

11. Р. В. Грищук, “Атаки на інформацію в інформаційно-комунікаційних системах”, Сучасна спеціальна техніка, №1(24), с.61 – 66. 2011.

12. Р. В. Грищук, і В. В. Охрімчук, “Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак”, Безпека інформації, Том 21, № 3, с. 276 – 282, 2015.

13. Ю. Г. Даник, Р. В. Грищук, “Синергетичні ефекти в площині інформаційного та кібернетичного протиборства”, Наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою держави”, Київ, 19 берез, 2015, с. 235 – 237.

14. Р. В. Грищук, В. В. Охрімчук, “Напрямки підвищення захищеності комп’ютерних систем та мереж від кібератак”, ІІ Міжнар. наук.-практ. конф. “Актуальні питання забезпечення кібербезпеки та захисту інформації” (Закарпатська область, Міжгірський район, село Верхнє Студене, 24-27 лют. 2016 р.). – К. : Видавництво Європейського університету, 2016 с. 60 – 61.

15. О. Архангельский, Д. Сютов, А. Кузнецов, “Как мы построили виртуальную инфраструктуру для киберучений промышленных предприятий” [Электронный ресурс]. Доступно: https://habr.com/ru/company/solarsecurity/blog/515626. Дата обращения: Дек. 25.08.2020.

16 С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч. 2”, Сучасна спеціальна техніка. Науково-практичний журнал, № 2(49), с. 10 – 17, 2017.

17 С. П. Евсеев, “Анализ защиты в национальной системе масовых электронных платежей”, Інформаційна безпека, № 3(15), № 4 (16), с. 15 – 28, 2014

18 О. К. Юдін “Інформаційна безпека. Нормативно-правове забезпечення”, К. : НАУ, 2011.

19 С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность. К. : Арий, 2008.

20 W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for criticalinfrastructures : Attack and defense modeling”, IEEETrans. Syst., Man Cybern. A, vol. 40, no. 4, pp.853 – 865, 2010.

21 Worldwide Infrastructure Security Report. 2014. Arbor Networks, Inc [Online]:

Available: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fpages.arbornetworks.com%2Frs%2Farbor%2Fimages%2FWISR2014_EN2014.pdf&ei=DyR2VfznJOPgyQOghoN4&usg=AFQjCNGP0_ZTliItqCtofJ-cXfZT9QHRiQ&sig2=4hgA_vIye1idQyQgsTIZXg&bvm=bv.95039771,d.bGQ. Accessed on: Des. 09, 2017.

22 Е. С. Пелевина, “Информационные угрозы кибертерроризма”, Евразийский Союз Ученых (ЕСУ), № 11 (20). Политические Науки, с. 100 – 103, 2015.

23 Е. В. Иванченко, и В. А. Хорошко, “Тенденции развития кибертерроризма”, МНПК “Современные информационные и электронные технологии”, Одесса, с. 105 – 106, 2014.

24 Г. П. Леоненко, и А. Ю. Юдин, “Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины”, Information Technology and Security, № 1(3), с. 44 – 48. 2013.

25 Р. В. Грищук, та Ю. Г. Даник, “Синергія інформаційних та кібернетичних дій”, Труди університету. НУОУ, № 6 (127), с. 132–143. 2014.

26 В. И. Ярочкин, “Безопасность банковских систем”, М.: Издательство: Ось-89, 416 с., 2012.

27 Постанова НБУ28.09.2017 № 95, “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”, URL : http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page. Дата звернення: листопад., 5, 2021.

28 Украинский ресурс по безопасности [Электронный ресурс]. Доступно: http://kiev-security.org.ua. Дата звернення: листопад., 5, 2021.

29 М. Н. Симаков, V Съезд директоров по информационной безопасности [Электронный ресурс] Доступно: http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf. Дата звернення: листопад., 5, 2021.

30 П. В. Ревенков, “Защита информации в банке: основные угрозы и борьба с ними”, [Электронный ресурс] Доступно: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html. Дата звернення: листопад., 5, 2021.

31 Звіт CERT-UA за 2010 – 2013 роки [Електронний ресурс]. Доступно: http://cert.gov.ua/?p=316. Дата обращения: Дек. 7, 2017.

32 Киберполигон как обучающая система, URL: https://habr.com/ru/post/502780/ Дата звернення: листопад., 5, 2021.

33 Кибершит Украины: кто стоит на страже кибергранiц страны, [Електронний ресурс]. Доступно: http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany. Дата звернення: листопад., 5, 2021.

34 Безопасность IP-сетей нового поколения для провайдеров услуг, [Электронный ресурс] : Доступно : http://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=IP_NGN.pd. Дата звернення: Груд. 7, 2017.

35 Магическая аура блокчейна, URL: https://habr.com/ru/company/asus/blog/373283/ Дата звернення: листопад., 5, 2021.

36 Сегменті Интернет вещей: общие принципы, URL: https://habr.com/ru/post/asus/300608/ Дата звернення: листопад., 5, 2021.

37 Кибер-физические системы в современном мире, URL: https://habr.com/ru/company/toshibarus/blog/438262/ Дата звернення: листопад., 5, 2021.

38 Самые громки кибер-атаки на критические инфраструктуры, URL: https://habr.com/ru/company/panda/blog/316500/ Дата звернення: листопад., 5, 2021.