МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

**МАГІСТЕРСЬКА РОБОТА**

НА ТЕМУ:

# КОМПЛЕКСНА РОБОТА: SMART GRID. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ

Освітньо-кваліфікаційний рівень “Магістр”
Спеціальність 122 – “Комп'ютерні науки”

| | | |
|---|---|---|
| Науковий керівник роботи: | _____ (підпис) | Г. Ф. Кривуля (ініціали, прізвище) |
| Консультант з охорони праці: | _____ (підпис) | Я. О. Критська (ініціали, прізвище) |
| Студент: | _____ (підпис) | Ю. С. Старцева (ініціали, прізвище) |
| Група: | | КН-17Дм |

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки
(шифр і назва)
Спеціальність 122 – «Комп'ютерні науки»
(шифр і назва)

**ЗАТВЕРДЖУЮ:**

Завідувач кафедри
І.С. Скарга-Бандурова
«_____» _____20____р.

**З А В Д А Н Н Я**
**НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ**

Старцевій Юлії Сергіївні
(прізвище, ім'я, по батькові)

1. Тема роботи **КОМПЛЕКСНА ТЕМА: SMART GRID. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ**
керівник проекту (роботи) Кривуля Г.Ф., д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " 18 " 10 2018 р. № ____
2. Термін подання студентом роботи
3. Вихідні дані до роботи Матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз методів забезпечення кібербезпеки систем релейного захисту та автоматики в Smart Grid
Розробка об’єктної моделі для прогнозування та симуляції атак
Розрахунок ймовірних атак за ступенем уразливості
Питання охорони праці, екології.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

| Розділ | Прізвище, ініціали та посада Консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Охорона праці | Критська Яна Олександрівна | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проекту (роботи) | Строк виконання етапів проекту ( роботи ) | Примітка |
|---|---|---|---|
| 1 | Аналітичний огляд літератури за темою роботи | 1.09.18 – 1.10.18 | |
| 2 | Аналіз методів і моделей забезпечення кібербезпеки в Smart Grid | 1.09.18 - 2.10.18 | |
| 3 | Аналіз властивостей та ризиків моделей кібербезпеки в Smart Grid | 3.10.18 – 9.10.18 | |
| 4 | Визначення загроз кібербезпеки в Smart Grid | 10.10.18 – 24.10.18 | |
| 5 | Розробка моделі для симуляції атак | 25.10.18 – 25.11.18 | |
| 6 | Розгляд питань охорони праці та основних напрямків їх дотримання | 13.11.18 – 15.12.18 | |
| 7 | Оформлення пояснювальної записки | 22.12.18 – 28.12.18 | |
| 8 | Оформлення презентації роботи | 29.12.18 – 7.01.19 | |
| | | | |
| | | | |
| | | | |
| | | | |

**Студент** _____ _____
( підпис ) (прізвище та ініціали)

**Керівник** _____ _____
( підпис ) (прізвище та ініціали)

## АНОТАЦІЯ

Старцева Юлія Сергіївна. Комплексна тема: Smart Grid. Методи забезпечення кібербезпеки систем релейного захисту та автоматики.

В роботі проведено аналіз існуючих методів, моделей та стандартів забезпечення кібербезпеки Smart Grid. Визначені вимоги до кібербезпеки згідно діючих стандартів, розподілено кроки атак та представлено результати моделювання і варіанти захисту. В процесі дослідження було розроблено об'єктну модель для оцінки імовірних ризиків системи, прогнозування, симуляції атак та заходів захисту від атак.

**Ключові слова: Smart Grid, вразливості, SCADA, граф, кіберграф, кібератака, архітектура, моделювання, модель.**

## АННОТАЦИЯ

Старцева Юлия Сергеевна. Комплексная тема Smart Grid. Методы обеспечения кибербезопасности систем релейной защиты и автоматики.

В работе проведен анализ существующих методов, моделей и стандартов обеспечения кибербезопасности Smart Grid. Определены требования к кибербезопасности согласно действующих стандартов, распределены шаги атак и представлены результаты моделирования и варианты защиты. В процессе исследования была разработана объектная модель для оценки возможных рисков системы, прогнозирования, симуляции атак и мер защиты от атак.

**Ключевые слова: Smart Grid, уязвимости, SCADA, граф, кибергграф, кибератака, архитектура, моделирование, модель.**

## ABSTRACT

Startseva Julia Sergeevna. Integrated Smart Grid theme. Cybersecurity methods for relay protection and automation systems.

The paper analyzes the existing methods, models and standards for cyber security Smart Grid. Requirements for cyber security according to current standards are defined, attack steps are distributed, and simulation results and protection options are presented. In the course of the study, an object model was developed to assess the possible risks of the system, to predict, simulate attacks, and attack protection measures.

**Keywords: Smart Grid, vulnerabilities, SCADA, graph, cybergraph, cyber-attack, architecture, modeling, model.**

**ЗМІСТ**

# ПЕРЕЛІК СКОРОЧЕНЬ

DG - distributed generation

ICT - Information and communications technology

DR - demand response

ES - energy storages

DER - distributed energy resources

IED - intelligent electronic devices

SG - Smart Grid

SGAM - Smart Grids Architecture Model

SCADA - Supervisory Control And Data Acquisition

EMS - energy management system

PMU - phasor measurement units

WAWS - wide-area monitoring system

PDC - phasor data concentrators

WAN - wide area network

SDLC - Systems Development Life Cycle

IDS - Intrusion Detection System

ID - Intrusion Detection

IEC - International Electrotechnical Commission

MG - Microgrid

MGEMS - Microgrid Energy Management System

DSO - Distribution System Operator

SE - Systems Engineering

IEC - International Electrotechnical Commission

DNP3 - Distributed Network Protocol

GOOSE - Generic Object Oriented Substation Event

TLS - Transport Layer Security

SNMP - Simple Network Management Protocol

ARP - Address Resolution Protocol

OCL - Object Constraint Language

# ВСТУП

Зараз енергосистема зіткнулася з проблемами, пов'язаними з кібер-атаками, які підняли питання про уразливість безпеки на критичну інфраструктуру енергосистеми.

Інтелектуальна мережа (Smart Grid) - це система, заснована на комунікаційних та інформаційних технологіях у виробництві, постачанні та споживанні енергії.

Мережа використовує двосторонній потік інформації для створення автоматизованої і широко розподіленої системи, яка має нові функціональні можливості, такі як контроль в режимі реального часу, ефективність роботи, стійкість до мережі і найкраща інтеграція відновлюваних технологій. Однак в смарт-мережах все ще існують ризики. Будь-які перебої в виробленні електроенергії можуть порушити стабільність інтелектуальної мережі та можуть потенційно мати значні соціально-економічні наслідки. У міру обміну цінними даними між інтелектуальними мережевими системами крадіжка або зміна цих даних можуть порушувати конфіденційність споживачів. Через ці недоліки інтелектуальна мережа стала основною метою атакуючих, яка привернула увагу уряду, промисловості та наукових кіл.

Енергетичні мережі необхідні для фізичного та економічного добробуту. При розгортанні рішень для інтелектуальних мереж важливо, щоб безпека розглядалася для захисту найважливіших активів електроенергетичної системи.

Увага кібербезпеки пов'язана з системами інформаційних технологій, метою яких є захист інформації та інформаційних систем щодо несанкціонованого доступу, використання, модифікації або будь-яких дій, які можуть поставити під загрозу конфіденційність, цілісність або доступність інформації. Кібербезпека для інтелектуальних мереж вимагає спільної уваги до інформаційної безпеки для IT-систем, мережі зв'язку і фізичного обладнання електричної мережі.

NIST (Національний інститут стандартів і технологій) визначає архітектуру інтелектуальних мереж як модель, що складається з семи доменів, визначених в такий спосіб:

1) Клієнти - кінцевий користувач електроенергії, який також може генерувати, зберігати і управляти використанням енергії. Зазвичай клієнти класифікуються як житлові, комерційні та промислові.

2) Ринок - оператори та учасники ринку для покупки і продажу енергії;

3) Постачальники послуг - організації, які надають електропостачання клієнтам;

4) Операція - керуючі потоками енергії на всіх рівнях - від генерації, передачі і розподілу;

5) Покоління - включає традиційну централізовану генерацію і розподілену генерацію;

6) Передача - відповідає за транспортування енергії на великі відстані;

7) Розподіл - розподіл електроенергії споживачам.

Інтелектуальна мережа має можливість оптимізувати енергоресурси, знизити витрати, підвищити надійність і підвищити ефективність електроенергії.

Необхідно визначити проблеми кібербезпеки, ознайомитися з класифікацією можливих наслідків і збитків кіберзагроз, простежити причинно-наслідкові зв'язки по всьому ланцюжку, розглянути ефективність і надійність мережі для мінімізації втрат при розподілі та ризики безпеки.

У систему інтелектуальних мереж необхідно включити три основні завдання безпеки:

1. наявність безперебійного електроживлення відповідно до вимог користувача
2. цілісність переданої інформації
3. конфіденційність даних користувача.

Питаннями розробки методів забезпечення кібербезпеки електроенергетичних мереж займалися Ferran Torrent Fontbona, Alessandra Pieroni, Noemi Scarpato, Luca Di Nunzio, Francesca Fallucchi, Mario Raso, Ahmed Elgargouri, Reino Virrankoski, Mohammed Elmusrati, Giang T. Pham.

Разом з тим, все ще існують проблеми з затримками, які можуть дати зловмисникові додаткову тривалість, щоб як небудь вплинути на систему, з втратою потужності, з якістю і зміною напруги, з управлінням захистом від замикань на землю і при зміні конфігурації мережі, з дизайном архітектури комунікацій Smart Grid: енергетичними послугами, інтероперабельністю, величезною сумою даних, зміною трафіка, якістю обслуговування і безпекою.

**Мета роботи:** підвищення кібербезпеки електроенергетичних мереж за рахунок оцінки ризиків і властивостей використання розробленої моделі та методів в програмному інструменті архітектури для забезпечення прогнозування і аналізу атак і захисту. Для досягнення мети дослідження необхідно вирішити такі **завдання**:

- аналіз методів і стандартів забезпечення кібербезпеки
- аналіз методів прогнозування ймовірного моделювання архітектури
- аналіз властивостей та ризиків моделей безпеки на моделях архітектури підприємства

- імовірна оцінка і прогнозування властивостей системи
- визначення та застосування рамки оцінки для виконання
- створення об’єктної моделі для прогнозування та симуляції атак
- розрахунок ймовірних атак за ступенем серйозності уразливості і представлення результату моделювання

**Об’єкт дослідження** – процеси забезпечення кібербезпеки систем релейного захисту та автоматики.

**Предмет дослідження** – моделі та методи забезпечення кібербезпеки в системах РЗА.

**Практичне значення отриманих результатів** полягає в тому, що основні наукові положення магістерської роботи реалізовані у виді розрахункових моделей, які дозволяють визначити ступені серйозності уразливості моделей при виникненні небезпечних загроз та їх запобіганню за допомогою програмного інструмента моделювання для застереження та захисту від шкідливих атак .

**Особистий внесок здобувача**. Усі основні результати отримані автором особисто. У роботах, опублікованих у співавторстві, автору належать: розробка об’єктної моделі для оцінки і прогнозування інформаційної безпеки підприємства з використанням атак і захисту.

**Апробація матеріалів дисертації.** Основні положення та результати магістерської роботи обговорювалися на науково-технічних конференціях і тематичних семінарах, у тому числі Форумі ІТ-Ідея (м. Сєвєродонецьк, 2016, 2018 рр.).

**Публікації.** За темою роботи з викладенням її основних результатів опубліковано 3 наукові праці, з яких 1 стаття в науковому фаховому виданні України; 2 публікації у збірниках матеріалів і праць конференцій.

**Структура та обсяг магістерської роботи.** Магістерська робота містить анотацію, перелік скорочень, вступ, 4 розділи, перелік посилань з 51 найменувань, 1 додаток. Пояснювальна записка містить 130 сторінок, 16 таблиць та 32 рисунка.

# РОЗДІЛ 1
# АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В SMART GRID. ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕНЬ

## 1.1 Аналіз вимог до функціональних характеристик Smart Grid і Micro Grid

### 1.1.1 Визначення Smart Grid і Micro Grid. Основні структурні компоненти Smart Grid і Micro Grid

Smart Grid представляє собою розвиток традиційних електричних мереж для інтеграції нових суб'єктів та сценаріїв, щоб забезпечити безпеку, стабільність та доступність електроенергії, високий рівень якості та надійність постачання.

Основні можливості інтегрованої мережі включають інтеграцію розподілених енергетичних ресурсів та великомасштабні відновлювані джерела та впровадження різних систем і функцій для реагування на попит. Системна інтеграція має вирішальне значення для забезпечення цих можливостей [1].

Microgrid - це система з самостійним управлінням з конкретною місією, яка діє, щоб зберегти свою здатність виконувати цю місію. З цією метою він набуває і споживає електроенергію. Мікросхема може зберігати електроенергію, щоб вона могла виконувати свою місію в майбутньому, незалежно від того, чи доступна потужність [2]. Microgrid складається з розподілених енергетичних ресурсів, силових електронних пристроїв і силових пристроїв, системи зв'язку і системи управління, як показано на рисунку 1.1 [3].

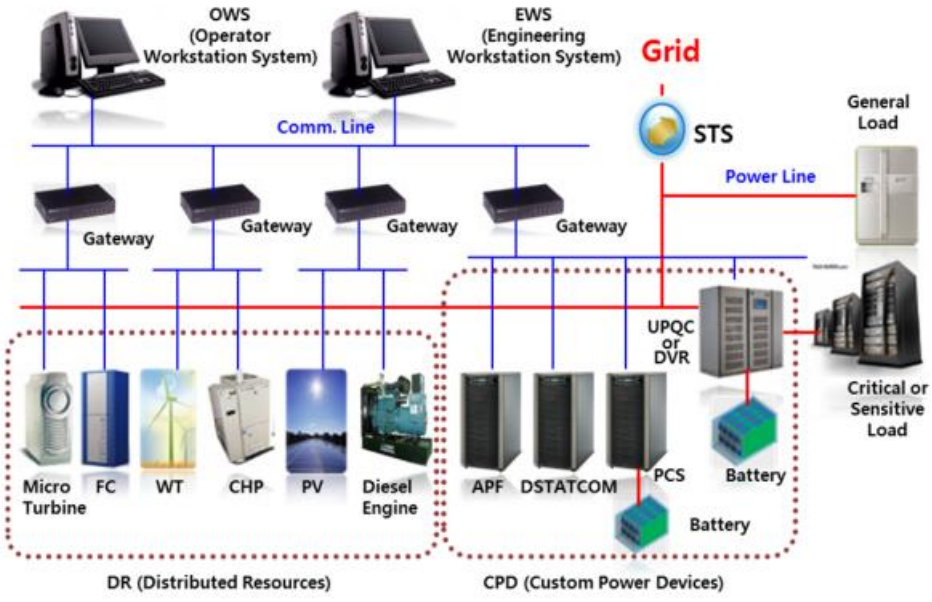


Рисунок 1.1 – Типова конфігурація Microgrid

Модель ринку дуже важлива для визначення функціональності і архітектури Microgrid Energy Management System (MGEMS)

Основні функції Microgrid:

1) Функції планування генерації.

Функції планування генерації MGEMS аналогічні функції системи управління енергією великої площі.

2) Функції управління попитом.

Система управління енергією Microgrid повинна включати в себе функціональні можливості розподілених ресурсів типу попиту. Майже всі функції сконструйовані в нормальних умовах, за винятком скидання навантаження в аварійному стані, який повинен бути інтегрований з процесом відновлення по послідовному списку процесів після переходу в нормальний стан

3) Залежні функції пристроїв харчування

Період сканування для телеметричного значення зазвичай становить кілька хвилин, а найкоротший період сканування може становити кілька секунд в якомусь спеціальному випадку. Для безперебійної роботи при виникненні несправності в основній сітці потрібно дуже швидкий поділ між основною мережею і мікросхемою, а потім безперервне енергопостачання з системою зберігання енергії, яка може бути виконана тільки з програмною системою управління енергією. У певному стані стійка експлуатація заборонена через правила приєднання [3].

Вимоги Smart Grid можуть бути розділені на вимоги користувачів, функціональні вимоги і вимоги до продуктивності Основною вимогою для системи захисту є те, що вона може надійно виявляти будь-які несправності в зоні захисту [4].

Найбільш важливими вимогами Smart Grid є [1]:

– Проста інтеграція DG.

– Можливість адаптуватися до змінюваним умовам системи.

– Підвищена надійність при поставці шляхом самовідновлення.

– Використання повного потенціалу передової технології ICT (Information and communications technology).

– Забезпечення застосування основних системних технологій, які пропонують економічно ефективний спосіб підвищення надійності системи.

Елементи системи Smart Protection:

– Телекомунікація

– Адаптивність

– Релейне програмне забезпечення та алгоритми

Для аналізу функціональних вимог захисту Smart Grid потрібен належний поділ вивченої системи розподілу на захисні зони. Поділ зони повинен бути зроблений з урахуванням можливостей для функцій самовідновлення. В якості ефективного методу аналізу вимог до захисту Smart Grid застосовується систематичний підхід, заснований на обмеженому наборі різних типів захисних зон. Захисна зона визначається як частина енергосистеми і обмежена захисними пристроями.

Визначені основні типи захисних зон: радіальні, кільце та сітка [1].

Інтелектуальна енергетична інфраструктура і додатки Smart Grid можуть обговорюватися в трьох підрозділах як виробництво електроенергії, передача і розподіл [5].

Компоненти зв'язку інтелектуальної мережі можуть включати в себе проводові та бездротові способи, такі як комунікації лінії електропередач, технології, засновані на протоколі IEEE 802.15.4 та / або механізми управління агентами, див. рис. 1.2.

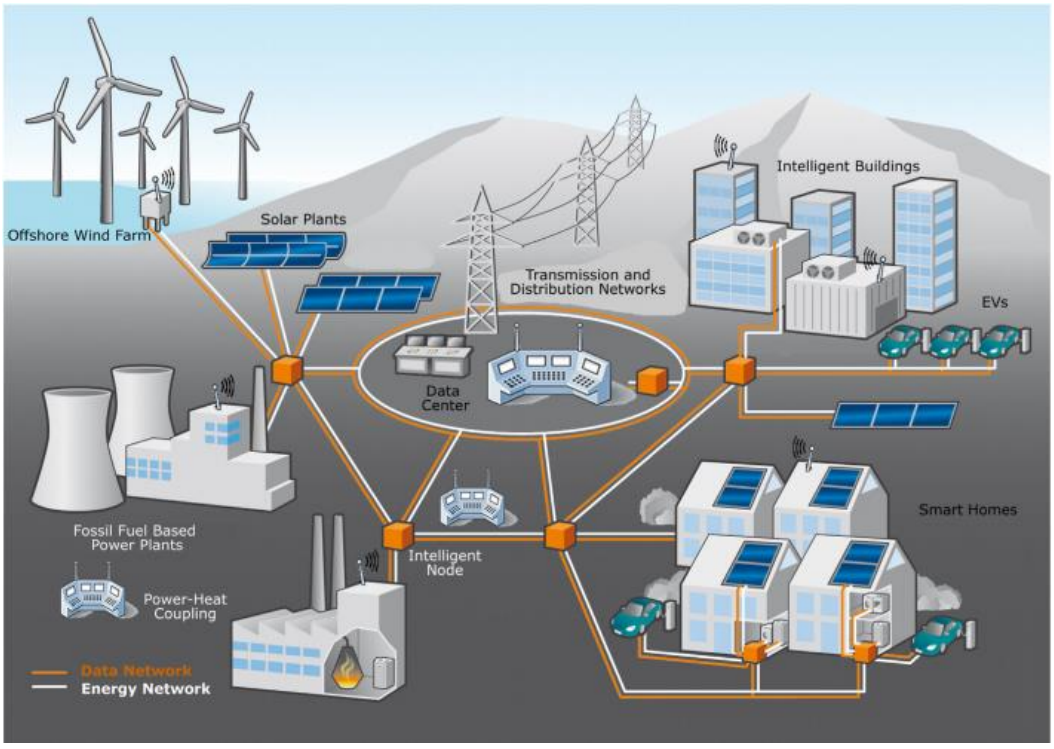


Рисунок 1.2 – Перспектива Smart Grid з усіма компонентами.

*Компоненти Smart Grid*

Основними компонентами Smart Grid є: нові і вдосконалені компоненти мережі, інтелектуальні пристрої та інтелектуальний облік, інтегровані комунікаційні технології, програми підтримки прийняття рішень і людські інтерфейси, а також вдосконалені системи управління. Огляд основних компонентів Smart Grid представлений на рис. 1.3 [6].

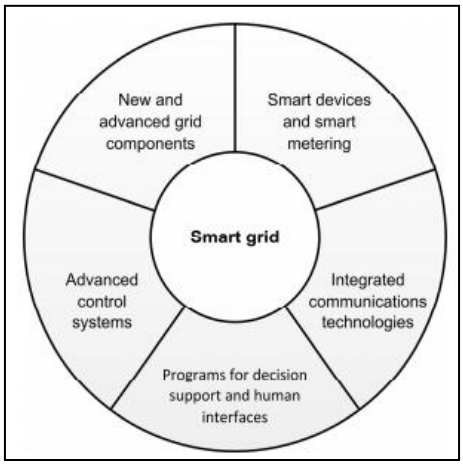


Рисунок 1.3 – Основні компоненти Smart Grid

Microgrid можуть генерувати і розподіляти енергію з використанням різних джерел енергії, таких як вітряні турбіни, паливні елементи і фотоелектричні системи, які підключені до пристроїв зберігання, які допомагають в постійному подачі місцевих навантажень і знижують перебої в подачі електроенергії. Є два типи локальних навантажень. Перший - це чутливе навантаження, яка відноситься до постійного навантаження, а другий - нечутливе навантаження, що є навантаженням, яка може бути відключена в разі виникнення перешкод в основній grid.

Microgrid можуть працювати в двох режимах:

– Режим підключення до grid: де, як видно з назви, мікросхема підключена до grid і може або отримати від неї енергію, або передати їй енергію.

– Острівний режим: в цьому режимі microgrid працює автономно. Його мета - задовольнити потреби місцевих вантажів, створюючи необхідну кількість енергії, не покладаючись на grid комунальних послуг [7].

### 1.1.2 Варіанти архітектур Smart Grid і Micro Grid

Smart Grid - це системи систем з широким охопленням, що об'єднують електроенергію, інформацію, комунікації, бізнес-процеси і різноманітні прилади, на додаток до взаємозв'язку з іншими системами. Проблема взаємодії пов'язана з інтеграцією різних компонентів різними учасниками (промисловими, кінцевими користувачами) і побудовою у відповідності з різними стандартами.). В якості складової частини технічної довідкової архітектури представлена структура моделі інтелектуальних мереж (SGAM), див. рис. 1.4.

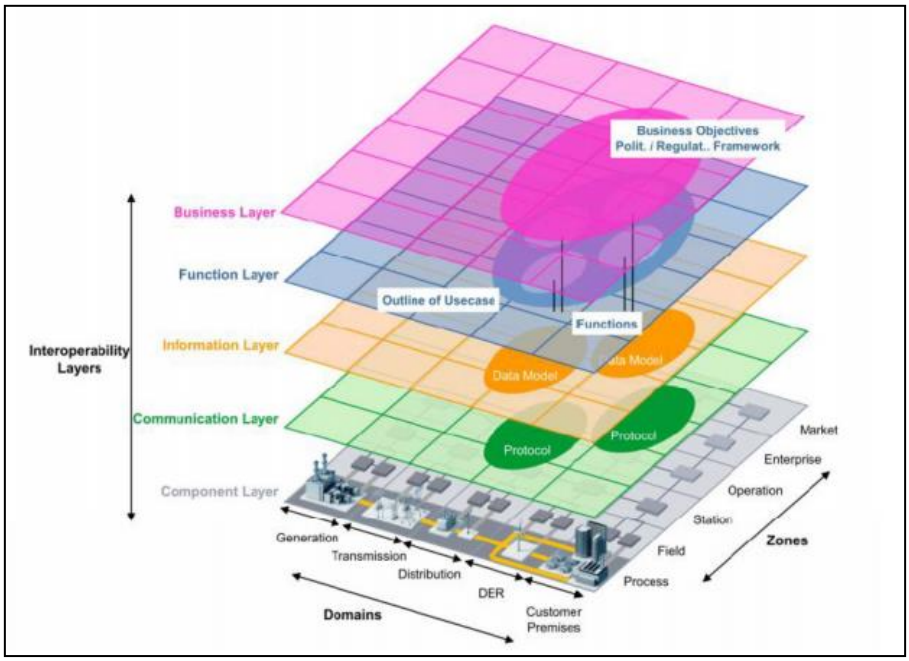


Рисунок 1.4 – SGAM - архітектурний режим Smart Grid

Рисунок 1 показує, що SGAM є тривимірна модель, яка об'єднує вимір п'яти рівнів взаємодії (бізнес, функція, інформація, зв'язок і компонент) з двома вимірами площині Smart Grid, тобто зонами (що представляють ієрархічні рівні управління енергосистемою: процес, поле, станція, експлуатація, підприємство і ринок) і домени (охоплюють цілий ланцюжок конверсії електроенергії: масове виробництво, передача, розподіл, розподілені енергетичні ресурси і приміщення для клієнтів) [4].

Smart Grid можна розглядати як ієрархічну тришарову взаємопов'язану структуру, як показано на рисунку 1.5

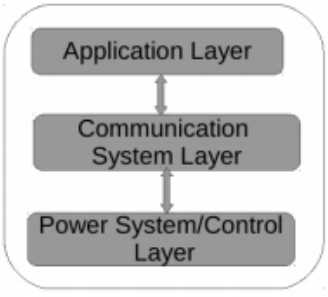


Рисунок 1.5– Концептуальна модель

Шар енергосистеми Smart Grid складається з децентралізованої генерації з відновлюваних і невідновлюваних джерел, високої і середньої напруги і до низької напруги. Шлях передачі контролюється класом пристрою, відомого як інтелектуальний електронний пристрій (IED), такий як блок моніторингу фаз (PMU) для вимірювання миттєвої напруги

шини, лінійного струму і частоти. Інші пристрої включають цифрові реєстратори порушень, реклоузери і конденсаторні банки. Також, датчики, автоматичні фідерні перемикачі та конденсаторні контролери використовуються для управління і контролю домену поширення. Це означає, що для забезпечення підтримки пристроїв, що генерують дані і систему управління ними, потрібна надійна архітектура [8].

У таблиці 1.1 представлені архітектурні особливості, які забезпечують керівництво для своєчасної реалізації інтелектуальної мережі [8].

Таблиця 1.1 - Архітектурні характеристики Smart Grid

| Особливість | Визначення |
|---|---|
| Масштабованість | Просте розширення та розширення архітектури |
| Повсякденність | Незалежний доступ до місця розташування авторизованим користувачам |
| Взаємодія | Безпечний зовнішній обмін інформацією між двома або більше мережами або пристроями |
| Цілісність | Гарантує роботу під час переривань і надійності |
| Стандартизація | Відкрите та чітко визначене з'єднання елементів мережі |
| Можливість модернізації | Віддалене програмне забезпечення, налаштування та алгоритми оновлення |

*Microgrid Energy Management System*

Великі постачальники EMS / DMS надають модулі додатків, які допоможуть використовувати Microgrid. Ринок мікро-листків швидко зростає, але немає типової форми Microgrid Energy Management System.

Платформна архітектура буде підходящою, коли ринок MGEMS буде рости в аналогічній формі системи управління енергією в масштабах всієї області, див. рис. 1.6. В цьому випадку Microgrid буде побудований з більш масштабним пілотованим або безпілотним центром, а одна центральна система управління енергією може обробляти всі множинні дочірні мікрографи.

1) Alstom Grid

Alstom Grid має свою платформу e-terra і безліч відповідних електронних терас, заснованих на базовій платформі в системі генерації / передачі енергії. Для MGEMS для прогнозування і планування надається електронний трафік для планування, і для роботи розподілених ресурсів передбачений e-terradisgen. Крім того, e-terraDRBiznet надається для відповіді на запит.

2) Siemens

Siemens має платформу Spectrum Power і безліч відповідних Spectrum PowerCC, заснованих на базовій платформі в системі генерації / передачі енергії. Передбачена система Spectrum Power 7 MGMS (Microgrid Management System) як MGEMS, де реалізовані спеціальні функції, такі як створення і управління навантаженням, додатки для прогнозування і додатки оптимізації [3].

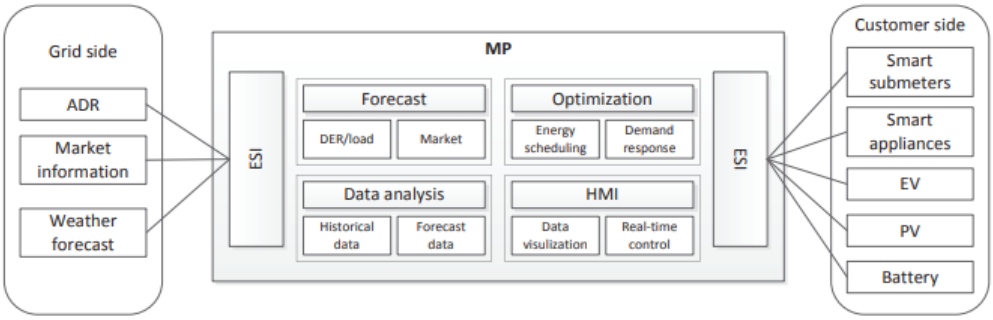


Рисунок 1.6 – Системна архітектура реалізації платформи Microgrid [9]

### 1.1.3 Методи і способи розподілу електричної енергії в різних архітектурах Smart і Micro Grid

Близько 8-10% електричної енергії, що з'являється на терміналах генератора, буде втрачено на шляху до споживачів в мережах передачі та розподілу. Передавальна система має важливе завдання - мінімізувати втрати енергії та підтримувати стабільність системи. Тому важливим є збереження здоров'я мережі шляхом постійного моніторингу та контролю. Відправною точкою моніторингу є система енергоменеджменту (EMS). EMC - це центральна нервова система трансмісійної сітки, що надає комунальним підприємствам можливість керувати генерацією; а також збирати, управляти та відправляти потужність на рівні передачі. EMS виконує оптимальний аналіз потоку потужності та рекомендує оптимізаційні дії.

Широкоорієнтована система моніторингу (WAMS) є високошвидкісною, ієрархічною мережею фазових вимірювальних пристроїв (PMU), метою яких є інформування фазових вимірювань напруги та струму (амплітуда, частота та фаза). За умови достатньої кількості фазерів у реальному часі, можна відслідковувати стан сітки (напруга та фазовий кут кожної шини). Таким чином, WAMS підвищує ситуативну обізнаність існуючої системи EMS на базі SCADA, додаючи функціональні можливості моніторингу, контролю та захисту в режимі реального часу.

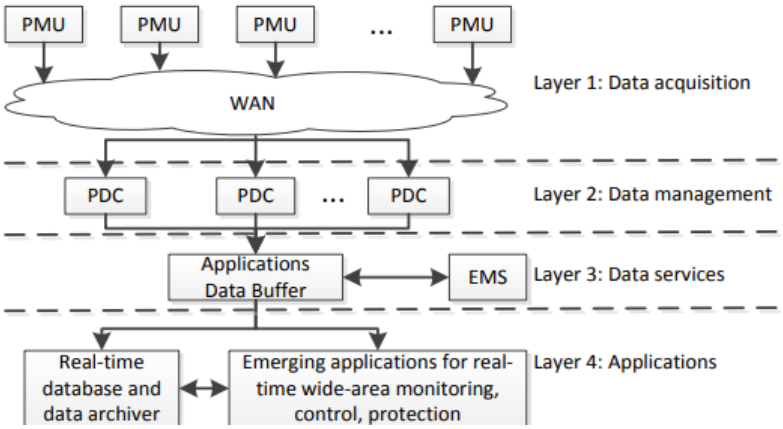


Рис 1.7 – Загальна архітектура WAMS

WAMS складається з чотирьох компонентів: синхронізованих блоків вимірювання фаз, концентраторів фазових даних (PDC), глобальної мережі (WAN) та в реальному часі бази даних і архіватора даних. На рисунку 1.7 показана чотиришарова загальна архітектура WAMS. PMU передають фазову інформацію в PDC на рівні 2 через WAN. PDC зіставляють дані з позначкою часу і пересилають дані в служби даних на рівні 3. Служби даних відстежують дані для втрати, помилок і синхронізації на додаток до надання даних в необхідному форматі додатків на рівні 4. Рівень 4 складається з бази даних і архіватора даних в режимі реального часу, який відповідає за збір і архівування даних для аналізу і оцінки. Цей рівень складається з додатків для моніторингу, аналізу, управління і захисту. Ці широкосмугові додатки класифікуються як управління коливаннями, управління напругою, контроль частоти і функції контролю температури лінії.

Основні причини втрат енергії в розподільчій мережі включають: індуктивний реактивний вплив кабелів і трансформаторів на мережу та коливання навантаження [10].

З технічної точки зору збільшується ймовірність кібератак в Smart Grid через залежність від інтелектуальних електронних пристроїв, гнучких комунікаційних інфраструктур, розподілених центрів управління і сучасної інфраструктури вимірювань.

Кібер-інфраструктура збільшує комунікаційні можливості, автоматизацію і контроль, а також використовує стандартизовані інформаційні технології. У поєднанні з посиленням мотивації для атак кібербезпека Smart Grid являє собою актуальну інженерну проблему.

У таблиці 1.2 наведені статистичні дані про недавні повідомлення засобів масової інформації про випадки перебоїв з подачею електроенергії по всьому світу. Виходячи з повідомлень про отримані випадки, більшість з них пов'язані зі зловмисною кібератакою.

Таблиця 1.2 - Зведена статистика недавно зареєстрованих випадків перебоїв з подачею електроенергії

| Атрибут | Процент (%) | Атрибут | Процент (%) |
|---|---|---|---|
| Зловмисна атака | 71.4 | Помилка оператора | 28.6 |
| Вирішено протягом 48 год | 76.4 | Вирішено через 48 год | 23.6 |
| Постраждалі> 100 000 чоловік | 71.4 | Порушено <100 000 | 26.6 |
| Вирішено внутрішньо | 50.0 | Вирішено ззовні | 50.0 |

Дослідження і механізми кібербезпеки фокусуються на обміні даними між IED-пристроями і центрами управління і використовують орієнтовані на інформацію метрики продуктивності. Існує значна потреба в кількісному обліку фізичних наслідків кібератак, так як кінцевою метою Smart Grid є забезпечення надійної і безпечної доставки енергії. Вплив, який даний набір даних надає на можливості доставки енергії дозволяє розставити пріоритети щодо пом'якшення[11].

*Розширені операції Microgrid*

Розширена, взаємопов'язана система Microgrid повинна відповідати всім вимогам по експлуатації та підключенні, які повинні задовольняти електричні мережі.

Незалежно від того, чи є обладнання і програмне забезпечення комерційними або звичайними, компоненти повинні бути сумісні і з інтерфейсами, які відповідають функціональним стандартам, визначеним EMS.

Кожна електрична утиліта повинна надавати на запит послугу мережевого з'єднання будь-якому споживачеві, що обслуговується електричною корисністю. Для цілей цього пункту термін «послуга мережевого з'єднання» означає послугу споживачу електричної енергії, відповідно до якого на місці експлуатації об'єкта на об'єкті споживача підключається місцевий розподільний пристрій [12].

*Система управління енергією Microgrid*

Прогнозування енергетичної діяльності виконується в різних часових масштабах. А передбачені дані подаються в процес оптимізації для операцій з microgrid. EMS повинна приймати управлінські рішення для оптимізації потоків потужності шляхом настройки потужності, що імпортується з / або в сітку, контрольованих навантажень і диспетчерських розподілених енергетичних ресурсів. EMS збирає величезну кількість даних про енергетичні навантаження та енергетичний ринок. Зібрані дані повинні бути проаналізовані належним чином, забезпечуючи розуміння, щоб краще зрозуміти характеристики

енергетичної діяльності. Це може бути додатково використано для підвищення ефективності прогнозів і моделей оптимізації, див. рис. 1.8 .[9]

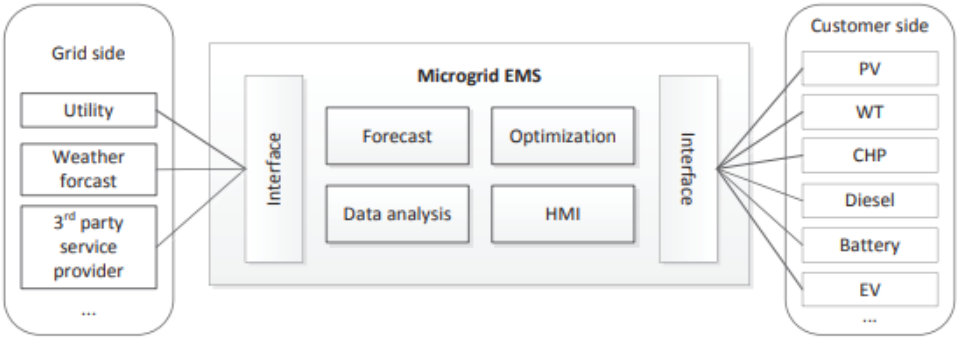


Рисунок 1.8 – Ілюстрація системи управління енергією Microgrid

Для забезпечення безпеки, стабільності та високого рівня якості електроенергії та вирішення проблем взаємодії інтеграції компонентів різних систем використовують Smart та Micro Grid. Їх функціональні можливості надійно виявляють будь-які несправності в зоні захисту та забезпечують ефективний спосіб підвищення надійності системи. Вони намагаються задовольнити потреби споживачів та згенерувати необхідну кількість енергії за допомогою вдосконалення Smart та Micro Grid. Щоб мінімізувати втрати енергії потрібно проводити постійний моніторинг та контроль, який дозволяє збирати, управляти та відправляти потужність на рівні передачі, виконувати оптимальний аналіз потоку потужності та рекомендувати оптимізаційні дії. Високошвидкісною мережею фазових вимірювальних пристроїв є широкоорієнтована система моніторингу, яка підвищує ситуативну обізнаність системи додаючи можливості контролю та захисту в режимі реального часу. Для точного прогнозування енергетична система повинна чітко проаналізувати зібрані дані для оптимізації потоків потужності розподілених енергетичних ресурсів.

## 1.2 Аналіз вимог до кібербезпеки систем Smart Grid і Micro Grid

### 1.2.1 Класифікація атак на Smart Grid і Micro Grid

В Smart Grid існують чотири основні типи кібератак: атака пристрою, атака даних, атака приватного життя і атака доступності мережі. Ці атаки перераховані в таблиці 1.3. Вони мають різні цілі і часто є будівельними блоками більш складних атак. Атака пристрою спрямована на компрометацію (контроль) мережевого пристрою. Це перший крок складної атаки, в якій скомпрометований пристрій буде використовуватися для запуску додаткових

атак, таких як атаки даних і атаки доступності мережі, в Smart Grid або виконання шкідливого фізичного приведення в дію (якщо це елемент управління).

Таблиця 1.3 – Основні види кібератак в Smart Grid

| Назва | Опис |
|---|---|
| Атака пристрою | Він спрямований на компроміс (контроль) мережевого пристрою. Часто це перший крок складної атаки |
| Атака даних | Він намагається змагально вставити, змінити або видалити дані в мережевому трафіку, щоб ввести smart grid в оману, щоб приймати неправильні рішення |
| Атака конфіденційності | Вона спрямована на вивчення / виведення особистої інформації користувачів, аналізуючи дані про використання електроенергії |
| Атака на доступ до мережі | Він спрямований на використання або придушення комунікаційних та обчислювальних ресурсів інтелектуальної мережі та призвести до затримки або невдачі зв'язку. |

Наприклад, скомпрометований IED (Intelligent Electronic Devices), також як автоматичний вимикач, може порушити схему зловмисно і привести до відключення електроенергії. Іншим прикладом є те, що скомпрометований мережевий пристрій може різко збільшити навантаження, щоб викликати переповнення схеми. Щоб протистояти атакам пристроїв, необхідний суворий контроль доступу. Атака даних намагається вставляти, змінювати або видаляти дані або команди управління в мережевому трафіку, щоб ввести smart grid в оману, щоб приймати неправильні рішення / дії [13].

Шкідливі атаки засновані на цілях безпеки Smart Grid, тобто доступності, цілісності і конфіденційності.

– Атаки, спрямовані на доступність, також звані атаками типу «відмова в обслуговуванні» (DoS), спроби затримати, заблокувати або пошкодити зв'язок в Smart Grid.

– Атаки, спрямовані на цілісність, націлені на навмисну і незаконну зміну або порушення обміну даними в Smart Grid.

– Атаки, спрямовані на конфіденційність, призначені для отримання несанкціонованого інформації з мережевих ресурсів в Smart Grid.

*Атаки відмови в обслуговуванні*

Існуючі DoS-атаки можуть відбуватися на різних комунікаційних рівнях в Smart Grid, які показані в таблиці 1.4.

Таблиця 1.4 – Атаки відмови в обслуговуванні в енергосистемах

| Рівень зв'язку | Атаки в енергосистемах |
|---|---|
| Прикладний рівень | - |
| Мережа | Рух затоплення |
| Транспортний шар | Буферне затоплення |
| Рівень MAC | ARP-спуфінг |
| Фізичний шар | Глушіння на підстанціях |

Прикладний рівень. Атаки нижнього рівня фокусуються в основному на пропускної здатності каналів зв'язку, комп'ютерів або маршрутизаторів. Однак DoS-атаки на рівні додатків спрямовані на вичерпання ресурсів комп'ютера, таких як пропускна здатність ЦП. Атаки прикладного рівня можуть легко перевантажити комп'ютер з обмеженими обчислювальними ресурсами, затопивши обчислювальні запити.

Мережевий і транспортний рівні. Відповідно до моделі протоколу TCP / IP ці два рівня повинні забезпечувати контроль надійності для доставки інформації по багато перехідних комунікаційних мереж. DoS-атаки на обох рівнях можуть серйозно погіршити наскрізну продуктивність зв'язку, таку як атаки з розподіленим трафіком і поширення хробака в Інтернеті. Останнім часом в кількох дослідженнях оцінювався вплив DoS-атак мережевого / транспортного рівня на продуктивність мережі енергосистем. Наприклад, недавнє дослідження вивчило вплив атаки з переповненням буфера на мережу SCADA на базі DNP3 з використанням реального апаратного і програмного забезпечення системи SCADA і показало, що поточна система SCADA досить уразлива для атаки DoS .

Рівень MAC. Рівень MAC відповідає за надійний зв'язок точка-точка, а також за справедливість. Зловмисник (наприклад, скомпрометований пристрій) може навмисно змінити свої параметри MAC (наприклад, параметри відкату), щоб мати кращі можливості доступу до мережі за рахунок зниження продуктивності інших, які спільно використовують один і той же канал зв'язку. В Smart Grid спуфінг являє собою відносно небезпечну загрозу на рівні MAC, оскільки він націлений як на доступність, так і на цілісність. Зловмисник, користуючись відкритістю полів адреси в кадрі MAC, може маскуватися під інший пристрій для відправки неправдивої інформації на інші пристрої. Наприклад, в мережі електропідстанції зловмисний вузол може транслювати пакети протоколу ARP для відключення з'єднань всіх IED з вузлом шлюзу підстанції.

Фізичний шар. Глушіння каналу є одним з найбільш ефективних способів запуску DoS-атак фізичного рівня, особливо для бездротового зв'язку. Оскільки зловмисникам

потрібно тільки підключатися до каналів зв'язку, їм дуже легко запускати DoS-атаки на фізичному рівні. В Smart Grid, оскільки бездротові технології будуть широко використовуватися в локальних системах, бездротові перешкоди стають основною атакою фізичного рівня в таких мережах.

*Атаки на чесність і конфіденційність*

На відміну від DoS-атак, які можуть бути запущені на різних рівнях, атаки, націлені на цілісність і конфіденційність в цілому, відбуваються на прикладному рівні, оскільки вони намагаються отримувати або маніпулювати інформацією про дані в Smart Grid.

Атаки, спрямовані на цілісність даних, намагаються приховано змінити дані, щоб пошкодити обмін важливою інформацією в Smart Grid. Метою може бути або інформація про клієнтів (наприклад, інформація про ціни і залишок на рахунку), або значення стану енергосистем (наприклад, показання напруги і стан роботи пристрою). Оскільки така інформація в енергосистемах цінна як для кінцевих користувачів, так і для комунальних підприємств, в енергосистемах використовуються відмовостійкі методи і методи перевірки цілісності для захисту цілісності даних.

Існує ряд робіт, спрямованих на створення і протидію новим класам помилкових атак з використанням даних. Наприклад, атаки на введення помилкових даних були поширені на ринок електроенергії, щоб навмисно маніпулювати інформацією про ринкові ціни. Це може привести до значних фінансових втрат для соціального забезпечення. Атака перерозподілу навантаження - це ще один особливий тип атак з помилковим введенням даних, в яких можна атакувати тільки вимірювання з інжекцією шини навантаження і вимірювання потоку потужності в лінії. Такі атаки є реалістичними атаками з введенням помилкових даних з обмеженим доступом до певних лічильників. У таблиці 1.5 класифікуються існуючі хибні атаки з використанням даних і пов'язані з ними дії на домени Smart Grid.

Таблиця 1.5 - Класифікація помилкових атак з використанням даних.

| Цільові системи | Вплив |
|---|---|
| DC SCADA | Невірна оцінка стану |
| AC SCADA | Невірна оцінка стану |
| Ринок електроенергії | Потенційні фінансові втрати |

У порівнянні з зловмисниками, націленими на цілісність, зловмисники, націлені на конфіденційність, не мають наміру змінювати інформацію, передану по високовольтних електромережах. Вони прослуховують канали зв'язку в електричних мережах для

отримання необхідної інформації, такої як номер рахунку клієнта і споживання електроенергії. Типовими прикладами є прослуховування телефонних розмов і аналізатори трафіку[11].

*Аналіз атак в Microgrid*

Атаки можуть бути спрямовані на те, щоб поставити під загрозу одну з трьох цілей безпеки: доступність, цілісність або конфіденційність.

Фізичні передумови і поточний стан справ в управлінні енергосистемою накладають ряд обмежень на потенційні кібератаки. Важко заподіяти фізичну шкоду енергетичному устаткуванню за допомогою кібератак. Кожен вхідний параметр для силового обладнання перевіряється за допомогою внутрішнього алгоритму управління з рядом допустимих значень. Цей діапазон забезпечує безпечну роботу пристрою для запобігання фізичного пошкодження. Захисні пристрої по всій сітці безперервно перевіряють неприйнятні умови і автоматично ізолюють електричні несправності. Це не заважає зловмисникові досягти неприйнятного стану в сітці, але обмежує можливості поширення помилки. Крім того, захисні реле жорстко підключені до ліній електропередачі та, як такі, не можуть бути атаковані з кібер-домену.

*Розподілена відмова в обслуговуванні (DDoS)*

Атаки з розподіленим відмовою в обслуговуванні (DDoS) вивантажують ресурси системи, відправляючи запит на флуд, щоб запобігти доступу законного користувача до системи. Ефекти DDoS-атак на інтелектуальну мережу можуть бути катастрофічними. Атаки DDoS використовують помилки в мережевих протоколах, так що системі жертви доводиться витрачати більше часу і ресурсів на обробку невірного запиту зловмисників.

Аналіз побічних каналів:

1) Довідкова інформація. Моніторинг в режимі реального часу необхідний для забезпечення ситуаційної обізнаності про умовах Microgrid і забезпечення постійного доступу до електроенергії для споживачів.

2) Агрегація збоку бокового каналу часу з використанням зв'язку енергетичного лічильника: аналіз побічних каналів витягує інформацію, спостерігаючи за артефактами реалізації.

На рисунку 1.9 зображена тактика атаки на аварію в Microgrid [14]:

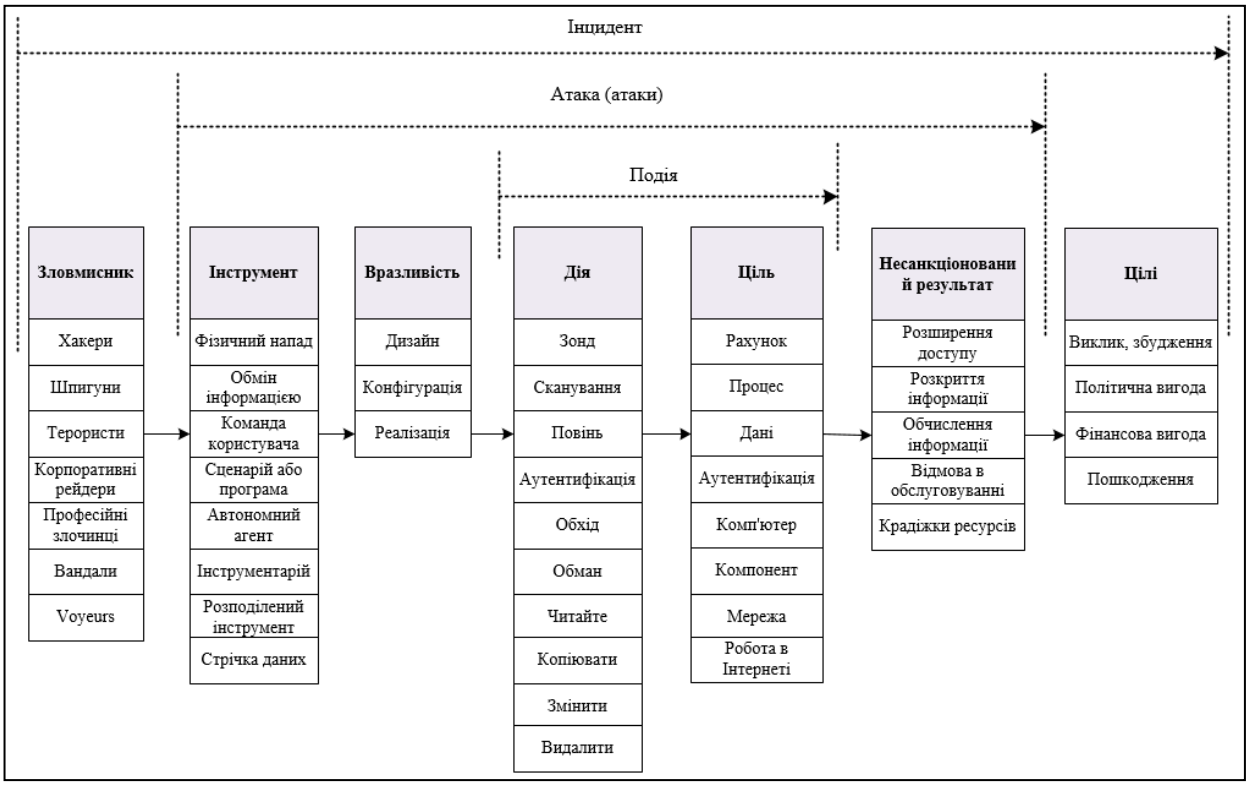


Рисунок 1.9 – Тактика атаки на аварію

### 1.2.2 Вимоги до кібербезпеки Smart Grid і Micro Grid згідно діючих стандартів

Вимоги безпеки Smart Grid відрізняються від інших критичних інфраструктур. Цілі безпеки інтелектуальної мережі можна розділити на три групи:

– Доступність даних
– Цілісність даних
– Конфіденційність даних

Для того, щоб виконувати постійно зростаючий попит на навантаження, важливо керувати енергосистемою з максимальною потужністю. Для безпечної та надійної роботи енергосистеми оператори повинні контролювати систему, оскільки вона проходить через різні режими роботи. Різні інтелектуальні електронні пристрої (IED), наприклад, пристрої віддаленого терміналу (RTU), використовуються для контролю стану системи. Ці дані вимірювань можуть бути пошкоджені зловмисником або можуть бути відсутніми через несправність датчика. Оператори енергосистем повинні мати впевненість у даних вимірювань. З цієї причини стан оцінки широко використовується операторами енергосистеми для обчислення станів системи. Алгоритми оцінки стану можуть виявити будь-які погані дані та забезпечити високу точність оцінки за допомогою обмеженого вимірювання [15].

Структурний підхід до забезпечення систем ICT, таких як Smart Grid, вимагає, щоб результати оцінки ризику входили до системи управління безпекою та ризиками. Як приклад, стандарт HMG IS1 розглядає оцінку ризику як "знімок" дослідження ризиків. Національний стандарт HMG IS1 визнає, що на ранньому етапі розробки можлива лише рудиментарна концепція системи, її оточення та відповідні ризики. Він поширює ітераційний підхід, покращуючи оцінку ризику, коли формується системний дизайн. Стандарт HMG IS1 використовує високо структурований підхід, що забезпечує прозорість щодо визначення рейтингу ризику.

Стандарти для інтеграції розподілених енергетичних ресурсів і зберігання в системах передачі та розподілу, які належним чином регулюють перешкоди, які вони можуть сформувати при увімкненні та вимкненні (запобігання можливим каскадним впливам на умови спрацьовування), будуть необхідними для забезпечення стабільності та надійності інтелектуальної мережі. Для цього потрібні належні стандарти для моделювання таких ресурсів.

Заходи до кібербезпеки вже існують для певних програм та доменів. Вони відрізняються деталізацією та обсягом, класифікуючи процес, орієнтований на технічні стандарти. Деякі стандарти звертаються до оператора, в інших - дуже детальні вимоги щодо виконання. Деякі стандарти складають відповідні документи [16]:

– IEC 62351-1 до 6, Управління енергетичними системами та пов'язаний з ним обмін інформацією - безпека даних і засобів зв'язку.

– NERC CIP-002 і CIP-003 до CIP-009.

– IEEE 1686-2007, Стандарт IEEE для підсистем інтелектуальних електронних пристроїв підстанцій (IEDs), Інституту інженерів з електротехніки та електроніки.

– ISO / IEC 27001: 2005, Інформаційні технології - Технології безпеки - Системи управління інформаційною безпекою - Вимоги

– ANSI / ISA-99, безпека для промислової автоматизації та систем управління

– Спеціальна публікація NIST 800-82

З точки зору електрозв'язку важливо повністю використовувати можливості, передбачені стандартом IEC 61850. Використовуваний загальний стандарт забезпечує не тільки сумісність IEDs (Intelligent Electronic Devices) від різних постачальників, але і надає кошти для інтеграції різних типів DER в систему. Останнє можливо з новою частиною стандарту IEC 61850-7-420, яка до сих пір реалізована тільки в деяких експериментальних пілотних проектах, таких як в проекті MoreMicroGrids.

У стандарті IEC 61850 найменша частина функцій, функціональних елементів, представлена як логічні вузли (LN). Логічні вузли знаходяться в певних фізичних пристроях

(PD), які зазвичай є IED. Зазвичай IED містить кілька логічних вузлів. Набір логічних вузлів формує фактичну функцію захисту або управління. LN, що утворюють одну функцію, можуть бути розподілені між кількома PD. Це дозволено шляхом визначення логічних з'єднань (LC) між LN, щоб вони могли зв'язуватися один з одним і діяти як єдиний об'єкт. LC між різними PD використовує одну або більше фізичних з'єднань (PC) [1].

*Microgrid standards*

Основними кібератаками, які загрожують Smart і Micro Grid є атаки пристрою, даних, конфіденційності та атака на доступ до мережі. Вони спрямовані поставити під загрозу: доступність, цілісність або конфіденційність. Щоб забезпечити безпечну роботу пристрою потрібно за допомогою внутрішнього алгоритму управління безперервно перевіряти умови та ізолювати електричні несправності. За допомогою стандартів для інтеграції розподілених енергетичних ресурсів регулюються перешкоди, що можуть сформуватися при увімкненні та вимкненні. Для цього важливо використовувати можливості стандарту IEC 61850, який забезпечує сумісність інтелектуальним електронним пристроям та є ключовим рішенням для управління та передачі інформації.

IEC 61850 є стандартом для проектування автоматизації електричних підстанцій. У новій редакції додано більше можливостей для розподілених енергетичних ресурсів та для відповідності сучасним енергосистем. Він визначає електричні пристрої та структуру зв'язку для стандартизації компонентів і візуалізації підсистеми. Є багато бажаних функцій, які важливі для microgrid. Наприклад, структуровані дані дозволяють SCADA (Supervisory Control And Data Acquisition) отримувати доступ не тільки до точок даних, але і до моделей пристроїв. Стандарт може бути зіставлений з рядом застарілих протоколів, особливо з об'єктами спільної об'єктно-орієнтованої підстанції (GOOSE), які забезпечують швидкий зв'язок між вузлами. IEC 61850 пропонується в якості одного з ключових рішень для управління і передачі microgrid. Приклад microgrid з лініями зв'язку і протоколами показаний на рисунку 1.10 [17].

IEEE 1547.4 охоплює ключові міркування для планування і роботи Microgrids. Це включає в себе: вплив напруги, частоти, якості електроенергії, включення єдиної точки загальної зв'язку (PCC) і декількох PCC, схем захисту і модифікацій, моніторингу, обміну інформацією і контролю, розуміння вимог навантаження клієнта, знаючи характеристики розподілених енергетичних ресурсів, визначаючи стійкий стан і перехідні умови, розуміючи взаємодії між машинами, резервні поля, скидання навантаження, реакцію попиту, завантаження холодної нагрузки, додаткові вимоги до обладнання та додаткові функції, пов'язані з інверторами [18].

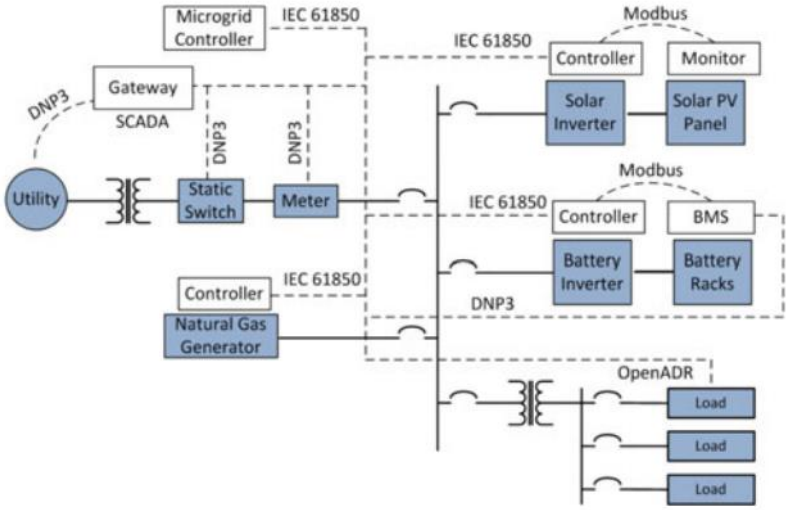


Рисунок 1.10 – Конфігурація прикладу мікросмужкових комунікацій

### 1.2.3 Існуючі стандарти і пов'язані з ними кіберзагрози

Два найбільш використовуваних протоколи для системної автоматизації і управління в електроенергетиці - це протокол розподіленої мережі (DNP3.0) для систем диспетчерського управління та збору даних (SCADA) і служби повідомлень MMS 61850 (MMS), повідомлення про події загальної об'єктно-орієнтованої підстанції (GOOSE ) і повідомлення семплірованних виміряних значень (SMV) в більш пізніх системах.

Незважаючи на те, що ці протоколи дозволили децентралізувати, підвищити надійність і більш точний контроль енергосистеми, вони привели до деяких уязвимостям з точки зору кібербезпеки. Кожен з вищезазначених протокольних костюмів має свої власні уразливості, які раніше використовувалися для запуску успішних атак на електричні мережі. Наприклад, [19], представили успішну атаку маніпулювання даними в пакеті DNP3, який має 4 об'єкти керуючого реле для роботи 4 автоматичних вимикачів на підстанції. Атака емуляції GOOSE була представлена для того щоб генерувати команди перемикання шкідливих вимикачів як повідомлення GOOSE. Ці атаки залишалися неясними з мережі IDS, оскільки зловмисники встановлювали підроблені дані в якості законних мережевих пакетів, але зі шкідливим контентом. Основним посередником у таких атаках є те, що мережі зв'язку енергосистеми повинні підтримувати роботу мережі в режимі реального часу. Тому на обмін комунікаційними сигналами накладаються жорсткі вимоги до часової затримки. Оскільки поточні мікроконтролери і інтелектуальні електронні пристрої (IED) мають низьку обчислювальну потужність, такі промислові мережі управління залишаються незашифрованому, а іноді і без аутентифікації. Проведене дослідження показує, що навіть

новітні процесорні технології не можуть задовольняти вимогам часу затримки від 4 мс, встановленим стандартними стандартами IEC 61850 за повідомленнями GOOSE. Оскільки ця робота націлена на виявлення атак, пов'язаних з управлінням, то для управління статусами вимикачів в досліджуваній системі вибирається протокол обміну повідомленнями видавця / передплатника GOOSE. Як буде показано нижче, латентність пропонованого алгоритму виявлення припадає на затримку часу в 4 мс, встановлену для обміну повідомленнями GOOSE.

#### 1.2.3.1 Оцінка безпеки МЕК 62351

МЕК61850 - це стандарт зв'язку на основі Ethernet (IEEE 802.3), пропонований для управління і автоматизації електричних підстанцій. Він був розроблений спільно МЕК (Міжнародної електротехнічної комісією) і IEEE з метою забезпечення цілісність, автентичність і конфіденційність різних протоколів, використовуваних в енергосистемах.

У стандарті розглядається інформаційна безпека для операцій управління енергосистемами, і загальна мета полягає в збереженні властивостей конфіденційності, цілісності, доступності та неспростовності в системі, головним чином шляхом впровадження механізмів аутентифікації.

Стандарт розділений на десять різних частин, які адресують різні області.

МЕК 62351-1: перша частина містить загальний огляд стандарту МЕК 62351, в якому викладається мета стандарту, а також короткий вступ в різні глави. У ньому також міститься загальна інформація про безпеку, перерахування загроз безпеки (як ненавмисне, так і навмисне, наприклад, збої устаткування, кібер-хакери і т. д.), А також загальний огляд можливих заходів безпеки. У цій частині також коротко описуються такі поняття, як оцінка ризиків, управління ключами і процеси безпеки, між іншим.

Інформація, що міститься в цій частині стандарту, містить огляд безпеки в енергосистемах, перерахування різних загроз для системи і відповідні вимоги безпеки, які можуть пом'якшити ці загрози. Перерахувань досить повно, починаючи від ненавмисних загроз, таких як стихійні лиха, до навмисних загроз, таких як незадоволені співробітники, промислове шпигунство і хакери.

В цілому, ця частина містить всебічний огляд проблем безпеки, які мають відношення до енергосистеми. Однак в інших частинах стандарту не зачіпають всі проблеми, згадані в цій частині, але зосереджені на контрзаходи, які реально можуть бути реалізовані еволюційним чином.

МЕК 62351-2: Друга частина стандарту МЕК 62351 - це глосарій термінів, що пояснює такі терміни, як Контроль доступу, Безпека даних і т. д..

Список термінів і скорочень, перерахованих в цій частині стандарту, досить великий, надаючи короткий опис кожного перерахованого терміна. Ця частина містить великий список термінів разом з відносно докладним описом кожного елемента.

МЕК 62351-3: Третя частина МЕК 62351 стосується безпеки протоколів на основі TCP / IP, які використовуються для систем автоматизації в домені розподілу електроенергії. Метою є забезпечення достовірності та цілісності даних на транспортному рівні і конфіденційність з використанням механізмів шифрування TLS. Використання TLS також враховує такі загрози, як атаки «середній рівень» і повторні атаки. Ця частина стандарту також вимагає взаємної аутентифікації через сертифікати, і наказує алгоритми і деякі мінімальні довжини ключів, які будуть використовуватися, а також як обробляти анулювання сертифіката.

Частина 3 стандарту МЕК 62351 націлена на протоколи автоматизації енергосистеми на основі TCP / IP і спрямована на досягнення наступних цілей безпеки:

– Захист цілісності повідомлення (Повідомлення не можуть бути змінені або вставлені). Це протистоїть загрозі атаки «людина в середині».

– Конфіденційність повідомлень (шифрування). Це протидіє загрозі підслуховування.

Ключовою частиною МЕК 62351-3 є використання TLS (Transport Layer Security) в якості основного протоколу для забезпечення наскрізної транспортної безпеки для протоколів автоматизації енергосистем разом з сертифікатами X.509 через різних вимог OT (операційна технологія) в порівнянні з IT (інформаційні технології ) стандарт також надає інформацію про те, як усунути ці відмінності.

Стандарт підтримує використання декількох центрів сертифікації (ЦС) в одному ІЕУ з використанням розширення TLS. Це корисно, коли доступ до IED здійснюється з різних адміністративних доменів. Також обробляються анулювання сертифіката та закінчення терміну дії сертифіката.

МЕК 62351-3 не містить конкретного переліку наборів шифрування TLS, які необхідно підтримувати. Замість цього він забезпечує підтримку RSA і DSS як сигнатурних алгоритмів.

Пропоноване використання TLS для протоколів автоматизації енергосистем на основі TCP / IP є підходящим вибором, який використовує протокол замість того, щоб намагатися впровадити пропрієтарні протоколи безпеки. Стандарт залишає вибір

прийнятних наборів шифрів для TLS іншим стандартам, ризикуючи несумісними реалізаціями і використанням наборів шифрів, які не забезпечують достатньої безпеки.

Одна атака, яку не захищає МЕК 62351-3, - це IED-пристрої, які були скомпрометовані зловмисником, оскільки скомпрометовані IED-пристрої і надалі будуть визнані легітимними іншими пристроями в системі.

Додаткова проблема з МЕК 62351-3 для безпечного зв'язку в енергосистемах, яка повинна бути врахована, полягає в тому, що зловмисники можуть використовувати зворотну сумісність, щоб обійти деякі функції безпеки. Якщо IED пропонує безпечну і небезпечну зв'язок, зловмисник може вирішити використовувати небезпечний канал зв'язку, щоб обійти вимоги аутентифікації.

МЕК 62351-4: ця частина стандарту МЕК 62351 призначена для захисту таких профілів, як специфікація виробничих повідомлень (MMS) (Міжнародна організація по стандартизації (ISO), яка використовується в інших стандартах МЕК. Ця частина дає рекомендації для А-профілю, а також Т-профілю на основі TCP / IP. Для А-профілю МЕК 62351-4 описує використання сертифікатів X.509 для аутентифікації додатків, тоді як для Т-профілю TCP стандарт описує, як використовувати TLS в якості рівня між TCP і транспортною службою ISO (Rose and Cass ) з використанням іншого TCP-порту для захищених з'єднань.

У частині 4 стандарту МЕК 62351 описані заходи щодо захисту MMS (специфікація виробничих повідомлень (Міжнародна організація по стандартизації (ISO)). У стандарті пропонується безпеку для А-профілю (тобто безпеки на рівні додатків), а також для Т-профілю на основі TCP / IP.

Безпека для А-профілю (рівня додатки) досягається за допомогою аутентифікації сурогатної суті на основі сертифікатів під час налаштування асоціації. Зокрема, пристрій буде включати в себе сертифікат X.509 разом з міткою часу і сигнатурою на позначці часу з використанням даного сертифіката в запиті асоціації.

Для TCP Т-профілю стандарт рекомендує використовувати TLS між TCP і RFC 1006 на окремому порту.

Основною проблемою захисту МЕК 62351-4 для A-Profile є те, що він не охоплює цілісність повідомлення або конфіденційність. Він охоплює тільки початкову аутентифікацію, але аутентифікація не поширюється на наступні повідомлення в сеансі. Крім того, аутентифікація охоплює тільки тимчасову мітку, включену в початкове повідомлення, і мітка часу повинна бути точною з точністю до 10 хвилин від локальних годинника пристрою. Це залишає A-Profile відкритим, принаймні, трьома різними атаками:

– первинний PDU може бути змінений (крім позначки часу) без анулювання підпису

– значення мітки часу і аутентифікації може бути вилучено з PDU і повторно використано в підробленому PDU на інший пристрій протягом 10 хвилин після відправки вихідного PDU

– оскільки проміжні повідомлення не автентифіковані і не захищені, після первинної перевірки автентичності зловмисник може створювати або змінювати PDU, якими обмінюються дві пристроями

Що стосується безпеки T-профілю, обов'язковий шифр, визначений у стандарті, не використовує ефемерний Diffie-Hellman (* DHE * або * EDH *), але використовує тільки звичайний Diffie-Hellman (* DH *) і, отже, не підтримує ідеальні форвардна секретність (PFS). Якщо бездоганна пряма секретність викликає заклопотаність, тоді стандарт повинен також наказувати шіфровие сюїти, що підтримують PFS. Стандарт також не містить рекомендацій для будь-яких наборів шифрів з використанням еліптичних кривих.

МЕК 62351-5: п'ята частина стандарту МЕК 62351 яка описує безпеку протоколів, що відносяться до IEC 60870-5, і таких похідних, як DNP-3 (IEEE Standards Association). Ці протоколи засновані на повідомленнях, тому аутентифікація повинна виконуватися для кожного повідомлення. Будь-які механізми безпеки повинні враховувати часто обмежену обчислювальну потужність, доступну в порушених пристроях. Оскільки ключі, які використовуються для аутентифікації і / або шифрування, повинні регулярно змінюватися, в цій частині також пропонуються механізми, що дозволяють віддалено оновлювати ключі на пристрої.

Ядром цієї частини стандарту є механізм перевірки автентичності відповідача з використанням HMAC з попередньо розділеними секретними ключами для захисту цілісності даних. Повідомлення (ASDU), які є критичними, можуть бути захищені механізмом аутентифікації запиту-відповіді, де відправляє станція повинна відповісти на виклик, відправлений приймаючій станцією, перед обробкою ASDU.

МЕК 62351-6: Частина 6 стандарту МЕК 62351 захищає протоколи, описані у відповідному стандарті МЕК 61850. У цій частині пропонується розширення до блокам протоколів GOOSE і SMV IEC 61850 (блок даних протоколу), додавши в PDU поле, що містить інформацію, що відноситься до безпеки. Розширення призначене для аутентифікації PDU, що містить підписаний хеш PDU. Ця частина стандарту також додає розширення до мови конфігурації підстанцій (SCL) (МЕК), які дозволяють включати визначення сертифікатів в конфігурацію. У стандарті містяться рекомендації по конфіденційності в разі ослаблених вимог в реальному часі. Пропоновані розширення в

МЕК 62351-6 адресують деякі з погроз, наприклад цілісність повідомлень, і деякий захист від повторення повідомлень.

МЕК 62351-7: інфраструктура енергетичних систем широко використовує взаємопов'язані інформаційні системи для управління операціями. У частині 7 стандарту IEC 62351 описуються моделі об'єктів даних, які будуть використовуватися, які відносяться до енергосистем.

У частині 7 визначені об'єкти даних мережевого і системного управління (NSM), які можуть використовуватися разом з простим протоколом мережевого управління (SNMP) для моніторингу та налаштування такої інфраструктури. Область охоплення полягає в моніторингу і контролі не тільки мереж зв'язку, а й кінцевих пристроїв.

Вплив цієї частини стандарту в основному полягає в створенні загальної структури, що дозволяє управляти і контролювати інфраструктуру зв'язку та інформації, як це показано в енергосистемах. Список можливих об'єктів досить повних, що охоплюють широкий діапазон від аварійних сигналів, до даних стану, вимірів і т. д.

Стандарт не визначає, як ці об'єкти зіставляються з базовим протоколом (наприклад, SNMP), залишаючи це для інших стандартів. Він також не визначає докладно, як контролювати доступ до цих об'єктів.

МЕК 62351-8: Частина 8 стандарту МЕК 62351 визначає системний контроль доступу на основі ролей для інфраструктури енергосистем. Він розглядає різні способи доступу, такі як прямий і віддалений доступ, а також доступ користувачів і автоматичний доступ комп'ютерних агентів. Крім того, стандарт визначає певні обов'язкові права і ролі.

Частина 8 стандарту МЕК 62351 визначає використання управління доступом на основі ролей (RBAC) в енергосистемах. Використання RBAC в енергосистемах дозволяє зменшити кількість дозволів, які повинні бути призначені певним користувачам, так що у них є тільки дозволи, необхідні для виконання своїх обов'язків.

Частина 8 визначає власний протокол для безпечного встановлення сеансу.

МЕК 62351-9: ця частина стандарту призначена для вирішення питань, пов'язаних з управлінням сертифікатами і / або ключами. Він визначає управління криптографічними ключами, а саме, як створювати, поширювати, відкликати і обробляти сертифікати відкритого ключа та криптографічні ключі для захисту цифрових даних і їх зв'язку.

МЕК 62351-10: Частина 10 стандарту МЕК 62351 містить загальні рекомендації по архітектурі безпеки енергосистем. Це включає в себе огляд елементів управління безпекою, які можуть застосовуватися в енергосистемах, а також рекомендації по архітектурі системи про те, як структурувати комунікаційну інфраструктуру енергосистем.

Ця частина стандарту дає всебічний огляд того, як різні стандарти адресують безпеку в системах харчування і автоматизації на різних рівнях. Також є детальний огляд можливих заходів безпеки, починаючи від технологічних засобів контролю безпеки (наприклад, перевірки автентичності, контролю доступу, брандмауерів) до процедурного (наприклад, відповідь на інцидент, рекомендації з кодування), а також нормативні засоби і контроль фізичної безпеки.

*Висновки*

Таким чином, згідно аналізу [20] стандарт МЕК 62351 вирішує проблеми безпеки в енергосистемах, забезпечуючи приватну аутентифікацію, цілісність і конфіденційність даних. У стандарті пропонуються як стандартизовані технології (наприклад, TLS), так і пропрієтарні розширення для промислових протоколів. Стандарт забезпечує значне поліпшення безпеки, забезпечуючи справжність, цілісність і час від часу конфіденційність даних.

Проте, ясно, що стандарт в якійсь мірі обмежений вимогами, пов'язаними з зворотною сумісністю, і, отже, не завжди забезпечує таку саму безпеку, яку можна було б забезпечити, якби була скасована зворотна сумісність. В цілому стандарт забезпечує збалансований підхід, який може бути реалізований з розумними зусиллями і забезпечує розумну ступінь безпеки, якщо він буде реалізований всебічно.

## 1.3 Аналіз особливостей Smart і Micro Grid як об'єкта оцінки і забезпечення кібербезпеки

### 1.3.1 Аналіз відмов архітектурних компонент Smart і Micro Grid

Стратегія кібербезпеки буде враховувати інформацію про вплив, уразливості і погрози для оцінки ризику. У типовому процесі управління ризиками ідентифікуються активи, системи та мережі; оцінюються ризики (включаючи уразливості), впливу і загрози; вимоги до кібербезпеки; і елементи управління кібербезпекою вибираються, впроваджуються, оцінюються по ефективності, вирішуються, а потім контролюються на протязі всього життєвого циклу системи.

National Electric Sector CyberSecurity Organization Resource (NESCOR) розділений на три робочі групи, кожен з яких має різну спрямованість. Група з оцінки загроз, вразливості і пом'якшення наслідків фокусується на розробці стратегій пом'якшення уразливих місць в цьому секторі. Група оцінки вимог до кібербезпеки і оцінки стандартів оцінює вимоги і стандарти кібербезпеки від NIST, DHS, NERC, UCA і інших організацій, щоб визначити, наскільки добре поточні стандарти відповідають цим вимогам. Робоча група по тестуванню

та перевірці технологій кібербезпеки фокусується на розробці методологій і планів тестування нових технологій, які можуть забезпечити захист кібербезпеки [21].

Через кібератаки мережа може зіткнутися з експлуатаційними збоями і втратою синхронізації. Ця відмова в роботі може привести до пошкодження критичних компонентів системи електроживлення, які можуть перервати електроживлення і привести до нестійкості системи, що призведе до високих фінансових штрафів.

Фізичний захист - захист фізичних інфраструктур в Smart Grid. У ньому розглядаються ненавмисні ситуації через збій обладнання, системи і мережі, людських помилок, стихійних лих і несподіваних явищ в інфраструктурах. Для фізичного захисту інтелектуальної сітки були враховані два компонента:

– надійність системи
– відмова в механізмі захисту.

Існує чотири методи забезпечення надійності системи:

1) надійність розподіленої генерації (DG) в розподільній мережі;
2) надійність інфраструктури вимірювань;
3) Надійність мережі перед реалізацією;
4) Підстанції для прийняття рішень.

*Відмова в механізмі захисту*

Механізм розділений на дві частини:

1. Прогнозування та запобігання відмові

Для ефективної роботи smart grid точність повинна полягати в прогнозуванні збою та запобігання виникненню збою. Один з підходів до прогнозування збою полягає в пошуку слабких місць в інтелектуальної сітці. Chertkov розробив підхід до ефективного прогнозування слабких місць в енергосистемі і визначенню можливих режимів відмови при розподілі статичного навантаження. Такий підхід може забезпечити точну прогностичну здатність в пошуку проблемних посилань на основі різних режимів відмови при роботі з навантаженням. Прогнозування помилки короткого замикання і прогнозування її величини в smart grid також важливі для запобігання відмови мережі. Chen представив алгоритм, який виявився ефективним для прогнозування величини короткого замикання в найкоротші терміни.

2. Ідентифікація, діагностика та відновлення відмови

Якщо стався збій, він повинен бути швидко ідентифікований в найкоротші терміни, щоб уникнути пошкоджень. Як тільки несправність була виявлена, її необхідно діагностувати для пошуку основної причини. Коли несправність очищається, мережа повинна бути повторно синхронізована і відновлена до нормальної роботи. Calderaro

представив метод виникнення і виявлення збоїв в інтелектуальних мережах. Метод виявляє відмову в передачі даних і збої в розподільній мережі за допомогою роботи матриці. Також була проведена перевірка методів. Завдяки перевірці виявляється, що метод здатний видалити більшу складність, пов'язану з аналізом даних, і дозволяє швидко оцінювати інформацію, уникаючи при цьому виникнення збоїв в захисті енергосистеми.

Одним з вирішальних кроків є діагностика відмови. Для цієї оцінки існують різні методи, наприклад, тест гіпотези, ступінчаста регресія, поетапний відбір по інформаційним критерієм Akaike's і т. д. Було відзначено, що для всіх випадків немає єдиного методу. Кожен метод має свій власний потенціал в конкретному випадку.

Відновлення відмов є важливою особливістю Smart Grid. Коли відбувається збій, реконфігурація при самовідновленні в інтелектуальній мережі розбиває мережу живлення на самодостатні мережі, щоб зупинити поширення відмови. Для відновлення відмови в мережі Li представив технологію реконфігурації системи самовідновлення з алгоритмом розбиття області, щоб мінімізувати дисбаланс потужності між генерацією (DG) і навантаженням в мережі. Завдяки цьому ефективному алгоритму і правильному управлінню системою його відновлення може бути покращено [22].

*Ідентифікація та оцінка вразливостей Micro Grid*

Ідентифікація потенційних вразливостей з високим рівнем ризику є ключовим аспектом стратегії захисту в поглибленої безпеці і повинна бути складовою частиною загальної програми управління ризиками.

Red-and Blue-Teaming - це два підходи, які можна використовувати як частину оцінки вразливості. Вони можуть використовуватися індивідуально, послідовно або навіть об'єднані в гібридний підхід. Вони також можуть використовувати різні специфічні методології для виявлення і оцінки вразливостей. Суворі зусилля почнуться з повною роботи Blue Team зі збору всієї необхідної інформації в звіт «знань про себе», що дозволяє Blue Team розробити план тестування і провести власні оцінки вразливості, які містять потенційну систему і місію наслідків кібератак [23].

### 1.3.2 Аналіз заходів забезпечення кібербезпеки на етапах життєвого циклу Smart і Micro Grid

Система управління життєвим циклом системи в галузі системного проектування та розробки програмного забезпечення - це процес створення або зміни систем, моделей та методологій, які люди використовують для розробки цих систем. У "Життєвому циклі

розвитку системи" існує п'ять основних етапів: ініціювання, опис, реалізація, операції та обслуговування, утилізація.

Цей цикл стосується всього шляху, який слід дотримуватися під час розробки продукту, забезпечуючи максимальний успіх продукту та мінімальний шанс на невдачу. Такий життєвий цикл був введений в області безпеки та відомий як "Життєвий цикл розробки системи (SDLC)". На рисунку 1.11 показано типовий життєвий цикл розробки системи. [24].


Рисунок 1.11 – Концептуальний вигляд SDLC65

*Життєвий цикл MicroGrid*

Життєвий цикл, показаний на рисунку. 1.12, включає в себе аспекти системної інженерії та концепції систем, адаптовані до контексту MicroGrid. Цей життєвий цикл є послідовним, але не односпрямованим. Ітеративний характер системи дозволяє постійно покращувати наступні результати після проведення попередніх результатів і проведення консультацій із зацікавленими результатами. Крім того, важливо мати на увазі, що процеси перевірки та валідації важливі на кожному етапі циклу, щоб поліпшити правильність і корисність моделей [25].

Мережа може зіткнутися з проблемою кібератаки, яка спричинить експлуатаційні збої і втрату синхронізації. Щоб забезпечити фізичний захист системи використовують основні методи: надійність розподіленої генерації в розподільній мережі, надійність інфраструктури вимірювань, надійність мережі перед реалізацією та підстанції для прийняття рішень. Для прогнозування та запобіганні відмові системи потрібно скористатися підходом пошуку слабких місць, який забезпечує пошук проблемних посилань. Коли з’являється збій в системі потрібно його виявити за допомогою метода виникнення і виявлення збоїв в інтелектуальних мережах.

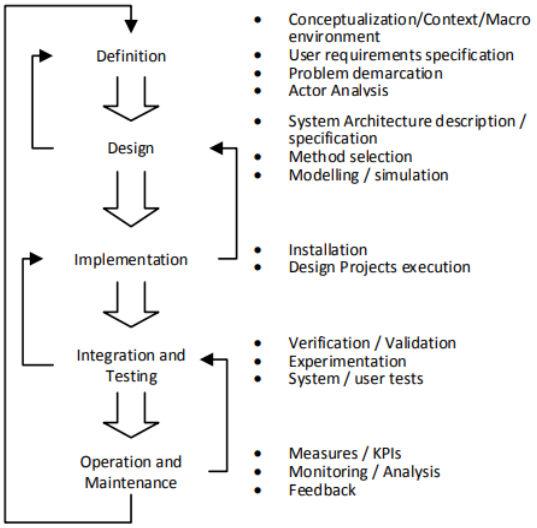


Рисунок 1.12 – Методологія довідки фази життєвого циклу Microgrid

Життєвий цикл Smart і Micro Grid забезпечує великий успіх продукту та низький шанс на невдачу. Він покращує результати після проведення перевірки на кожному етапі, чим поліпшує правильність та корисність моделі.

## 1.4 Аналіз моделей і методів забезпечення кібербезпеки на етапі проектування і експлуатації Smart і Micro Grid

### 1.4.1 Використання технології Blockchain в Smart і Micro Grid

Кібербезпека для електроенергетики стає все більш актуальною національною проблемою. Тому рішення безпеки, розроблені для мереж з інтелектуальною мережею, вимагають більш повного захисту. В цілому визнано, що безпека повинна бути сконструйована в кожному елементі інтелектуальної мережі з самих ранніх етапів процесу проектування. В багатьох випадках безпека є останньою проблемою для виробників обладнання і попереджається тільки після того, як система виявиться вразливою. Постачальники комунальних послуг і виробники продуктів послуг повинні знати про ці несприятливі наслідки, які можуть привести до величезних фінансових втрат для галузі. Вимоги до аутентифікації, авторизації та шифрування повинні бути обов'язковими для всіх продуктів і послуг, призначених для електроенергетики.

*Використання підходу «захист в глибину»*

Одним з основних принципів безпеки для смарт-сітки є перетворення «оптових» атак, які можуть поставити всю систему під загрозу, в «роздрібні» атаки, які обмежені дуже малою областю, на основі підходу до ізоляції і захисту в глибину. Smart grid - це сукупність

декількох мереж з великою кількістю рівнів комунікації між постачальниками, операторами, клієнтами та постачальниками послуг. Тому повинні бути створені кілька рівнів захисних і ізольованих доменів безпеки для пом'якшення оптових атак від всієї системи.

*Посилення традиційних заходів безпеки*

Надійність інтелектуальних мережевих сервісів сильно залежать від інформаційних і комунікаційних технологій і їх кібер-інфраструктури. Постачальники послуг використовують традиційні заходи безпеки, такі як аутентифікація, контроль доступу, авторизація, шифрування даних, інфраструктура з відкритим ключем, брандмауери, аналіз журналів, системи виявлення вторгнень і протоколи мережевої безпеки. Існує значний розрив між їх обмеженнями і новими вимогами безпеки через еволюції технологій і середовищ. Наприклад, використовуючи механізми управління доступом на основі ролей (RBAC) замість управління доступом на основі даних в великому середовищі, ми можемо надати більш масштабовані служби контролю доступу .

Існує багато методів оптимізації, і їх використання залежить від простору рішення і складності рішення проблеми оптимізації. Представлено короткий огляд основних методів оптимізації.

*Точні методи*

Точні методи - це ті, які здатні знайти оптимальне вирішення проблеми. Вони варіюються від дуже загальних методів (корисних для вирішення безлічі завдань оптимізації), таких як Branch and Bound, для алгоритмів, що залежать від проблеми, таких як алгоритм Dijkstra’s.

Загальні точні методи оптимізації можна класифікувати за такими парадигмами:

Евристичний є розширенням алгоритму Dijkstra’s. Це цілеспрямована стратегія обходу графа, здатна знайти шлях найменшої вартості (оптимальне рішення) від заданого вихідного вузла до цільового вузла. Він складається з упорядкування різних можливих шляхів (рішень) і вивчення найбільш перспективних. Алгоритм оцінює якість кожного шляху, використовуючи функцію вартості з плюсом-евристикою, де частина знань - це вартість переходу від вихідного вузла до поточного вузла, а евристика - це оцінка вартості переходу від поточного вузла до цільового вузла. Евристика повинна виконати набір вимог, що гарантують оптимальне рішення.

Гілка і кордон.  Був вперше запропонований Land and Doig. Алгоритм складається з систематичного перерахування рішень-кандидатів через запроваджене дерево пошуку. Алгоритм досліджує гілки дерева, які представляють собою підмножини набору рішень. Хоча алгоритм досліджує гілки, він перевіряє їх на верхню і нижню оціночні оцінки

оптимального рішення. Потім гілки відкидаються, якщо вони не можуть створити краще рішення, ніж краще, знайдене досі алгоритмом.

Динамічне програмування полягає у вирішенні складного завдання, розбиваючи її на послідовність менших і, отже, більш простих підзадач. Тоді рішення більшого завдання виявляється шляхом вирішення окремих менших завдань.

Лінійне програмування використовується для вирішення завдань оптимізації, які представлені лінійною цільовою функцією і обмеженнями лінійної нерівності. Простір рішень являє собою опуклий багатокутник, обмежений кількома площинами (обмеженнями). Загальний вид точних методів зображено на рисунку 1.13:

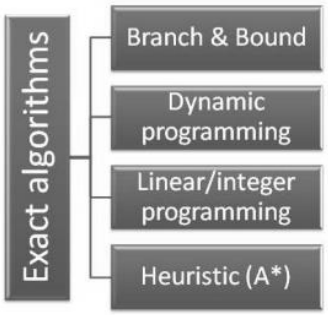


Рисунок 1.13 – Класифікація точних методів на основі парадигми

*Неточні методи*

Детермінований пошук. Ці алгоритми в значній мірі залежать від лінійної алгебри, оскільки вони зазвичай засновані на обчисленні градієнта цільової функції. Зазвичай зближення таких алгоритмів відбувається дуже швидко (потрібна оцінка невеликого числа альтернативних рішень), особливо в порівнянні з алгоритмами стохастичного пошуку. Детерміновані методи шукають стаціонарні точки змінних відгуку, і, таким чином, оптимальне знайдене рішення може бути локальним оптимальним замість глобального оптимуму.

Стохастичний пошук. Стохастичні алгоритми пошуку шукають рішення з використанням місцевих знань, що надаються визначенням околиці або набору приватних рішень. Оскільки вони засновані на рандомізованому процесі пошуку, вони не повинні повертати той же результат для різних прогонів з різним випадковим насінням.

Еволюційні алгоритми. Еволюційні алгоритми використання принципів біологічної еволюції для вирішення завдань оптимізації починаються з сукупності рішень, які розвиваються, покращуючи якість рішень, на рівні кінцевого числа ітерацій. Загальний вид точних методів зображено на рисунку 1.14:

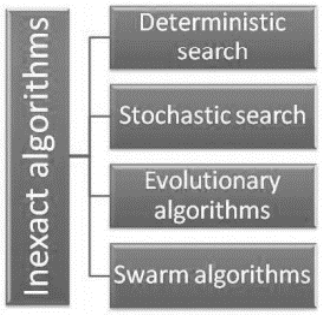


Рисунок 1.14 – Класифікація неточних методів на основі парадигми

Swarm алгоритми. Вони представлені як децентралізовані системи простих однорідних систем, взаємодіючих локально з навколишнім середовищем і один з одним. Незважаючи на відсутність централізованої структури управління агентом, локальнаа взаємодія між ними призводить до глобального поведінки системи в цілому [26].

*Система керування енергією MicroGrid*

EMS на основі лінійних і нелінійних методів програмування

Sukumar пропонує спільне використання потужності, безперервний запуск і змішаний режим MGEMS в режимі «включено-виключено». Режим поділу потужності розглядає торгівлю потужністю з основною мережею, в той час як паливний елемент повинен залишатися в режимі безперервного запуску. Обидва цих режиму вирішуються методом оптимізації лінійного програмування.

Anglani. запропонував оптимальну EMS для віддаленого військового MicroGrid. В якості цільової функції використовується кусочно-лінійна модель споживання палива дизель-генератора. Метод підрахунку дощу також використовується для визначення розміру батареї, заснованого на її життєвому циклі і глибині розряду, для компромісу між операційними і капітальними витратами MicroGrid.

Comodi представив MILP (Mixed-integer linear programming) для торгівлі електроенергією, засновану на моделях EMS для житлового MicroGrid. Метод радіальної основи нейронної мережі використовується для прогнозування вихідної потужності фотоелектричних і сонячних теплових енергетичних систем. Ефективна інтеграція теплового сховища реалізується за допомогою управління тепловим навантаженням. Однак батареї укладені як економічно нездійсненні для інтеграції на ринку житла через їх високі витрати на інвестиції та заміну.

Vergara запропонував EMS з обмеженням безпеки для трифазного житлового MicroGrid. Модель нелінійної оптимізації розроблена для мінімізації експлуатаційних

витрат MicroGrid, в той же час караючи скидання навантаження. Системні збої включені як обмеження для забезпечення надійності MicroGrid.

Tsikalakis та Hatziargyriou розробили централізовану архітектуру для управління енергією MicroGrid з сіткою. Пропонуються дві ринкові стратегії для визначення цінових заявок на участь MicroGrid в енергетичному ринку. Метою першої політики є мінімізація операційних витрат MicroGrid, в той час як друга політика спрямована на максимізацію її прибутку з урахуванням енергетичних транзакцій з основною мережею. Обидві ці оптимальні політики вирішуються з використанням методу послідовного квадратичного програмування.

Panwar представив стратегічний EMS MicroGrid, пов'язаний з сіткою, обмежений операційним вікном номінальної роботи трансформатора і захистом напруги. Розроблена модель мінімізує експлуатаційну вартість MicroGrid з використанням модифікованого методу рішення з градієнтним спусками. Алгоритм прямий перемотування вперед визначає рішення потоку потужності MicroGrid. В цільової функції враховуються три сценарії щодо переваг для користувача, втрат в мережі і вирівнювання навантаження [27].

*EMS на основі динамічного програмування и правил*

Heymann запропонував метод динамічного програмування Bellmans для оптимального управління енергією автономної MicroGrid.

Strelec і Berka представили приблизний підхід до динамічного програмування для подолання прокляття розмірності в пропонованої моделі EMS MicroGrid.

Choudar представив базову ієрархічну структуру на основі SOC для MGEMS і пропоновані ультраконденсатори для регулювання потужності і безперебійної роботи MicroGrid [27].

Blockchain - це цифровий договір, який дозволяє партнеру прямо звіряти транзакцію (наприклад, продаж електроенергії) іншого партнера. Концепція тимчасової мережі вимагає, щоб всі транзакції повинні зберігатися на комп'ютері, який є частиною мережі, що складається з постачальників і клієнтів, які беруть участь в транзакції. Використання технології Blockchain на енергетичних ринках було вперше представлено в 2014 році.

Blockchain - це нова технологія ICT, яка пропонує нові можливості, як приклад вона забезпечує прозорі та зручні для користувача програми, необхідні для реалізації процесу енергоспоживання. Технологія Blockchain була розроблена як механізм перевірки кріптоконверсій, але останнім часом багато досліджень використовують цю технологію для реалізації багатьох різних додатків. Системи на базі Blockchain в основному являють собою комбінацію розподіленого регістра з ім'ям «регістр», децентралізованого консенсусного механізму і деяких криптографічних заходів безпеки. Ці системи в поєднанні зі смарт-

контрактами можуть революціонізувати функціонування транзакційних систем і повністю децентралізувати ринкові платформи.

Blockchain - це однорангова розподілена система регістрів, яка зберігає всі транзакції, що відбуваються в мережі. Основна мета серверів, що входять до складу розподіленої системи, полягає в наданні консенсусу, використання різних консенсусних алгоритмів, про стан Blockchain в будь-який момент часу і зберіганні копії всіх транзакцій. Консенсусний механізм є однією з ключових концепцій Blockchain, він здатний уникнути поширення пошкодженої інформації. У публічному і без дозволу сценарії, тобто в системі без обмежень доступу, надання нової інформації повинно бути пов'язане з певною кількістю ресурсів. Наприклад, механізм консенсусу з підтвердженням роботи вимагає, щоб вузли, які беруть участь вирішували чисельну проблему. Таким чином, він створює (обчислювальні) витрати для додавання нової інформації. Менш дорогі механізми консенсусу можуть забезпечити ефективні альтернативи. Наприклад, аутентифікація користувача на основі хеша дозволяє агентам голосувати за правильність нової інформації на основі їх унікальної ідентифікації, так званої «Доказ Ідентичності» .

Blockchain забезпечує розподілену програмну архітектуру, яка дозволяє агентам (людині або штучно) взаємодіяти без центральної керівної установи і незважаючи на відсутність посередників, системи на основі Blockchain завжди покладаються на правильність визначених правил, і тому вкрай важливо забезпечити безпеку, надійність і точність, див. рис 1.15 [28].

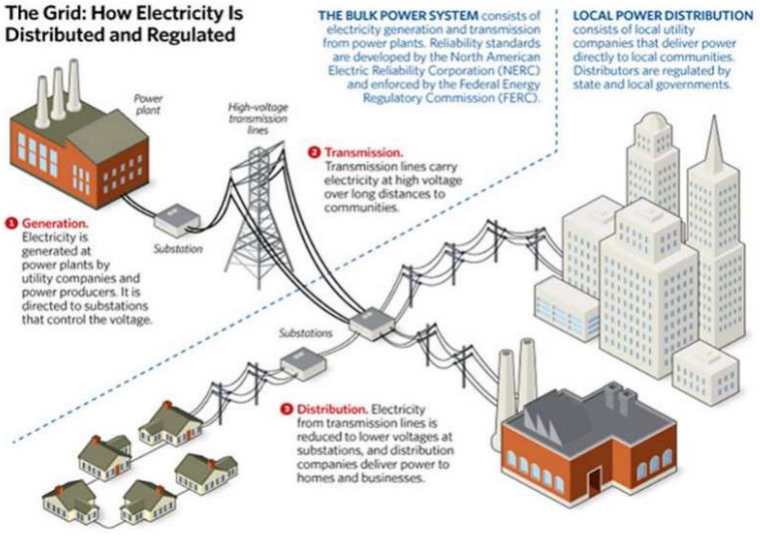


Рисунок 1.15 – Розгортання енергомережі

Технологія Blockchain в поєднанні з використанням технології Internet of Things (IoT) дозволить вести переговори про транзакції з розподіленою енергією. Використовуючи бездротові або дротяні лінії передачі даних, розподілені по сітчастої мережі, будуть

доступні корисні послуги в режимі реального часу для споживачів, наприклад інформація про надмірне споживання енергії. Споживачі зможуть автоматично реагувати на свої потреби в годуванні. Перевага, що використовує бухгалтерську книгу Blockchain, полягає в тому, щоб вирішувати постачальникам і споживачам енергетичні транзакції. З урахуванням вищевикладених припущень можна розробити можливість створення різних «Blockchain Smart Grids"» на локальній чи регіональній основі, як показано на рисунку 1.16 [28].

*Застосування Blockchain в Microgrids*

Децентралізована структура блокового ланцюжка вписується в децентралізований підхід для управління і бізнес-процесів в мікросередовищі.

1) PWR.Company. PWR.Company фокусується на торгівлі відновлюваною енергією P2P в Microgrids.

2) PowerLedger. PowerLedger надає механізм торгівлі і клірингу на ринку, заснований на блоковому ланцюжку .

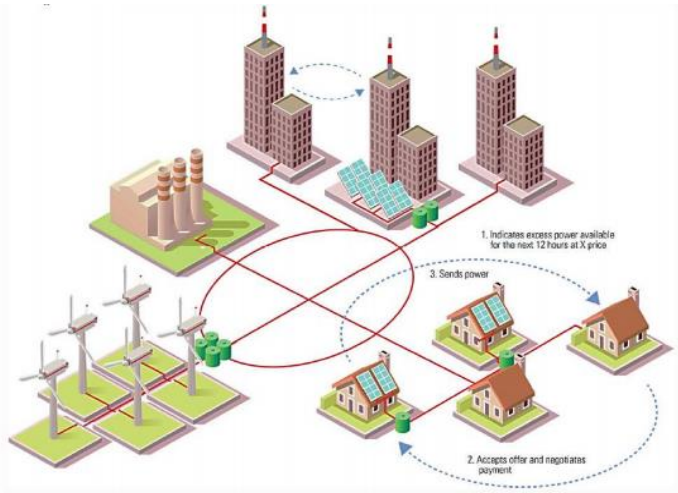


Рисунок 1.16 – Приклад Blockchain Smart Grids

3) Key2Energy. У концепції Key2Energy замість використання енергії з grid багатоквартирні будинки забезпечують самогенеруючу енергію своїм орендарям за нижчими цінами.

4) LO3 Energy - TransActive Grid і Brooklyn Microgrid. LO3 Energy розробили платформу TransActive Grid, засновану на Ethereum і смарт-контрактах. Платформа націлена на різні бізнес-моделі для розподіленого мережного і трансактивного енергетичного простору. Він дозволяє здійснювати транзакції за принципом «рівний-рівному», управляти розподіленими енергетичними ресурсами для балансування сітки, реагувати на запити, управляти аварійними ситуаціями та іншими видами використання.

5) Dajie. Dajie надає пристрої IoT і платформу на основі блоків. Для участі користувачі повинні встановити і зареєструвати один з пристроїв IoT від Dajie. Платформа

націлена на обмін енергією P2P, використання монет для оплати енергії і послуг енергетичним компаніям і погашення кредиту вуглецю монетами.

6) Share & Charge. Share & Charge - це мережа зарядних станцій електромобілів. Власники зарядних станцій можуть зареєструвати свою станцію і встановити тарифи для зарядки.

7) NRGcoin. NRGcoin використовує кріптовалютність на основі енергії в рамках об'єднання інтелектуальних контрактів. Схема інтелектуальних контрактів заснована на Ethereum.

8) GrunStromJeton - концептуальна основа, заснована на Ethereum. який служить підтвердженим доказом фактичної використовуваної суміші електрики. Замість енергії подачі враховується споживана енергія.

9) Мета SolarCoin. SolarCoin - посилити виробництво сонячної енергії.

10) TheSunExchange. TheSunExchange дозволяє «продавати натовп», де користувачі купують сонячні батареї і орендують їх, щоб заробити пасивний дохід.

11) Bankymoon. Bankymoon пропонує передплачені лічильники. Ідея полягає в тому, щоб забезпечити фінансування електроенергії, води і газу всім в світі. Лічильники можуть бути «завантажені», відправивши платежі на лічильник в різних кріптово-валютах.

12) GridSingularity. GridSingularity розробляє децентралізовану платформу обміну даними для енергетичного сектора.

13) Electron. Британська компанія Electron розробляє рішення на базі Ethereum для енергетичного сектора, які працюють разом з існуючими системами. Платформа реєстрації метрополітену є спільною платформою реєстрації для різних видів активів, таких як точки подачі газу і електроенергії, що дозволяє перемикати постачальника енергії в найближчому часі [29].

### 1.5 Постановка завдання

Для кращого розуміння ризику кібербезпеки і того, як ці ризики потенційно можуть вплинути на місію і успіх в бізнесі організації необхідна всеосяжна комунікаційна архітектура із захистом, вбудованою з самого початку. Загальні завдання забезпечення безпеки включають доступність, цілісність і конфіденційність.

Проведений аналіз надав основні відомості про покращення кібербезпеки електроенергетичних мереж за рахунок оцінки можливих ризиків і властивостей використання методів для забезпечення прогнозування, аналізу атак і захисту. В подальшому буде розроблена модель забезпечення кібербезпеки в РЗА, яка відобразить

основні вразливості даної системи і дозволить передбачити розповсюджені кроки атак.

Дана модель призначена для гідроелектростанції та побудована на основі електричного і кіберграфа. Буде проведено аналіз методів прогнозування ймовірного моделювання архітектури та імовірна оцінка і прогнозування властивостей системи.

Основними кроками дослідження технології інтелектуальних мереж для вдосконалення кібербезпеки РЗА виявилися:

– аналіз моделей, методів і стандартів забезпечення кібербезпеки на етапі проектування і експлуатації в Smart Grid;

– аналіз вимог, особливостей і заходів до Smart Grid як об’єкта оцінки забезпечення кібербезпеки;

– розробка моделі на основі лінійної схеми ГЕС та електричного і кіберграфа;

– моделювання та розрахунок ймовірних кроків атак на компоненти системи та прийняття додаткових мір.

### 1.6 Висновки до розділу 1

Для досягнення і збереження властивостей безпеки у ресурсів, спрямованих проти загроз безпеці в кібер-середовищі проводиться оцінка та дослідження методів забезпечення кібербезпеки.

При проведеному аналізі було розглянуто методи оптимізації інтелектуальних мереж, варіанти архітектур і їх відмов під час експлуатації, типи атак, проблеми, що виникають при розробці нових рішень безпеки, а також поточні та можливі рішення.

Результати проведеного аналізу моделей, методів, алгоритмів, функціональних характеристик, видів атак, стандартів в Smart Grid показали, що Smart Grid повинна мати такі характеристики:

– Адаптивність.

– Інтелектуальний підхід з точки зору застосування оперативних даних до практики обслуговування обладнання і виявлення можливих відключень до їх виникнення;

– Інтегрованість з точки зору функцій зв'язку і контролю в реальному часі;

– Гнучкість;

– Економічність.

Ключовими елементів бачення Smart Grid є:

– Створення інструментарію перевірених технічних рішень, які можна швидко і економічно розгортати, дозволяючи існуючим мережам приймати енергетичні ін'єкції з усіх енергетичних ресурсів.

– Узгодження нормативно-правових та комерційних рамок для полегшення транскордонної торгівлі як енергетичними, так і мережевими послугами, гарантуючи, що вони будуть охоплювати широкий спектр операційних ситуацій.

– Створення загальних технічних стандартів і протоколів, які забезпечать вільний доступ, дозволяючи розгортати обладнання у будь-якого обраного виробника.

– Розробка інформаційних, обчислювальних і телекомунікаційних систем, які дозволяють підприємствам використовувати інноваційні механізми обслуговування для підвищення їх ефективності та розширення своїх послуг для клієнтів.

– Забезпечення успішної взаємодії нових і старих конструкцій мережевого обладнання для забезпечення сумісності механізмів автоматизації і управління.

### 1.7 Перелік посилань до розділу 1

1. Kimmo Kauhaniemi and Sampo Voima «Functional requirements of Smart Grid protection», 2012;

2. Toby Considine, William Cox, Edward G. Cazalet «Understanding Microgrids as the Essential Architecture of Smart Energy», 2012;

3. Jin-Man Sohn, Sang-Yun Yun «Software Functional Requirements and Architectures of Microgrid Energy Management System», 2016;

4. Andreadou N., Olariaga Guardiola M., Papaioannou I., Prettico G. « Smart Grid Laboratories Inventory 2016 », 2016;

5. Yasin Kabalci «A survey on smart metering and smart grid communication», 2016;

6. Zoran Bojkovic, Bojan Bakmaz «Smart Grid Communications Architecture: A Survey and Challenges», 2012;

7. Hachem Karzazi «Designing a Smart MicroGrid», 2017;

8. Michael Emmanuel Winston K.G. Seah Ramesh Rayudu «Communication Architecture for Smart Grid Applications», 2018;

9. Eun-Kyu Lee, Wenbo Shi, Rajit Gadh, Wooseong Kim «Design and Implementation of a Microgrid Energy Management System», 2016;

10. Yee Wei Law, Hemanshu R. Pota, Jiong Jin, Zhihong Man, Marimuthu Palaniswami « Control and Communication Techniques for the Smart Grid: An Energy Efficiency Perspective », 2016;

11. D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos and K.L. Butler-Purry «Towards modelling the impact of cyber-attacks on a smart grid», 2011;

12. Ward Bower «The Advanced Microgrid Integration and Interoperability», 2014;

13. Xu Li, Inria Lille « Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges», 2012;

14. Xingsi Zhong, Lu Yu, Richard Brooks, Ganesh Kumar Venayagamoorthy «Cyber Security in Smart DC Microgrid Operations», 2015;

15. Adnan Anwar, Abdun Naser Mahmood «Cyber Security of Smart Grid Infrastructure», 2014;

16. Alejandro Pinto «Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids», 2012;

17. Qiang Fu, Adel Nasiri, Ashishkumar Solanki, Abedalsalam Bani-Ahmed, Luke Weber, Vijay Bhavaraju1 «Microgrids: Architectures, Controls, Protection, and Demonstration», 2015;

18. Benjamin Kroposki, Thomas Basso, Richard DeBlasio «Microgrid Standards and Technologies», 2008;

19. Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P., Iyer, R. «Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids» 2018;

20. Roman Schlegel, Sebastian Obermeier, Johannes Schneider «Assessing the Security of IEC 62351», 2008;

21. National Association of State Energy Officials «Smart Grid and Cyber Security for Energy Assurance», 2011;

22. Meenakshi Chahar, Deepali Puri «A review on physical protection of smart grid», 2016;

23. Alexander D. Schlichting «Assessment of Operational Energy System Cybersecurity Vulnerabilities», 2018;

24. Isaac Ghansah «Smart Grid information assurance and security technology assessment», 2010;

25. Franklin E. Pacheco, J. Chris Foreman «Microgrid Reference Methodology for Understanding Utility and Customer Interactions in Microgrid Projects», 2016;

26. Ferran Torrent Fontbona «Optimisation methods meet the smart grid», 2015;

27. Muhammad Fahad Zia, Elhoussin Elbouchikhi, Mohamed Benbouzida, «Microgrids energy management systems: a critical review on methods, solutions, and prospects», 2018;

28. Alessandra Pieroni, Noemi Scarpato, Luca Di Nunzio, Francesca Fallucchi, Mario Raso «Smarter City: Smart Energy Grid based on Blockchain Technology», 2018;

29. Andrija Goranovic, Marcus Meisel, Lampros Fotiadis, Stefan Wilke, Albert Treytl, Thilo Saute «Blockchain Applications In Microgrids», 2017;

# РОЗДІЛ 2 МОДЕЛІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ

## 2.1 Види вразливостей систем релейного захисту та автоматики, що використовуються в Smart Grid

*Вразливості і фактори ризику в Smart Grid*

Вразливості / недоліки кібербезпеки - це умови, що існують в будь-якому кібер-активі або організаційному процесі на різних рівнях, включаючи його проектування, впровадження, настройку, експлуатацію або управління. Вразливості можуть бути різних типів. У цьому розділі представлений список компонентів ІКТ для смарт-мереж, які необхідно розглядати як джерело вразливостей. Ця категоризація компонентів інфраструктури комунальних підприємств на верхньому рівні, які можуть мати кібер-уразливості [1]:

– Операційні системи: генератори, трансформатори, системи диспетчерського контролю та збору даних (SCADA), системи управління енергоспоживанням / розподілом (EMS / DMS), програмовані логічні контролери (ПЛК), підстанції, інтелектуальні лічильники та інші інтелектуальні електричні пристрої (СВУ).

– Класичні IT-системи: ПК, сервери, мейнфрейми, додатки, бази даних, веб-сайти, веб-сервіси і т. д.

– Мережі та протоколи зв'язку: Ethernet, Wi-Fi, PRIME, DLMS / COSEM, Zigbee, 4G, DNP3 і т. д.

– Кінцеві точки: смарт-лічильники, EV, смартфони та інші мобільні пристрої. Беручи до уваги як фізичні, так і логічні аспекти.

Згідно [2], існує 4 основні класи вразливостей, які створюють значні ризики і відкривають двері для різних кібератак:

Клас 1: Люди, політика і процедура. Відсутність необхідної підготовки та недотримання політики та процедур призводять систему до різних ризиків і проблем безпеки. В результаті зацікавлені сторони повинні мати певний рівень доступу до системи, в залежності від їх технічних обов'язків.

Клас 2: Уразливості програмного забезпечення та програмно-апаратних засобів. Програмне забезпечення та прошивка в системі несуть відповідальність за захист системи від несанкціонованого доступу людьми, які намагаються втручатися в систему і втручатися в бази даних і іншу інформацію.

Клас 3: Уразливості платформи. Програмне забезпечення, операційна система і апаратне забезпечення мають загальну проблему безпеки в мережі інтелектуальної мережі через складність архітектури та конфігурації.

Клас 4: Мережа. Мережа - це спосіб зв'язку між різними пристроями, що використовує стандартний протокол зв'язку для відправки та отримання даних. Мережа повинна володіти вимогами безпеки, призначеними для забезпечення цілісності, конфіденційності, доступності, шифрування протоколу і аутентифікації.

### 2.2 Визначення загроз безпеки Smart Grid

Відкритість SG робить їх дуже вразливим для основних атак системної безпеки. При використанні ІКТ в SG потужність електроживлення може контролюватися віддалено через Інтернет. Функціонування промислової і критичної інфраструктури в SG контролюється з використанням системи SCADA. З цих причин важливо проаналізувати загрози безпеки і ризики в системах SCADA для розробки належного вирішення безпеки.

Як приклад, представлений аналіз основних загроз безпеки системи, для розробки інтегрованої моделі загроз безпеки системи (МЗБС) SG.

На рис. 2.1 МЗБС та загрози, що відносяться до конкретного елементу (системі або з'єднанню) в архітектурі SG. Щоб вказати загрози в тексті, використані кутові дужки, наприклад, <TNo:>.

В SG дані можуть бути скомпрометовані, поки вони записані, збережені або передані в системі. Атакуючі можуть вводити підроблені значення між Smart Meter (SM) і вузлами колектора для зміни трафіку даних, <T27>.

Це може статися, якщо зловмисники можуть отримати криптографічні ключі, які використовуються для шифрування збережених даних. Атакуючі можуть проникати в мережу і вводити підроблені значення в лінію зв'язку, виконуючи керуючі команди в будь-якому внутрішньому вузлі колектора <T19, T23>. Це може вплинути на передану запис потреби і замінити її підробленими значеннями, коли вона проходить через вразливий вузол колектора. З огляду на те, що типовий SG має понад тисячу вузлів колектора, можуть бути порушені інші вузли колектора, і ефект цієї загрози може бути посилений.

Зловмисники можуть перехоплювати передачу даних в бездротовій мережі зі зворотним ходом (GPRS), потрібну для з'єднання вузлів колектора з центром управління, використовуючи атаку «людина в середині», <T21, T25, T26>. Він включає компрометацію каналів зв'язку, шлюзів і маршрутизаторів даних.

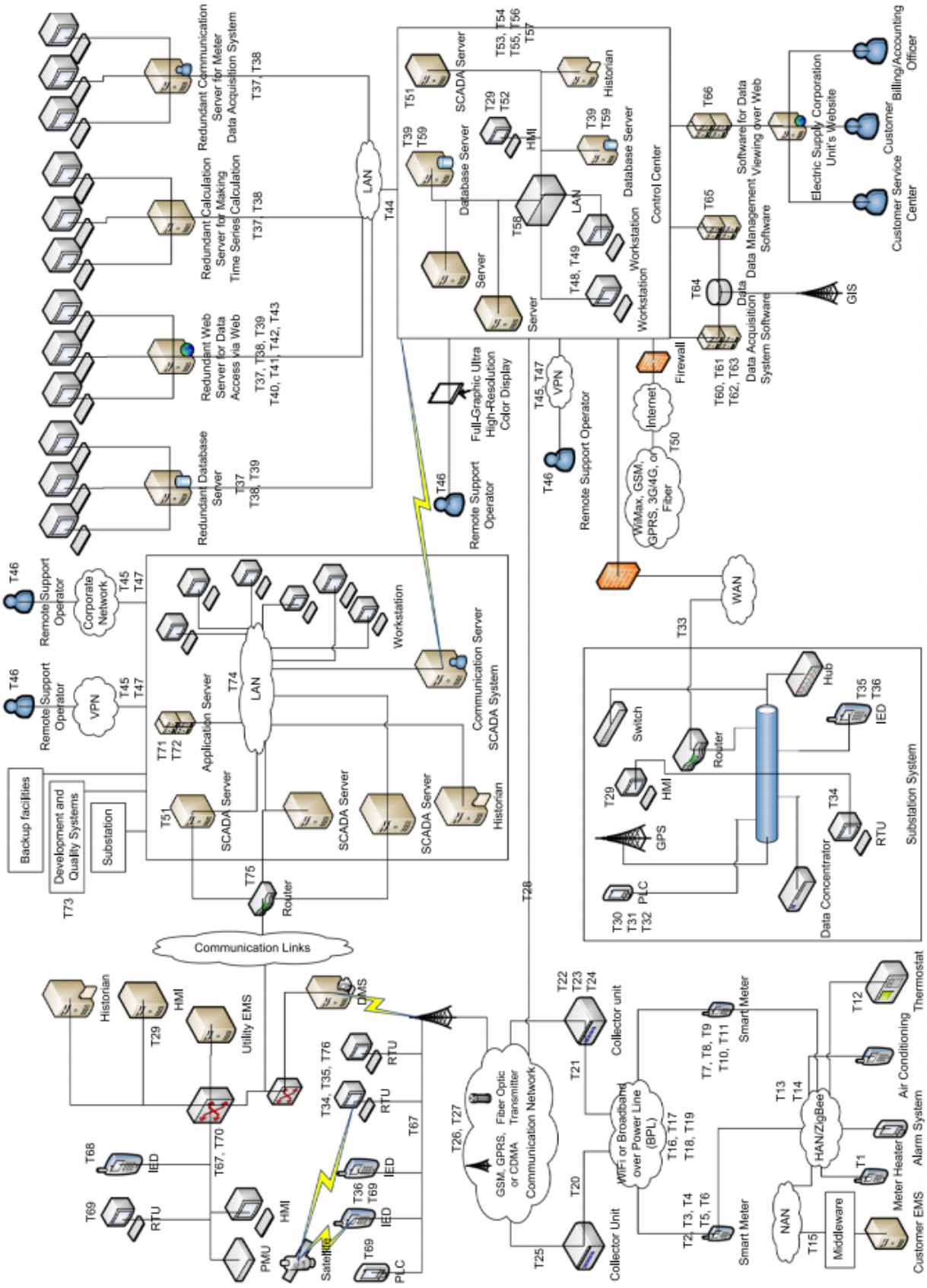


Рисунок 2.1 МЗБС SG для запобігання можливим загрозам (Джерело: [3])

Атакуючі можуть також читати і змінювати передані дані через скомпрометоване обладнання, <T20, T23>. Атакуючі можуть читати незашифровану інформацію і отримувати паролі, щоб скомпрометувати систему, заборонивши доступ законних користувачів до системи, <T8, T10, T11>. Наприклад, зловмисники можуть перехоплювати важливі дані, такі як повідомлення про відключення, відправлені в систему управління відходами в разі виявлення збоїв.

Атакуючі можуть перехоплювати звіти про споживання енергії, сигнали ціноутворення, термінові повідомлення, дані SM, звіти про відключення і повідомлення про помилки, відправлені з SM на утиліту, <T13, T14>. Атакуючі можуть також перехоплювати команди управління, відправлені з утиліти в SM, які включають в себе запити на зниження загального споживання енергії в домашньому домені.

Крім введення в оману даних, переданих на / з розподілених інтелектуальних пристроїв і SMs <T19>, зловмисники можуть наповнити їх небажаним трафіком даних. Атака на відмову в обслуговуванні (DoS), <T18, T69>. Дані передаються через Інтернет, GPRS-мережа або PLComm, які мають небезпечні канали для передачі даних, і дані плануються для зберігання в базі даних віддаленого доступу до даних про фактичне споживання енергії. Атака DoS в цьому випадку може затримувати і вводити в оману дані, якими обмінюються цими пристроями і іншими компонентами в SG <T16, T17>. DoS може знизити загальну продуктивність цих пристроїв, оскільки вони можуть не реагувати на зміни в системі. Атака DoS може вплинути на нормальне використання або управління SG. Це може вплинути на додатки SM, використовувані для вимірювання енергоспоживання доступних енергоресурсів. Він може перевантажувати або навіть перешкоджати доступу до SM, який не може тому виконувати свої функції. Отримані дані в центрі управління можуть бути неправильними і можуть не відповідати статусу SG. Це може вплинути на процес прийняття рішень в Центрі управління.

Атакуючі можуть завдати шкоди центру управління та його лініям зв'язку, наводячи їх небажаним трафіком даних, <T51, T56, T58, T59>. Ця загроза може вплинути на ресурси централізованого управління, системні служби і файлову систему, одним з можливих наслідків такої загрози є видалення IP-адресів SM, що зберігаються в центрі управління, Атакуючі можуть відправляти велику кількість пакетів для вичерпання доступних ресурсів. Лінії зв'язку можуть бути перевантажені і можуть викликати затримки зв'язку через обмежену пропускну здатність зв'язку. Це може сповільнити роботу центру управління і знизити його загальну продуктивність. Крім того, ця атака може побічно порушувати роботу серверів зв'язку, систем управління резервним копіюванням і розподілених серверів реляційних баз даних. Ця атака також може порушити послуги реального часу, що

надаються центром управління. Видалення файлової системи може призвести до відключення онлайн-системи моніторингу та центру управління. Як правило, атака центру управління SG вважається найнебезпечнішою атакою і може привести до катастрофи. Він може відключити весь SG, який централізовано контролюється центром управління. Величезні втрати важливої інформації, економічних втрат і збитків для обладнання також можливі в разі порушення безпеки центру управління.

Точка доступу проміжного програмного забезпечення, пов'язана з системою доставки EMS і сусіднєю мережею клієнта, може бути скомпрометована, <T15>. Ця загроза може бути використана зловмисниками, оскільки проміжне програмне забезпечення використовується в SG для встановлення зв'язку між клієнтом і утилітою за допомогою сервіс-орієнтованої архітектури. При використанні слабких механізмів аутентифікації можливі захоплення і модифікація інформації на сервері проміжного програмного забезпечення.

*Модель загрози безпеки систем SG*

В даному прикладі представлені посилання МЗБС SG і розширений аналіз загроз і вразливостей системної безпеки в МЗБС SG. МЗБС SG фіксує основні загрози безпеки системи. Можливість використовувати МЗБС SG для ефективного взаємозв'язку і розуміння вразливостей, потенційно використовуваних зловмисниками для компрометації даних, що зберігаються і передаються по дротових і бездротових каналах зв'язку в SG, може допомогти реалізувати відповідні рішення і засоби захисту систем безпеки. Інтегрований SG МЗБС показаний на рис.2.1. В табл. 2.1 показані основні загрози безпеки системи в SG. SM і інтелектуальні пристрої відправляють дані по каналах зв'язку в центр управління. SM є критичним компонентом в AMI SG. Пароль SM може бути скомпрометований шляхом виявлення переданих даних з оптичного комунікаційного порту SM або компрометації інтерфейсу входу адміністратора, <T4>. Атакуючі можуть змінити суму виписки про виставлення рахунку, щоб показати менше фактичного споживання енергії, щоб зменшити суму платежу. Це виконується шляхом виконання операції скидання запиту для скидання білінгової системи для перерахунку з нуля. Він побудований з часткових систем МЗБС.

Зловмисники можуть використовувати пристрій смарт-зчитувача з програмним забезпеченням для моніторингу для передачі даних, що передаються через оптичний порт зв'язку SM. Сигнали в цьому випадку можуть бути виявлені і записані для захоплення пароля.

Таблиця 2.1 – Умовні позначення та визначення загроз безпеки системи

| № | Опис загрози |
|---|---|
| T1 | Відправка фальшивих «включених» сигналів в групу електричних пристроїв для порушення попиту на навантаження |
| T2 | Обмежена і збережена обчислювальна потужність процесора, і обсяг пам'яті SM |
| T3 | DoS переповнення буфера для видалення вмісту SM |
| T4 | Захоплення пароля за допомогою програми моніторингу з пристроєм зчитування на оптичному комунікаційному порту |
| T5 | Порушення прошивки SM |
| T6 | Порушення збережених даних SM |
| T7 | Реконфігурація атаки шляхом установки нестабільної прошивки на SM |
| T8 | Відправка команд підключення / відключення до розподілених польових пристроїв |
| T9 | Spoofing / втілює SM під атакою |
| T10 | Обнюхування SM, незашифрованих пакетів |
| T11 | Використання слабких механізмів аутентифікації |
| T12 | Атака на пропрієтарну систему польових пристроїв, які призначені для певних функцій, таких як обслуговування, моніторинг і т. д. |
| T13 | Зміна даних, переданих від SM |
| T14 | Небезпечні проблеми бездротового з'єднання в межах HAN |
| T15 | Небезпечний клієнт для доступу до проміжного програмного забезпечення, що призводить до вразливого зв'язку між системою EMS і NAN клієнта |
| T16 | Спотворення даних датчика |
| T17 | Втрата даних датчика |
| T18 | Зупинка потоку даних або DoS-атаки на розподілені інтелектуальні пристрої |
| T19 | Впровадження підроблених значень для зміни переданих записів вимог між розподіленими інтелектуальними пристроями і SM |
| T20 | Аналіз несанкціонованого трафіку |
| T21 | Пакет Підслуховування між одиницями колектора і різними мережами WiFi / BPL |
| T22 | Зміна параметрів часу роботи польових пристроїв |
| T23 | Відправка неправильних команд або шкідливих параметрів через лінії зв'язку, шлюзи або маршрутизатори, що з'єднують вузли колектора з центром управління |
| T24 | Зміна налаштувань польових пристроїв |
| T25 | Протокол атаки на лінії зв'язку між збирачами і бездротовими мережами GSM / GPRS |
| T26 | Перехоплення обмінних даних між польовими пристроями і центром управління, атака «людина-в-середині» |
| T27 | Впровадження підроблених значень для зміни трафіку даних |
| T28 | Вводячи в оману дані, передані оператору центру управління |
| T29 | Підміна системи HMI для подання іншого інтерфейсу системному оператору |
| T30 | Перехоплення повідомлених даних з СВУ в центр управління |
| T31 | Рятувальна операція наглядового контролю на основі неточних даних поля, отриманих за допомогою неточних польових приладів |
| T32 | Неправильні команди управління для досягнення умови перевантаження для пошкодження різних польових пристроїв |
| T33 | Зовнішні загрози безпеки через WAN на маршрутизаторі та інших пристроях в системі підстанції |
| T34 | Відправка помилкових даних в польовий пристрій |
| T35 | Атака на пропрієтарну систему польових пристроїв, які призначені для конкретних функцій, наприклад, перетворювача, PMU, повторного включення схеми, лічильника, перемикача відгалужень і захисного реле |

Продовження таблиці 2.1

| | |
|---|---|
| T36 | Вимкнення IEУ та інших кінцевих пристроїв |
| T37 | Повінь надлишкових баз даних, Інтернету, обчислень і комунікаційних серверів з небажаним трафіком |
| T38 | DoS-атака на резервні бази даних, мережі, обчислення та комунікаційні сервери |
| T39 | Атака шкідливого коду на надлишкову базу даних і веб-сервери |
| T40 | Доступ до контролерів віддалено через веб-служби та модеми віддаленого доступу |
| T41 | Захоплення сеансу на надмірному веб-сервері (для доступу до даних через Інтернет) |
| T42 | Міжсайтовий скриптинг на резервному веб-сервері |
| T43 | Омана атаки на надмірному веб-сервері, де зловмисник робить вигляд, що він / вона є власником сесії |
| T44 | Команда управління уприскуванням |
| T45 | Використання поганої конфігурації VPN та інших корпоративних мереж |
| T46 | Компрометація клієнтської системи шляхом використання поганих клієнтських конфігурацій; для отримання несанкціонованого віддаленого доступу до системи SCADA |
| T47 | Вводячи в оману дані, передані в центр управління через VPN і корпоративні мережі |
| T48 | Отримання несанкціонованого доступу до робочих станцій, що дозволяє контролювати процеси розробки, що виконуються через ці робочі станції |
| T49 | Підміна робочих станцій |
| T50 | Зміна навантаження через Інтернет |
| T51 | Повінь головного і підлеглого SCADA для затримки передачі даних |
| T52 | Отримання несанкціонованого доступу до системи HMI |
| T53 | Зміна параметрів часу роботи розподілених польових пристроїв |
| T54 | Відправка неправильних команд або шкідливих параметрів в розподілені польові пристрої |
| T55 | Зміна налаштувань польових пристроїв |
| T56 | Повінь центру управління та його підключених серверів і програмних систем з небажаним трафіком (DoS) |
| T57 | Відправка вводить в оману даних оператору центру управління |
| T58 | Введення даних або команд в мережі SG, наприклад, в мережу центру управління |
| T59 | Маніпулювання джерелами даних, такими як сервери реляційних баз даних і файлова система |
| T60 | Перехоплення або зміна отриманих даних з підстанції SM-модемів в програмному забезпеченні системи збору даних |
| T61 | Запуск модуля управління аварійними сигналами для порушення роботи |
| T62 | Атака на серверні програмні системи центру управління для включення / виключення живлення будь-якого клієнта шляхом включення / вимикання або відтворення за допомогою лічильників клієнтів і стану їх харчування |
| T63 | Атака на модуль управління користувачами і, отже, гра з визначенням, ролями і правами користувача; для включення / вимикання або обмеження чутливих технічних змін (ліній зв'язку та обробки даних SM) |
| T64 | Перехоплення / зміна вихідних даних для обробки, обчислень і візуалізації |
| T65 | Перехоплення / зміна даних, зібраних з SM, таких як коефіцієнти потужності, струми, напруги і т. д. в програмному забезпеченні для керування даними |
| T66 | Виконання веб-атаки на веб-інтерфейси зовнішніх користувачів для доступу до даних SM |
| T67 | Пакети перехоплюють канали зв'язку, які з'єднують HMI, RTU, IED і PMU разом |

Продовження таблиці 2.1

| | |
|---|---|
| T68 | Вводячи в оману дані, що передаються на польові пристрої, такі як звіти про споживання енергії, сигнали ціноутворення, повідомлення про термінові повідомлення і збої |
| T69 | DoS-атака шляхом повені польових пристроїв небажаним трафіком даних |
| T70 | Застрявання каналів зв'язку, підключених до польових пристроїв за допомогою HMI, шляхом відправки сигналів з тією ж частотою сигналів корисності |
| T71 | Запуск сервера додатків для видачі команд FEP |
| T72 | Атака сервера додатків для управління різними додатками, використовуваними для управління частинами системи SCADA |
| T73 | Віддалений зв'язок на об'єктах резервного копіювання та підстанціях, пов'язаних з системою SCADA |
| T74 | Зміна даних, якими обмінюються сервери додатків, HMI і т. д. |
| T75 | Компрометація або злом маршрутизатора для вставки помилок в певні оцінки змінних стану |
| T76 | Повінь RTU з дійсними повідомленнями протоколу для насичення процесора, пам'яті або смуги пропускання |

Збережена фальсифікація даних - ще одна загроза, яка впливає на SM, тому що поведінка SM контролюється збереженими даними, <T6>. Якщо зловмисники можуть отримати контроль над даними резервування SM, це може вплинути на роботу SM. Атакуючі можуть порушувати тарифи на час використання, журнали фізичних подій і виконані команди, і записані мережеві команди. Атакуючі можуть збільшити або зменшити фактичний рівень споживання, щоб вплинути на фактичну ціну виставлення рахунку.

При порушенні (перезапису) мікропрограм SM може надати зловмисникам контроль над SM і іншими відповідними інтелектуальними пристроями за допомогою несанкціонованої прошивки. Вбудована прошивка може вплинути на пристрої або клієнтів, які використовують його, для виконання деяких важливих дій, таких як продаж енергії. Вбудована прошивка спрощує крадіжку і відключення живлення SM, <T5>.

Програмне забезпечення спуфінга може використовуватися зловмисниками для уособлення SM (при Інжекційному трафіку), <T9>. Програмне забезпечення спуфінга поширюється зловмисниками для обробки і відповіді на запити SM і утиліти, які не залишають ніяких доказів несанкціонованого доступу. Атакуючі в цьому випадку уособлюють дійсних користувачів. Важливі записи і звіти SM можуть бути захоплені зловмисниками. Цими записами можуть бути записи SM, які підсумовують використання мережі, або інформацію про виставлення рахунків і ціноутворення.

Атакуючі можуть вводити в оману дані, передані в пристрої з розподіленим полем, такі як інтелектуальні кінцеві пристрої (IED), <T30>, віддалені термінальні блоки, блоки вимірювання фаз (PMU), програмовані логічні контролери і т.д., <T12, T34, T35>. Ці пристрої можуть піддаватися атакам зовнішньої системи безпеки через глобальну мережу

(WAN) на маршрутизаторі та інших пристроях в системі підстанції <T33>. Ці пристрої призначені для того, щоб дозволити менеджерам віддалено звертатися до своїх призначених для користувача інтерфейсів для цілей діагностики, обслуговування, моніторингу, вимірювання та налаштування. Атакуючі можуть виконувати команди і операції диспетчерського управління на основі неточних польових пристроїв, <T31>, щоб центр управління отримував неправильні дані. Якщо ці пристрої скомпрометовані, зловмисники можуть: змінити параметри часу виконання, <T22, T53>; змінити налаштування пристрою, <T24, T55>; відправляти неправильні команди управління іншим польовим пристроям, <T23, T54>; вводити в оману дані, передані оператору центру управління, <T28>.

Атакуючі можуть також змінювати дані та інформацію про час та статус, відправлені з польових пристроїв в центр управління, наприклад команди управління підключенням / відключенням і настройки, звіти про споживання енергії, сигнали ціноутворення, повідомлення про несправності і т. д., <T68>. Наприклад, зловмисники можуть ввести в оману команди управління підключенням / відключенням, щоб викликати надмірне вироблення електроенергії з енергоресурсів, що може призвести до фінансових втрат, <T8, T32>. Неточні команди управління від зловмисників можуть порушити роботу польових пристроїв, викликати пошкодження обладнання, відключити польові пристрої, <T36> і викликати втрату обслуговування.

Ще одна загроза - повінь польових пристроїв, розподілених по всій SG, таких як SM, IED, RTU і ПЛК, <T3, T69, T76>. Атакуючі іноді неодноразово наповнюють ці пристрої дійсними повідомленнями протоколу, щоб вплинути на його загальну продуктивність. Мета полягає в тому, щоб споживати смугу пропускання каналів, щоб заперечувати вхідні та вихідні дані. Це може привести до насичення обчислювальної потужності центрального процесора (CPU) і вплине на обмежений простір пам'яті. Це може збільшити енергоспоживання вузла, що може знизити його загальну продуктивність.

Доступні ресурси SM і польових пристроїв обмежені. Обмежений простір пам'яті SM може ледь містити прошивку. Обмежений простір пам'яті може завадити відновленню прошивки, що неминуче через збільшення кількості виявлених вразливостей і помилок програмного забезпечення. Неможливість останнього оновлення прошивки SM може виставити SM для більшого проникнення. Атакуючі можуть скомпрометувати процес оновлення прошивки і замінити його на новий, сумісний з дизайном і призначенням зловмисників, <T7>. Обмежений простір пам'яті може навіть перешкодити архітекторам завантажувати свої криптографічні матеріали для своїх криптографічних функцій.

Дизайнери можуть розвантажити свої криптографічні ключі в окрему згадку, до якої також можна отримати доступ і зламати.

Крім того, обчислювальна потужність SM обмежена, <T2>. Якщо передані дані приймаються, коли простір пам'яті заповнений і центральний процесор зайнятий, це призведе до дуже частої відмови в обслуговуванні і обміну даними.

Деякі критичні місця розташування в SG можуть бути скомпрометовані через Інтернет. Атакуючі можуть змінювати навантаження <T50>, щоб викликати переповнення або несправність схеми, щоб погіршити або пошкодити обладнання для передачі енергії. Сервери центрів обробки даних в SG є придатними об'єктами для виконання такого роду атак. Атакуючі можуть скомпрометувати або розбити маршрутизатор, який передає дані в систему SCADA, <T75>. Атакуючі можуть вводити помилкові дані проти певних оцінок змінних стану. Крім того, зловмисники можуть відправляти підроблені сигнали включення в групу електричних пристроїв, щоб порушити попит на навантаження. Частини навантаження в SG, такі як кондиціювання повітря, нагрівання води та охолодження, знаходяться під прямим контролем утиліти. Атакуючі можуть відправляти сигнали команд управління (зокрема тони включення, <T1, T62>) через Інтернет, щоб погіршити якість харчування, викликати проблеми з напругою і викликати потенційні пошкодження обладнання для клієнтів.

Сигнал ціни може бути скомпрометований шляхом введення помилкових значень. Сигнали ціни отримують через Інтернет по утилітам, що дозволяє клієнтам самостійно контролювати свою навантаження. Атакуючі можуть використовувати цю функцію для подачі помилкових сигналів ціни через Інтернет. В результаті зниження цін, вимоги до навантаження можуть бути збільшені замовниками. Збільшення навантаження замовників може вплинути на автоматизоване планування споживання енергії, змінити загальне споживання енергії сотнями резиденцій і змінити профіль навантаження клієнтів. Основна проблема полягає в тому, що ціновий сигнал - це многоліковий сигнал, що відправляється багатьом клієнтам разом, і будь-яка фальсифікація ціни може збільшити ефект.

Атака перешкод може бути виконана шляхом відправки бездротових сигналів з шкідливого вузла з тією ж частотою сигналів корисності, <T70>. Крім того, загроза перехоплення пакетів, <T67>, може бути виконана в разі, якщо шкідливий вузол правильно обійшов процедуру аутентифікації і вважається довіреною з законним доступом до мережі. Підслуховування пакетів виконується пасивним способом без необхідності проведення активної атаки безпеки.

Система HMI використовується операторами SG для віддаленого моніторингу та управління віддаленими пристроями. Якщо зловмисники можуть отримати

неавторизований доступ і управління системою HMI, <T29, T52>, іноді використовуючи стандартні методи, може відображатися багато інформації, що відноситься до операцій системи SCADA. Потім атакуючі можуть виконувати довільні команди, необхідні для управління і контролю роботи інтелектуальних пристроїв, підключених до системи HMI.

Центр управління підключається через локальну мережу (LAN) до інших резервних серверів. Він включає внутрішні робочі станції і системи HMI. Підміна робочих станцій, <T49>, а системи HMI - це потенційна загроза, яка використовується для того, щоб вплинути на рішення операторів центру управління, проаналізувавши протокол зв'язку, який використовується для обміну даними. Атакуючі можуть дістати несанкціонований доступ до робочих станцій для контролю процесів розробки, що виконуються за допомогою цих робочих станцій, <T48>. Атакуючі можуть також видавати себе за систему HMI, щоб представити інший інтерфейс HMI оператору центру управління, <T29>. Відповідно, оператор приймає неправильні дії і виконує неправильні команди управління в системі SCADA на основі невірної інформації, представленої підробленою системою HMI, <T46, T57>. Дані, представлені в системі HMI, включають дані, дані з RTU і ПЛК. Він включає в себе звіти про стан обладнання та дані зчитування лічильників, зібрані з приводів і датчиків, які повинні зберігатися на сервері істориків. Це мережева атака, яка приймає форму атаки «людина-в-середині».

Віддалений доступ до контролерів через веб-служби та модемні модеми також доступний, і рідко потрібно аутентифікація. Якщо зловмисники успішно атакують контролери, зловмисники можуть видавати команди управління і можуть збирати логіку програмування та інформацію прошивки, <T40>.

Загроза захоплення сеансу може виникнути, коли зовнішній користувач звертається до онлайн-інформації за допомогою веб-порталів через резервний веб-сервер для доступу до даних через Інтернет, <T41>. Атакуючі можуть вкрасти ідентифікатор сеансу користувача (ID). Атакуючі можуть також видавати себе за сеанс, прикидаючись власником сеансу. Незашифрований ідентифікатор сеансу може викликати витік конфіденційної інформації про сеанс зловмисникам. Загроза міжсайтового скриптинга включає атакуючий центр управління з веб-додатків, що використовуються в SG, <T42>. Атакуючі можуть використовувати клієнтський веб-портал, який використовується для віддаленого доступу до даних, пов'язаних з енергоспоживанням, і до онлайн-інформаційним системам.

Інші загрози можуть вплинути на центр управління та пов'язані з ним сервери та програмні системи. Повінь серверів з небажаним трафіком даних можливо, <T56>. Ця загроза може вплинути на надлишковий сервер бази даних, надлишковий веб-сервер для доступу до даних через мережу, надлишковий сервер розрахунків для розрахунку часових

рядів і надлишковий сервер зв'язку для системи збору даних лічильника [21], <T37, T38>. Наприклад, атака шкідливого коду (шкідлива програма), <T39>, атака міжсайтового скриптинга, <T42>, атака захоплення сеансу, <T41> і підробка атаки, <T43> є можливими загрозами на надмірному веб-сервері. Ці сервери пов'язані з центром управління через ЛВС, що також вразливе, і дані, передані через нього, можуть бути перехоплені і змінені.

Серверні програмні системи центру управління також уразливі. Програмне забезпечення системи збору даних відповідає за опитування даних SM. Атакуючі можуть перехоплювати або змінювати дані, передані з підстанції SM-модемів, які збираються і зберігаються в програмній системі управління збором даних, <T60>. Модуль аварійного управління, який використовується для запуску аварійних сигналів в разі збою живлення і SM-втручання, також може бути скомпрометований, <T61>. Це може порушити стабільну роботу системи. Крім того, зловмисники можуть вмикати / вимикати харчування будь-якого клієнта, включивши / вимкнувши SM або змінивши статус включення SMs, <T62>. Крім того, модуль для користувача адміністрування може бути скомпрометований шляхом зміни визначень, правил і прав користувачів. Атакуючі в цьому випадку прагнуть включити або обмежити конфіденційні технічні конфігурації, такі як лінії зв'язку і обробка даних SM, <T63>.

Крім того, необроблені дані, передані з системи програмного забезпечення для збору даних в систему управління даними, уразливі для атаки, <T64>. Це передається для обробки, обчислень і візуалізації. Дані, зібрані програмним забезпеченням управління даними з SM, також можуть бути скомпрометовані, <T65>. Це включає в себе коефіцієнт потужності, активні / реактивні вимоги, напруги і струми, лінійні напруги і струми. Програмне забезпечення для управління даними отримує дані не тільки від SM і системи збору даних, але і від серверів зв'язку. У разі правильної компрометації системи управління даними зловмисники можуть змінювати виміряні дані, графіки, діаграми, таблиці, тарифи і т.д. Програмне забезпечення для управління даними іноді пов'язано з Географічною інформаційною системою (ГІС) для отримання фонових карт. Це виконується з використанням загальнодоступних протоколів, які також можуть бути використані. Інша загроза з'являється на інтерфейсі для перегляду даних через Інтернет, яка доступна для зовнішніх користувачів для доступа до даних лічильника, <T66>.

Система SCADA використовується для віддаленого доступу до вироблення електроенергії для управління потоком потужності. Вона також використовується для збору даних від розподілених інтелектуальних датчиків і пристроїв. Зібрані дані передаються і зберігаються в центрі управління для цілей контролю. Повінь головного і підлеглого серверів SCADA з небажаним трафіком даних є ще одним видом загроз, який

зазвичай може привести до відключення електроенергії в електричній інфраструктурі, <T51>. Це може привести до погіршення загальної продуктивності цих серверів і системи SCADA в цілому. Ця атака може вплинути на доступність і цілісність даних між серверами SCADA і підключеними робочими станціями. Це може привести до затримки в передачі даних, збою в обміні даними і збою в центрі управління.

Крім того, сервер додатків в системі SCADA є ще однією метою атаки. Атакуючі можуть відправляти запити, що запитує сервер додатків для видачі критичних команд передньому процесору (FEP), <T71>. Якщо зловмисники отримують несанкціонований доступ до сервера додатків, вони можуть дізнатися точні додатки, які використовуються для управління частинами системи SCADA і взяти їх під контроль [7], <T72>. Після успішного проникнення в систему SCADA зловмисники можуть посилати сигнали збою системним вимикачам для ізоляції генераторів і шунтів і відключати навантаження [38]. Крім того, успішне проникнення на сервер додатків може надати зловмисникам доступ до команд, недоступним для системного оператора.

Шлях зв'язку між мережею SCADA і корпоративною мережею (включаючи використання клієнтських систем) може бути скомпрометований, <T47>. Клієнтські системи повинні управляти бізнесом SG, надаючи конкретну інформацію. Якщо клієнтська система зламана, зловмисники можуть отримати легкий шлях доступу до системи SCADA.

Оператори іноді отримують віддалений доступ до системи SCADA для забезпечення підтримки. Віртуальна приватна мережа (VPN) і корпоративна мережа забезпечують середню можливість прямого доступу до системи SCADA. Загроза оператора віддаленої підтримки включає в себе компрометацію клієнтської системи, підключеної до VPN, для отримання несанкціонованого віддаленого доступу до системи SCADA з будинків або офісів зловмисників. Атакуючі можуть використовувати погані конфігурації VPN і корпоративної мережі, щоб атакувати систему SCADA, а також <T45, T46, T47>. Іноді VPN-сервер покладається на VPN-клієнт для забезпечення прав доступу. Мережа VPN також інтегрована з центром управління, і зловмисники можуть використовувати цю функцію для атаки центру управління. Якщо віддалений оператор підтримки, підключений до центру управління, скомпрометований, зловмисники можуть мати можливість відключати вимикачі за допомогою SM для відключення електроживлення. Крім того, зловмисники можуть використовувати лінії зв'язку для точок входу віддаленого сайту, таких як засоби резервного копіювання, системи розробки та системи якості, <T73>. Канали зв'язку віддаленого сайту іноді не захищені фаєрволом або VPN. Якщо він правильно зламаний, зловмисники можуть безпосередньо отримати несанкціонований доступ до системи SCADA без необхідності зламати корпоративну мережу.

## 2.3 Моделі кібер втручань в Smart Grid

### 2.3.1 Моделі кібератак на SCADA

З літератури [4] та проведеного аналізу видно, що кібервтручання в основному пов'язані з «Атаками хибного введення даних» і «Атаками перерозподілу навантаженням».

*Атака хибного введення даних*

Під час роботи енергосистеми оцінка стану важлива для роботи оптимальної витрати енергії, аналізу непередбачених обставин, автоматичного генераторного управління і т. д.

Стани в енергосистемі є складною величиною напруги і кутів кожної шини. Якщо вектор стану X, то

$$X = [\delta_1, \delta_2, \delta_3 \dots \dots \delta_n \, V_1 V_2 V_3 \dots \dots \, V_n]^T$$

Стани системи не можуть бути отримані безпосередньо, тому важливо використовувати оцінку стану для виведення станів з виміряних значень. Однак виміряні значення можуть бути гучними, що збільшує ймовірність помилки. В результаті оцінку стану можна формулювати як зважений критерій найменшого квадрата нижче:

$$z_i = h_i(x)$$

в протилежному випадку

$$z_i = h_i(x) + e_i$$

де e являє помилку у вимірі.

З розгортанням Smart Grid оцінка стану стає вразливою до кібер-атак. Зловмисник може атакувати дані вимірювань системи SCADA. Таким чином, центр управління отримує наступні виміряні дані через атаки шкідливих даних:

$$z_i = h_i(x) + e_i + \alpha$$

де α - вектор атаки.

Значна кількість досліджень проводиться для запобігання введеня помилкових даних, які можна розділити на три категорії, як показано нижче.

1) Аналіз вразливості оцінки стану
2) Аналіз наслідків

3) Розробка контрзаходів

Клас «Хибна атака введення даних» в електричній мережі показує, що вчасно не відслідкована атака може бути введена на основі обмеженої кількості метрів, і може значно погіршити ефективність результатів, отриманих з оцінки стану. Незважаючи на те, що в класичному алгоритмі оцінки стану було встановлено метод виявлення поганих даних, атака шкідливих даних розглядається як «найгірші взаємодіючі погані дані», введені зловмисником.

*Атаки перерозподілу навантаження в енергосистемі*

Атака перерозподілу навантаження є підкласом помилкової атаки на ін'єкції даних. Економічна відправка і оптимальний потік потужності сильно залежать від виходу оцінки стану. Тому через атаки перерозподілу навантаження неправильна оцінка станів може привести до неекономічних рішень і порушити стабільні умови роботи. Значне дослідження було зроблено на основі «Помилковою атаки введення даних», однак деякі з них виконуються з урахуванням моделі атаки перерозподілу навантаження. Модель атаки перерозподілу навантаження може бути сформульована як проблема дворівневого програмування. Ця модель атаки перерозподілу навантаження показана нижче:

$$\sum_{\mathrm{d}} \Delta \mathrm{D}_{\mathrm{d}} = 0$$

$$\Delta \mathrm{PL} = -\mathrm{SF}.\,\mathrm{KD}.\,\Delta \mathrm{D}$$

$$-\tau D_d \leq \Delta D_d \leq \tau D_d$$

Атака перерозподілу навантаження штучно збільшує або зменшує попит на шинах навантаження, хоча повна зміна навантаження залишається рівним нулю, як показано в першому рівнянні. SF - матриця коефіцієнтів зсуву, а KD - матриця падіння навантаження. Величина атаки ΔDd обмежена в межах обмеження рівності, як показано в останньому рівнянні. Для вирішення проблеми атаки перерозподілу навантаження запропоновано метод Каруша-Куна-Таккера (KKT). Метод на основі KKT знаходить глобальне оптимальне рішення, він є дуже вимогливим до обчислення. Ефективність запропонованого методу значно зростає з використанням розкладання Бендери.

### 2.3.2 Моделі атак на перемикання та мережеві атаки

В роботі [5] розрізняють два типи команд перемикання:

1. Команди автоматичного перемикання: це команди, якими обмінюються між IED / Агентами, щоб усунути помилки короткого замикання, і вони зазвичай обмінюються по локальній мережі (LAN). Зазвичай ці повідомлення є командами перемикання DNP3.0 або командами GOOSE.

2. Команди ручного перемикання: це команди, відправлені системним оператором в центрі управління з глобальної мережі (WAN). Ці повідомлення можуть бути повідомленнями DNP3.0 або Routable GOOSE (R-GOOSE), як визначено в МЕК TR 61850-90-5 для маршрутизації GOOSE через WAN.

В табл. 2.2 надано класифікацію команд перемикання і можливих атак. Як видно з таблиці, повідомлення GOOSE представляють собою повідомлення рівня 2 Open System Interconnect (OSI), які обмінюються по локальній мережі.

Модель OSI ділить мережу на сім рівнів абстракції з метою забезпечення взаємодії з системами зв'язку. У цій роботі ми припускаємо, що зловмисник може виконати атаку спуфінга і відображення GOOSE. По-перше, зловмисник вивчає мережу для повідомлень GOOSE. Оскільки ці повідомлення незашифровані, зловмисник може декодувати вміст повідомлення GOOSE і змінювати поля даних (тобто Змінити команду ВІДКРИТИ на ЗАКРИТИ або навпаки).

Таблиця 2.2 – Класифікація команд перемикання і можливих атак

| ARP зараження людина-в-середині | Відкритий з'єднувальний шар системи | Мережа | Можливі атаки |
|---|---|---|---|
| GOOSE | Layer 2 Data Link (MAC) | LAN | Зараження і спуфінг GOOSE |
| R- GOOSE | Layer 3 Network (IP) | LAN/WAN | ARP зараження людина-в-середині |
| DNP3.0 | Layer 4 Transport (TCP/IP) | LAN/WAN | ARP зараження людина-в-середині |

Важливо розуміти, що повідомлення GOOSE управляються подіями, і кожне повідомлення пов'язано з інкрементним лічильником, так званим номером статусу (stNum). Наприклад, IED починається з відправки повідомлення GOOSE за допомогою stNum = 1. Якщо станеться помилка, IED розпізнає цю помилку і видасть нові команди GOOSE за допомогою stNum = 2, щоб відкрити автоматичний вимикач і усунути несправність.

Знаючи це, зловмисник потім публікує хибне повідомлення GOOSE з новим інкрементом stNum і підробленою MAC-адресою. Тобто, зловмисник використовує MAC-адресу початкового відправника. Цей процес показаний на рисунку 2.2а.

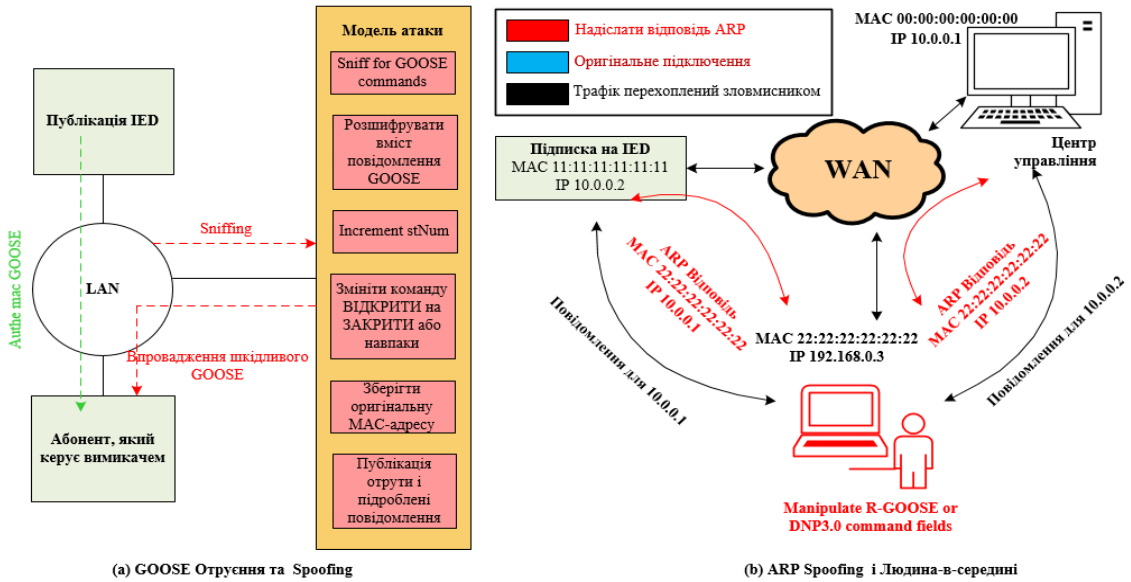


Рисунок 2.2 – (а) Процедура зараження GOOSE і Spoofing; (б) зараження ARP і R-GOOSE і DNP3.0 Атака «Людина в центрі».

У таблиці 2.2 також показано, що R-GOOSE і DNP3.0 є повідомленнями рівня 3 і рівня 4, відповідно. Це означає, що вони обмінюються по IP-мережі. Вони сприйнятливі до відбиття протоколу дозволу адреси (ARP) і нападам «людина в центрі». ARP - це протокол зв'язку, який використовується для перетворення IP-адресів в MAC-адреси. Як показано на рисунку 2b, зловмисник відправляє відповідь ARP для установки підробленої IP-адреси і зіставлення MAC-адреси іншим хостам в мережі. Таким чином, IP-адреса зловмисника тепер пов'язана з неправильною MAC-адресою. Це дозволяє зловмисникові перехоплювати повідомлення, якими обмінюються центр управління та IED абонента. Потім зловмисник може виконати атаку «Людина в центрі» і маніпулювати полями даних в пакетах R-GOOSE або DNP3.0.

Хоча більшість промислових комунікаційних мереж не відкриті для загальнодоступного Інтернету, можна припустити, що до них можна проникнути через корпоративні мережі або персональні пристрої співробітників за допомогою таких методів, як злом паролів, бекдор і промахів серед інших.

### 2.3.3 Аналіз безпеки і аудит автоматизованих підстанцій на базі МЕК 61850

В даному підрозділі розглядається схема аудиту безпеки мережі та інтелектуальних електронних пристроях (IED) на базі МЕК 61850, запропонована в [6]

У загальному вигляді, аналіз безпеки на автоматичної підстанції МЕК 61850 виконується спочатку з упором на можливі цілі зловмисника. Далі йде розробка схеми

аудиту безпеки такої мережі. Враховуються показники безпеки, оскільки вони забезпечують відчутні способи кількісної оцінки безпеки мережі. Схема аудиту перевіряється, використовуючи її для перевірки безпеки мережі МЕК 61850. Потім результати порівнюються з двома іншими метричними схемами: метрикою Mean Time to Compromise (MTTC) і метрикою VEA-bility, які використовуються для аудиту звичайних комп'ютерних мереж. Вхідні дані для обох показників отримані за допомогою засобу мережевої безпеки для сканування IED-мереж мережі. На додаток досліджується вплив використання засобів безпеки мережі з високою пропускною спроможністю на критичну за часом мережу МЕК 61850. Індексні терміни - безпека інформації, аналіз безпеки, аудит безпеки, показники безпеки, МЕК 61850, засоби забезпечення безпеки, автоматизація підстанцій.

Перший етап починається з аналізу безпеки електричних підстанцій. Потім слід введення в пропоновану схему аудиту. Далі представлений новий показник для ІЕУ. Розглянуто і досліджено вплив засобів безпеки на мережу. В кінцевому підсумку детально викладаються результати вибіркового аудиту з використанням схеми.

*Аналіз безпеки*

Мета аналізу безпеки - виявити можливі загрози для автоматичної підстанції МЕК 61850. Існують численні схеми для ідентифікації різних аспектів інформації та мережевої безпеки. Ці схеми можна розділити на дві основні категорії, які є ідентифікацією відповідно до перспективи захисника або перспективою зловмисника.

*A. Перспектива захисника*

Аналіз безпеки в перспективі захисника передбачає розгляд вимог безпеки. Це призводить до політики безпеки, яка, в свою чергу, вимагає наявності механізмів забезпечення безпеки. Виконуваність політики безпеки залежить від використовуваних механізмів, які повинні бути обрані таким чином, щоб вони не погіршували продуктивність системи.

*B. Перспектива атакуючого*

Інший метод проектування безпеки включає розгляд проблеми з точки зору зловмисника. Інтуїтивно ця перспектива більш ефективна, тому що зловмисник завжди мотивований на досягнення поставленої мети. Дослідження в цьому контексті більш реалістичні, оскільки дані можуть бути отримані за допомогою імітованих атак і мереж приманки, відомих як Honeypots.

*C. Ідентифікація загрози*

Наступним кроком буде застосування методу аналізу для системи на базі МЕК 61850.

У цьому контексті дві основні мети зловмисників можуть бути ідентифіковані з використанням перспективного підходу, атакуючого. це:

1) Порушення служби сервісу (атака на доступність).

2) Отримання доступу до конфіденційної інформації для зловмисних цілей, таких як недобросовісна конкуренція, шантаж і т. д. (Атака на конфіденційність).

Потім ці дві мети можна проаналізувати детально, щоб визначити методи, які зловмисник може використовувати для їх досягнення. Такі загальні атаки разом з їх можливими контрзаходами можна визначити, використовуючи підхід Ohta і Chikaraishi [7], як показано в таблицях 2.3 і 2.4.

Таблиця 2.3 – Атаки на конфіденційність

| Шар | Атака | Механізми безпеки |
|---|---|---|
| Вузол | Доступ до вузла для отримання конфіденційної інформації | Контроль доступу<br>Шифрування<br>Аутентифікація<br>Перевірка цілісності<br>Виявлення вторгнень |
| | Хибна команда | Аутентифікація<br>Перевірка цілісності |
| LAN | Доступ до інфраструктури LAN або WLAN для перехоплення конфіденційної інформації | Контроль доступу (як фізичний, так і логічний)<br>Шифрування<br>Аутентифікація<br>Перевірка цілісності виявлення вторгнень |
| | Хибна команда | Аутентифікація<br>Перевірка цілісності |
| WAN | Перехоплення конфіденційної інформації у шляху по глобальній мережі | Шифрування<br>Аутентифікація<br>Перевірка цілісності |
| | Хибна команда | Аутентифікація<br>Перевірка цілісності |

Таблиця 2.4 – Руйнування обслуговування

| Шар | Атака | Механізми безпеки |
|---|---|---|
| Дані | Знищення даних | Процедура резервного копіювання |
| Вузол | Використання вузла для DoS-атаки | Контроль доступу<br>Аутентифікація<br>Перевірка цілісності<br>Виявлення вторгнень |
| | DoS-атака на критичному вузлі | Контроль доступа<br>Аутентифікація<br>Перевірка цілісності<br>Виявлення вторгнень<br>Надмірність |
| | Хибна команда | Перевірка цілісності аутентифікації |

Продовження таблиці 2.4

| | | |
|---|---|---|
| LAN | DoS attack on LAN or WLAN infrastructure | Контроль доступу (як фізичний, так і логічний)<br>Аутентифікація<br>Перевірка цілісності<br>Резервування виявлення вторгнень |
| | Хибна команда | Перевірка цілісності аутентифікації |
| WAN | DoS attack on WAN infrastructure | Надмірність |
| | Хибна команда | Перевірка цілісності аутентифікації |

*D. Механізми безпеки МЕК 61850*

Існуючі механізми безпеки МЕК 61850, які згадуються в МЕК 62351-4 і МЕК 62351-6 включають:

1) МЕК62351-4 визначає шифри, які використовуються МЕК 61850 для шифрування. Крім того, МЕК62351-6 визначає використання безпеки транспортного рівня (TLS).

2) Безпека для профілів МЕК 61850 з використанням VLAN. Поділ мережі на VLAN запобігає несанкціонований доступ до IED за межами виділеної VLAN.

3) Безпека для простого мережевого протоколу часу (SNTP) за допомогою обов'язкового використання алгоритмів аутентифікації RFC2030. Це запобігає несанкціоноване використання пакетів помилкових тимчасових штампів.

4) Явна протидія атакам «людина-в-середині» і фальсифікація з використанням коду аутентифікації повідомлення (MAC) стандарту МЕК 62351-6.

5) Явна протидія повторним атакам через спеціалізовані машини обробки станів, згадані в МЕК 62351-4.

Ці механізми безпеки здатні протистояти значній кількості загроз безпеці, перерахованих в таблицях I і II. Проте, певний зловмисник повинен впроваджувати нові методи з плином часу, щоб скомпрометувати ці існуючі механізми безпеки.

*Схема реалізації безпеки*

Аудит безпеки - це процес оцінки безпеки комп'ютерної системи і надання рекомендацій клієнту. Перевірювана мережа МЕК 61850 складається з IED, комутаторів, маршрутизаторів, брандмауерів / шлюзів, HMI і серверів. Пропонована схема аудиту складається з наступних етапів:

1) попереднє опитування мережі для визначення її компонентів, топологій і т. д.

2) Оцінка безпеки хостів мережі (наприклад, IED, шлюзу, HMI і серверів) та інших компонентів (наприклад, комутаторів і маршрутизаторів).

3) Розкриття результатів і рекомендацій клієнту

4) Перевірка виконання рекомендацій

Основна увага приділяється оцінці безпеки хостів. Цей етап складається з:

1) Оцінка інструменту безпеки, щоб визначити потенційно вразливі місця всій мережі, які можуть бути видні зловмисникові

2) Оцінка ІЕУ для виявлення вразливостей кожного ІЕУ і розрахунку запропонованої метрики ІЕУ з отриманих результатів

Обсяг цієї схеми аудиту орієнтований на мережеву інфраструктуру і може бути інтегрований в аудит безпеки організації, такий як ISO / МЕК 27001.

*Метрика безпеки novel ied*

Основна мотивація досліджень по отриманню показників для мережевої безпеки - це матеріальні засоби вимірювання безпеки мережі. Через технічну різницю між IED і стандартним комп'ютером, застосування Common Scaling System (CVSS) для погроз може бути виконано тільки для комп'ютерних вузлів МЕК 61850, таких як сервери баз даних, інженерні станції, HMI і шлюзи. Необхідна абсолютно нова метрична схема для ІЕУ. Ця нова метрична схема порівнюється з метриками безпеки, розробленими для звичайних комп'ютерів. До них відносяться середній час для компромісів (MTTC), запропоноване Leversage and Byres і McQueen et al. і метрика VEA-доступності, запропонованої Таппер і Цінціром-Хейвудом.

Якщо подивитися на IED з точки зору зловмисників, різні категорії IED матимуть різний рівень важливості в залежності від мети атакуючого. Залежно від їх важливості різні підрозділи матимуть різні рівні безпеки. Тому показник безпеки для IED повинен мати такі властивості:

1. Здатність оцінювати загрозу для ІЕУ на основі мети атакуючого.
2. Він повинен кількісно визначати вразливість ІЕУ на основі його функцій безпеки.
3. Він повинен бути здатний протиставляти безпечну і небезпечну мережу, подібну метриці VEA-bility.

*А. Ідентифікація загрози*

Перший крок - виявити загрози для різних категорій ІЕУ. Це робиться шляхом вибору категорій ІЕУ відповідно до їх призначеної категорії функцій і визначення можливих сценаріїв атаки, як фізичних, так і логічних. Крім того, приховані загрози безпеки через використання небезпечних протоколів (наприклад, ftp, telnet) або вразливостей безпеки в операційних системах можуть бути ідентифіковані за допомогою перевірки, виконаної засобом безпеки. При використанні в широких категоріях можливі сценарії включають:

1) Unauthorized Access (UA) - доступ до IED, щоб дати помилкову команду, змінити налаштування або отримати доступ до конфіденційних даних.

2) Відмова в обслуговуванні (DoS) - виключення ІЕУ з мережі шляхом його відключення або придушення.

3) Spoof (SP) - IED підміняється фізично або логічно, щоб ввести в оману інші пристрої.

4) Дані перехоплення даних (DI) перехоплюються.

5) Stepping Stone (SS) - IED можна логічно використовувати в якості кроку для запуску атаки на іншу мету.

*B. Ідентифікація протидії*

Як тільки загрози для ІЕУ були ідентифіковані, тепер можна перевірити, чи є у пристрої відповідні заходи безпеки. Вони визначаються:

1. Перевірка функцій безпеки IED, зазначених виробником (наприклад, шифрування даних, використання захищених протоколів).

2. Вивчення механізмів безпеки мережевої інфраструктури (наприклад, обмеження MAC-адрес комутаторами для боротьби з атакою сніффер DoS або ARP).

3. Якщо у пристрої є уразливості в його програмному забезпеченні або операційній системі, перевірте наявні контрзаходи в репозиторіях вразливостей, таких як база даних Common Vulnerabilities and Exposures (CVE).

Якщо конкретна загроза має відповідні контрзаходи, вона може бути скасована (тобто виключена) зі списку загроз.

*C. Сприйнятливість*

Кожна загроза також може бути скоригована відповідно до її відносної сприйнятливості. Наприклад, для того щоб обдурити конкретне ІЕУ, може знадобитися фізичне маніпулювання пристроєм.

*D. Метрична формула і розрахунок*

З цього можна привести формулу для кількісної оцінки безпеки IED і мережі МЕК 61850. Процедура розрахунку включає:

2) Попередня ідентифікація всіх відомих загроз для кожного окремого IED (m загроз).

3) Ідентифікація доступних контрзаходів для кожної загрози i (де i = 1, 2, ..., m). Якщо конкретна загроза має одну або кілька контрзаходів, її коефіцієнт протидії ($c_i$) встановлюється рівним одиниці. Значення $c_i$ встановлюється рівним нулю, якщо не існує ніяких контрзаходів.

4) Ідентифікація сприйнятливості ($s_i$) кожної загрози:

- Якщо атака може бути виконана на ІЕУ віддалено з глобальної мережі, підключеної до мережі IEC61850, $s_i = 1$
- Якщо він повинен бути виконаний з мережі IEC61850 (LAN), $s_i = 0,2$
- Якщо для запуску атаки потрібно фізична маніпуляція, $s_i = 0,1$

Значення вибираються таким чином, щоб відносний ризик між атакою на вузлі, локальною мережею або глобальною мережею був протилежний за їх ймовірності.

Найбільш імовірним типом атаки є віддалена атака, запущена з віддаленого місця розташування, в той час як найменш ймовірна атака пов'язана з фізичним маніпулюванням пристрою, де існує високий ризик виявлення зловмисника.

5) Виходячи з цього, оцінка може бути розрахована для кожної загрози

6) З цього можна обчислити оцінку для кожного ІЕУ

7) Нарешті, можна отримати оцінку для всієї мережі. Щоб обчислити оцінку для конкретної загрози ($t_i$) на основі її сприйнятливості ($s_i$) і коефіцієнта протидії ($c_i$).

$$t_i = s_i(1 - c_i)$$

Таким чином, оцінка для $j^{th}$ IED за допомогою $m_j$-загроз буде:

$$E_j = \sum_{i=1}^{m_j} t_i$$

Нарешті, загальний бал мережі з n IED може бути розрахований з:

$$R = 10 - \min(10, \sum_{j=1}^{n} E_j)$$

*Е. Поріг дотримання*

На основі остаточної оцінки (R) можна визначити поріг відповідності. Наприклад, мережа може вважатися безпечною тоді і тільки тоді, коли оцінка для R перевищує 9. У такому випадку:

– Невелика вразливість, при якій атака повинна виконуватися шляхом безпосереднього управління IED або локальною мережею, призведе до зниження оцінки до 9,9 або 9,8 відповідно

– Якщо мережа має серйозну вразливість, коли атака може бути запущена через WAN, оцінка буде дорівнює 9, тому мережа буде вразливою і несумісною

– Якщо є невелика кількість серйозних вразливостей або велика кількість незначних вразливостей, оцінка буде прагнути до нуля і вказувати на вкрай небезпечну мережу

У зв'язку з цим нормалізація результату відповідно до розміру мережі або з урахуванням географічного поширення не потрібно.

*Аналіз транспортного забезпечення безпеки*

Час доставки для певних пакетів IEC61850 має вирішальне значення. Пропонована схема аудиту безпеки в значній мірі залежить від даних, отриманих при скануванні на ІЕУ, з використанням засобів безпеки. Тому необхідно оцінити вплив трафіку, що генерується засобом безпеки, що використовуються в мережі. Це вимагає збору даних, моделювання і тестування доступних засобів мережевої безпеки і зважування їх проти їх переваг.

*А. Збір даних*

Дані збираються з використанням Ethereal, аналізатора з відкритим вихідним кодом, доступного як на платформах Windows, так і на Linux. Поки Ethereal працює, кожен інструмент безпеки використовується для сканування цільової машини. Потім отриманий трафік захоплюється і використовується для аналізу. Випробувано всього 10 цільових машин, з яких 5 мають операційні системи на базі Windows, а решта - операційні системи на базі Linux. Перевіреними мережевими інструментами були Nessus 3.2.1 і NMap 4.68. Обидва інструменти були протестовані на платформах Windows і Linux.

*В. Аналіз даних.*

Зібрані дані потім аналізуються з використанням MATLAB. Спочатку обчислюється миттєва швидкість трафіку в пакетах в секунду для кожного сканування. Якщо швидкість миттєвого трафіку більше 100 пакетів / с, то вважається високою і на підставі цього досягається час, протягом якого генерується високий трафік. З цього часу середній час, протягом якого засіб безпеки генерує високий трафік, може бути отриманий. У таблиці 2.5 приведена статистика трафіку для кожного інструменту для конкретної платформи хоста. Відповідно до цього, Nessus, який виконує більш повний набір тестів, займає більше часу, щоб оцінити машину Windows, ніж комп'ютер Linux. Те ж саме можна сказати і про Nmap. Важливим фактором, який слід враховувати, є час, протягом якого інструмент генерує високий трафік. У таблиці 2.5 наведено короткий опис високого завантаження для різних інструментів і цільових машин. Подальше вивчення впливу засобів безпеки здійснюється шляхом моделювання.

*C. Паралельні сканування*

Nessus 3.2.1 дозволяє паралельно сканувати кілька хостів. На рисунку 2.3 показаний трафік, що генерується при паралельному скануванні 5 хостів. Час сканування становить приблизно 140 с, але середній трафік складає близько 3000 пакетів / с, що майже в 5 разів більше максимального значення для одного хоста (таблиця 2.6). Протягом майже 80% часу сканування (110 секунд) трафік значно перевищує 100 пакетів / с.

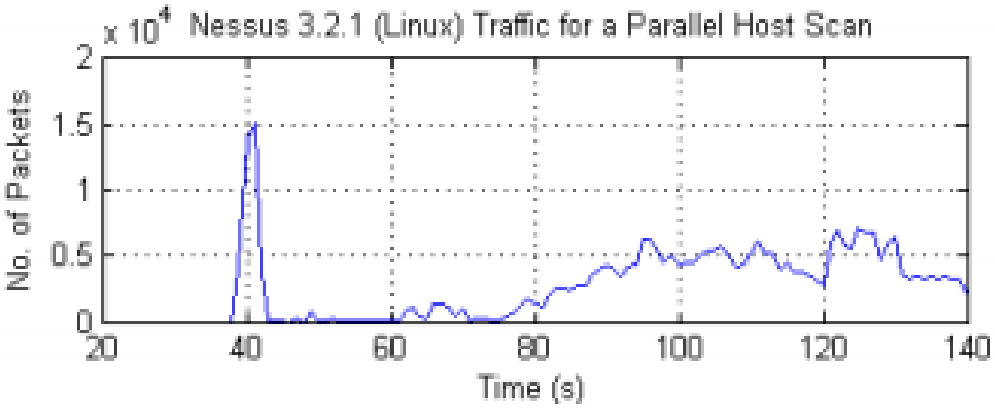


Рисунок 2.3 – Трафік, створений Nessus 3.2.1 (Linux) для паралельного сканування хоста

Таблиця 2.5 – Статистика роботи засобів забезпечення безпеки

| Платформа цільового вузла | Середні тарифи (пакети / с) | Середні тарифи (пакети / с) | | | Середній час сканування | |
|---|---|---|---|---|---|---|
| | | Середн | Макс | Високий (%) | Усього | Високий |
| Windows | Nessus 3.2.1 (Windows) | 377.0 | 11360.0 | 5.67 | 861.2 | 48.9 |
| | Nessus 3.2.1 (Linux) | 145.4 | 3079.2 | 13.74 | 225.8 | 31.0 |
| | NMap 4.68 (Windows) | 58.6 | 1073.2 | 11.96 | 90.0 | 10.8 |
| | NMap 4.68 (Linux) | 172.2 | 919.2 | 29.18 | 42.4 | 12.4 |
| Linux | Nessus 3.2.1 (Windows) | 208.2 | 2750.2 | 17.13 | 188.2 | 32.2 |
| | Nessus 3.2.1 (Linux) | 677.7 | 8760.4 | 39.45 | 75.2 | 29.7 |
| | NMap 4.68 (Windows) | 125.7 | 2634.0 | 39.45 | 32.0 | 2.4 |
| | NMap 4.68 (Linux) | 157.8 | 1957.2 | 9.58 | 33.2 | 3.2 |

*D. Моделювання*

Моделювання ефекту інструменту безпеки виконується з використанням симулятора з відкритим вихідним кодом під назвою Network Simulator 2.33 (NS 2.33). Використовуючи

симуляцію, аналізуються затримки і швидкість передачі пакетів і порівнюються із стандартами МЕК 61850-5.

1) Модель IED: NS-2 логічно абстрагує мережевий вузол (рисунок 2.4) в вузол, який містить посилання на дані і фізичні рівні моделі OSI. Мережевий і транспортний рівні обробляються сутністю, відомої як агент, в той час як прикладний рівень обробляється додатком. Елементи з'єднання використовуються разом для з'єднання вузлів.

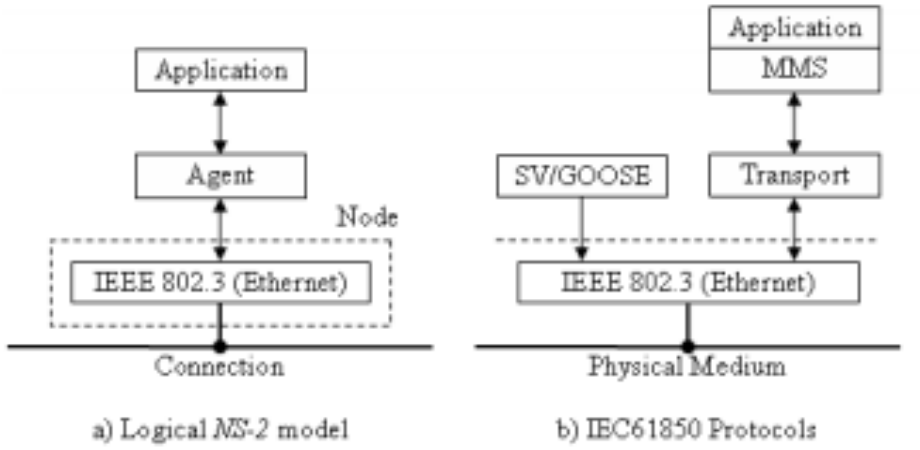


Рисунок 2.4 – Логічна модель NS-2

Для зв'язку двох вузлів відправляючий вузол повинен мати відповідний вихідний агент для передачі даних відповідно до необхідного протоколом і додатком. Приймаючий вузол повинен мати агент-приймач. При моделюванні IED з використанням NS-2 можна моделювати пакет, який обходить стек TCP / IP в якості агента UDP з постійним бітрейтом (CBR). Інші пакети, які використовують стек протоколу TCP / IP, можуть бути змодельовані з використанням різних агентів TCP.

2) Мережа підстанцій: для моделювання повинні бути побудовані ІЕУ, відповідні відсіку трансформатора і фідерному відсіку. Фідерний відсік буде складатися з складального блоку (MU), в якому використовуються необроблені зразки даних, два захисних і керуючих реле (ПК) для контролю необроблених даних і автоматичного вимикача (СВ) для роботи у відповідності з несправністю. Трансформаторний відсік буде складатися з MU, двох ПК і двох СВ. Все ІЕУ конкретного відсіку будуть підключені до одного комутатора.

На рисунку 2.5 показано фізичне і логічне з'єднання мережі відсіку. Кожен перемикач байпаса, в свою чергу, підключається до перемикача центральної станції. Сервер, що збирає дані з підстанції та HMI, також буде підключений до цього комутатора. Вся топологія мережі станцій показана на рисунку 2.6.

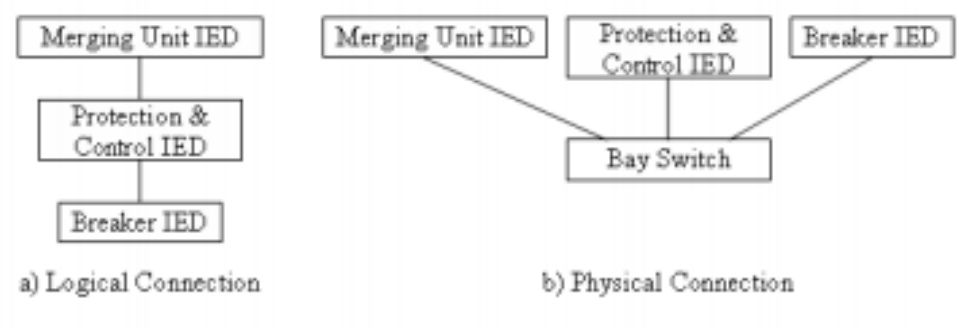


Рисунок 2.5 – Фізичне і логічне з'єднання мережі затоки

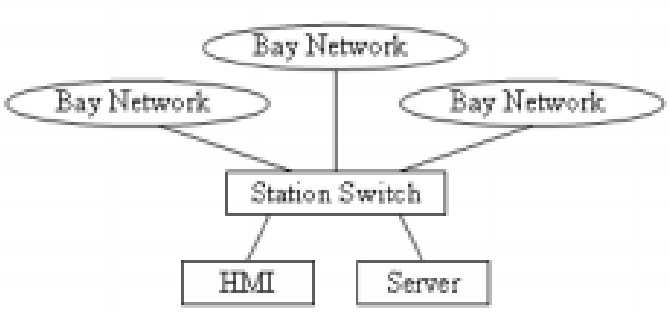


Рисунок 2.6 – Топологія всій мережі підстанцій

Для моделювання використовуються підстанції, що складаються з двох відсіків трансформаторів і від двох до шести відсіків трансформаторів. Передбачається, що кожен MU приймає 1920 вибірок сирих даних в секунду для забезпечення захисту класу P3. Під час збою ПК IED відправляє пакети GOOSE в CB, а CB повертає відповідь для підтвердження прийому. Чотири пакета обмінюються по-різному. Помилка виражається кожні 0,5 с. Крім того, кожен ПК IED завантажує на сервер 2-кратний звіт про стан кожні 2 секунди.

3) Модель обладнання безпеки: наступний етап моделювання включає розробку моделі для інструменту безпеки. Передбачається, що під час аудиту безпеки він буде підключений до комутатора станції через ноутбук. Інструмент безпеки моделюється як сплеск великого трафіку, який триває час завантаження. Через обмеження часу моделювання і для узагальнення ситуації тривалість пакета обмежена 10 секундами, протягом яких генерується трафік в 1000 пакетів в секунду. Агент UDP з трафіком Pareto використовується для створення трафіку засобів безпеки.

4) Результати. У табл. 2.6 показані результати моделювання для 10 Мбіт / с і 100 Мбіт / с Ethernet відповідно з точки зору затримки пакетів і швидкості передачі.

Таблиця 2.6 Результати моделювання мережі

| Сценарій | 2 відсіку для подачі | | | | 4 відсіку для подачі | | | | 6 відсіків для подачі | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Затримка (мс) | | Падіння (%) | | Затримка (мс) | | Падіння (%) | | Затримка (мс) | | Падіння (%) | |
| | 10 Mb | 100 Mb | 10 Mb | 100 Mb | 10 Mb | 100 Mb | 10 Mb | 100 Mb | 10 Mb | 100 Mb | 10 Mb | 100 Mb |
| 1 | 9.81 | 1.17 | 3.79 | 1.35 | 10.10 | 1.21 | 3.97 | 1.52 | 9.49 | 1.17 | 3.78 | 1.40 |
| 2 | 11.15 | 1.15 | 4.75 | 1.72 | 10.33 | 1.20 | 4.08 | 1.61 | 10.45 | 1.15 | 4.60 | 1.70 |
| 3 | 5.76 | 1.23 | 34.46 | 14.02 | 7.04 | 1.21 | 26.55 | 7.57 | 9.04 | 1.15 | 36.07 | 6.76 |
| 4 | 7.35 | 1.23 | 41.43 | 10.53 | 8.10 | 1.25 | 23.97 | 9.41 | 8.20 | 1.19 | 25.05 | 8.06 |
| 5 | 12.24 | 1.19 | 10.80 | 1.94 | 9.73 | 1.16 | 6.50 | 1.50 | 10.52 | 1.17 | 6.05 | 1.50 |
| 6 | 10.57 | 1.16 | 8.58 | 1.91 | 11.54 | 1.25 | 6.85 | 1.82 | 9.94 | 1.16 | 6.60 | 1.95 |
| 7 | 7.45 | 1.20 | 43.05 | 10.45 | 7.78 | 1.24 | 28.23 | 8.44 | 8.70 | 1.21 | 25.72 | 5.77 |
| 8 | 7.73 | 1.22 | 32.36 | 7.85 | 8.68 | 1.21 | 15.11 | 11.51 | 9.39 | 1.19 | 33.64 | 6.60 |

Моделювання виконується для наступних сценаріїв:

1) Нічого (тільки значення вибірки)
2) Система з передачами ftp
3) Система з запущеним інструментом безпеки
4) Обидві передачі ftp і інструмент безпеки
5) Система з несправністю
6) Помилка з ftp-передачами
7) Несправність за допомогою інструменту безпеки
8) Помилка з передачею ftp і інструментом безпеки

Результати показують, що кожного разу, коли використовується інструмент, спостерігається значне збільшення швидкості передачі пакетів. Ефект від затримки пакетів не представляється значним. Незважаючи на це, безпека мережі як і раніше залежить від того, що під час використання інструменту безпеки критичний пакет (наприклад, GOOSE-пакет) може бути видалений.

### 2.4 Висновки до розділу 2

Щоб зробити Smart Grid розумнішими, у всьому світі робляться значні ініціативи. Ці заходи будуть не тільки модернізувати сітку, але і підвищувати загальну ефективність, стабільність і надійність системи. Але проблеми безпеки повинні підтримуватися для

забезпечення безперебійного енергопостачання кінцевих користувачів і захисту національної електричної мережі від терористичних атак. Важливо відзначити, що належним чином розроблена захисна оболонка проти кібер-атаки повинна охоплювати всі аспекти, пов'язані з кібер-злочинністю, в складній кібер-фізичної інфраструктурі електромереж. Це означає, що слід розглядати не тільки цілеспрямовану кібер-атаку, але також слід враховувати ненавмисні аномалії, пов'язані з ІКТ, наприклад, помилки оператора, помилки програмного забезпечення, збої устаткування і, очевидно, проблеми, пов'язані зі стихійним лихом.

У процесі підвищення енергоефективності енергосистеми в сітці впроваджується більш автоматизоване управління. Ризик кібер-атаки буде зростати в міру того, як сітка стане більш автоматизованою. Спеціально, центри управління є головною метою кібер-терористів. Енергетичні підприємства застосовують передові технології і плани кібербезпеки, щоб уникнути кібератаки. Розширені методи виявлення і запобігання вторгнень можуть бути реалізовані в різних точках входу в складну сітку. Системи управління безпекою впроваджуються в різних утиліти. Постачальники енергії також приймають різні стратегії управління ризиками та захисний підхід до кібератаки.

Очевидно, що інтелектуальна мережа надає безліч переваг, в тому числі енергоефективний розумний будинок, більш екологічні технології, такі як сонячна енергія і вітер, економічне управління попитом, інтелектуальні зарядні станції для електромобілів і так далі. Для забезпечення цих переваг необхідно підтримувати заходи безпеки в мережі.

### 2.5 Перелік посилань до розділу 2

1. Annex II. Security aspects of the smart grid «SMART GRID SECURITY», 2012;
2. Mustafa Saed, Kevin Daimi, Nizar Al-Holou «SMART GRID SECURITY CONCEPTS AND ISSUES», 2013;
3. Husam Suleiman, Israa Alqassem, Ali Diabat, Edin Arnautovic, Davor Svetinovic «Integrated smart grid systems security threat model», 2014;
4. Adnan Anwar, Abdun Naser Mahmood «Cyber Security of Smart Grid Infrastructure», 2014;
5. Mohamad El Hariri, Samy Faddel, Osama Mohammed «Physical-Model-Checking to Detect Switching-Related Attacks in Power Systems», 2018;
6. Upeka Premaratne, Jagath Samarabandu, Tarlochan Sidhu, Robert Beresh, Jian-Cheng Tan «Security Analysis and Auditing of IEC61850 Based Automated Substations», 2010;
7. T. Ohta and T. Chikaraishi «Network security model», 1993.

# РОЗДІЛ 3 РОЗРОБКА МОДЕЛІ ОЦІНКИ КІБЕРБЕЗПЕКИ СИСТЕМИ РЗА ДЛЯ SMART GRID

## 3.1 Аналіз впливу кібератак

Процес оцінки вразливості для постачальників енергетичної інфраструктури включає ряд етапів аналізу:

– характеристика інформаційних загроз з боку фінансово мотивованих осіб / організацій, інформаційних воєн з боку інших країн, екологічних або політичних терористів і неструктурованих супротивників;

– аналіз архітектури кібер-мережі для визначення процедур забезпечення інформації

– тестування на проникнення для виявлення вразливостей мережі;

– аналіз взаємозалежності з іншими критично важливими інфраструктурами, такими як телекомунікації і транспорт;

– аналіз впливу несанкціонованого доступу до кібер-інфраструктури на фізичні операції системи.

Характеристика ризику даного збою *F* пов'язана з ймовірністю і серйозністю системних вразливостей, погроз і процесів атаки, що викликають *F*, а також з впливом, кількісно визначає наслідки *F* для служби харчування.

Ризик визначається як:

$$R\,(F) = L\,(F) \times I\,(F), \tag{3.1}$$

де R (F), L (F) і I (F) представляють ризик, ймовірність і вплив даного збою F через кібератаки. Імовірність L (F) може бути розбита на добуток імовірності загроз і вразливостей, щоб дати тривимірний метод оцінки ризику.

$$R\,(F) = L\,(F) \times I\,(F) = T\,(F) \times V\,(F) \times I\,(F), \tag{3.2}$$

де *T (F)* і *V (F)* позначають ймовірність загроз і вразливостей, пов'язаних з *F*. Бракує історичних даних для достатньої оцінки будь-якої з перерахованих вище величин, що вимагає розробки відповідних інструментів аналізу, орієнтованих для нових енергетичних систем.

Запропонована парадигма для аналізу впливу кібератак, в якій використовується теоретико-графічна структура і структура динамічних систем для моделювання складних взаємодій між різними компонентами системи [1].

### 3.2 Аналіз застосування графів і динамічних систем

Граф - це математична структура, яка представляє попарні відносини між набором об'єктів. Граф визначається набором вершин (також званих вузлами) і набором ребер, які з'єднують пари вузлів. Залежно від використання графа його ребра можуть мати або не мати напрям, що веде до спрямованих або неорієнтованих класів графів відповідно. Графіки надають зручний і компактний спосіб показати взаємозв'язок і взаємозв'язок залежностей в кібер-фізичних енергетичних системах. Моделювання електричної мережі є життєво важливим компонентом ефективної структури аналізу впливу.

Один підхід до фізичного моделювання складних інженерних взаємодій використовує динамічні системи. Динамічна система - це математична формалізація, використовувана для опису еволюції в часі стану $x$, яка може представляти вектор фізичних величин. У безперервному часу детерміноване правило еволюції описує майбутні стани з поточних станів наступним чином [1]:

$$\dot{x} = f(x, u) \tag{3.3}$$

де $\dot{x}$ - похідна за часом від $x$, а $u$ - вхідний вектор. Теорія динамічних систем мотивується звичайними диференціальними рівняннями і підходить для представлення складних фізичних взаємодій енергосистеми.

Формулювання динамічних систем на основі графів ефективне для структури аналізу впливу кібератак на Smart Grid по ряду причин.

По-перше, аналіз впливу Smart Grid вимагає співвіднесення кібератак з фізичними наслідками в електричній мережі. Парадигма динамічних систем забезпечує гнучку структуру для моделювання (з різним ступенем деталізації і серйозності) причинно-наслідкових зв'язків між кібер-даними і сигналами стану електричної мережі і пов'язує їх з показниками доставки енергії. Можуть бути представлені вторинні ефекти, за допомогою яких наслідки самої атаки впливають на триваючу ступінь атаки.

По-друге, графіки забезпечують більш тісний зв'язок між кібер і фізичними доменами. Для Smart Grid кібер-фізичне з'єднання часто представляється через керуючі сигнали, які приводять в дію зміни в енергосистемі, а фізичне кібер-з'єднання зазвичай

відбувається через отримання показань датчика стану харчування. Ці зв'язки можуть бути виражені як спеціально розташовані ребра графіків. Графи викликають динамічний системний опис всієї Smart Grid, яка зручно висловлює складні змінювані в часі взаємозв'язку. Таким чином, можуть бути представлені каскадні збої і виникаючі властивості високо пов'язаної системи. Підходи до пом'якшення часто включають в себе виділення grid або розбиття основних компонентів Smart Grid на функції оптимізації, і формулювання динамічних систем на основі графів також може відображати такий поділ.

Основний ефект включення кібератак в традиційний аналіз надійності полягає в тому, що він збільшує розмір досліджуваної системи на кілька порядків. Запропоноване математичне формулювання має потенціал для того, щоб дослідження можна було відстежувати, тому що дана деталізація деталей може бути налаштована, а використання динаміки може забезпечити складну поведінку без відповідного збільшення складності.

### 3.3 Синтез моделі динамічних систем на основі графів

Вихідні дані етапу перевірки використовуються для повторного калібрування запропонованого підходу до синтезу.

На етапі синтезу даної моделі були використані динамічні системи для систематичного моделювання кібер і електричних мереж. Це дозволило гнучко налаштувати деталізацію деталей. Використання графів зручно полегшує включення складних залежностей усередині і між кібер і електричними компонентами. Цей етап є критичним, так як він визначає відносну точність аналізу впливу Smart Grid і визначає можливі інструменти аналізу, що дозволяють отримати уявлення про уразливість і стратегії зміцнення системи. Розроблено загальний і системний підхід до моделювання системи Smart Grid з використанням динамічного системного підходу на основі графів.

*Система з одним генератором*

У дослідженні використано схему лінійної системи живлення ГЕС (рис. 3.1). У вихідній системі $G_1$, $G_2$ і $G_3$ є звичайними генераторами, які обслуговують чотири навантаження, позначені $Z_1, Z_2, Z_3$ и $Z_4$. Трансформатори $T_1, T_2, T_3, T_4, T_5, T_6$ знижують напругу і підключаються до кабелів 3, 4, 5, 6, 7, 12, 13. Кабелі 1, 2, 3, 10, 11 і 12 підключаються до навантажень, як показано на рисунку 3.1. Шестикутні символи представляють кібер-інфраструктуру. Показано центр управління системою, і він передає сигнали управління кожному з шести показаних перемикачів. Для перемикача $i$ (позначеного шестикутником з $i$ в центрі) центр управління передає керуючий сигнал $c_i(t)$, де $c_i(t) = 0$ позначає відкритий перемикач, а $c_i(t) = 1$ означає закритий перемикач в момент часу $t$.

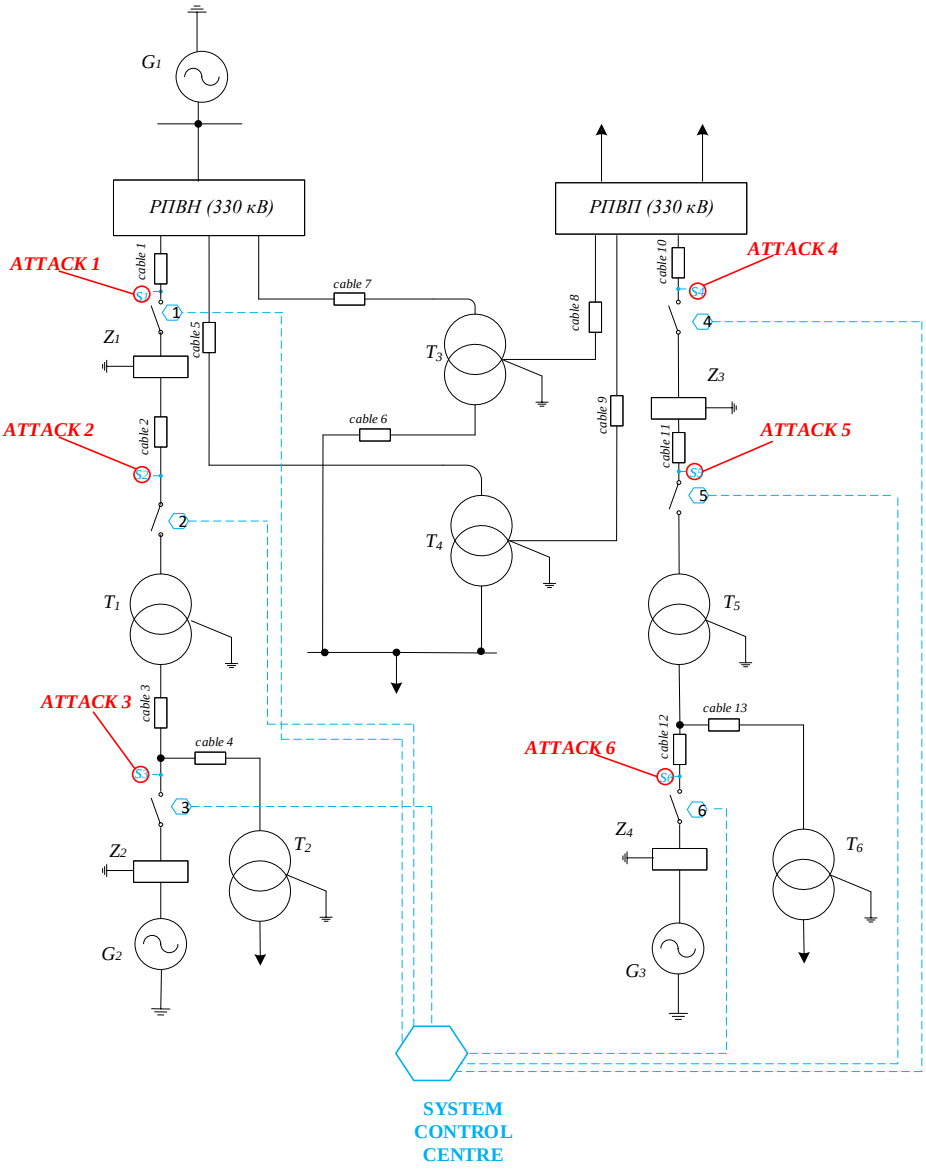


Рисунок 3.1 – Лінійна схема системи живлення ГЕС.

Центр управління сприймає інформацію на виходах генераторів $G_1$, $G_2$, $G_3$ позначених $s_1$, $s_3$, $s_6$ і на виходах кабелів 2, 10, 11 позначених $s_2$, $s_4$, $s_5$ відповідно. Ця інформація передається в центр управління, який використовує простий алгоритм відключення навантаження, щоб в ідеалі уникнути ситуації перевантаження, якщо навантаження перевищує генерацію. Якщо виміряна загальна потреба в навантаженні перевищує генерацію, то управління навантаженням скидає одне або обидва навантаження, щоб уникнути нестабільності, відкриваючи відповідні перемикачі за допомогою сигналів управління. Якщо виявлена інформація показує, що жодне навантаження не може обслуговуватися $G_1$, $G_2$ чи $G_3$ індивідуально, то обидва навантаження скидаються. Якщо виявляється, що може бути обслужений тільки один, то менше навантаження скидається за

умови, що $G_1$, $G_2$ чи $G_3$ може обслуговувати більше навантаження, в іншому випадку подається менше навантаження.

Кібератаки застосовується для розтину датчиків $s_1$, $s_2$, $s_3$, $s_4$ $s_5$, $s_6$, які дозволяють центрам управління приймати рішення по управлінню навантаженням. Типова кібератака може включати в себе фальсифікацію або підробку інформації про датчик, тому управління навантаженням припускає неправильне прийняття рішення. У такій ситуації навантаження скидаються, коли їх можна обслуговувати, або навантаження не падають, коли потреба перевищує генерацію, що призводить до зниження частоти генератора і, нарешті, відключення генератора.

На цьому етапі моделювання електричних та кібер-графів формуються так, що кожен вузол являє пов'язані елементи grid. У цьому поданні вузлами можуть бути генератори, трансформатори, навантажувальні або підключені гібриди, автоматичні вимикачі (електричні), перемикачі та центри управління, датчики і елементи управління виконавчими механізмами вимикача. З огляду на цю деталізацію деталей, ребра вибираються для того, щоб представляти залежності стану між різними компонентами.

Показаний граф, відповідний рисунку 3.1. На рисунку 3.2 електричні та кібер-графіки показані разом з ребрами, що представляють залежності між компонентами в тій же мережі або на кібер-фізичному мосту. Таким чином, існує вузол для кожного генератора, трансформатора, гібридного пристрою навантаження / підключення, автоматичного вимикача, перемикача, центру управління, датчика і виконавчого механізму. Спрямовані зв'язки існують між вузлами, якщо існує залежність від енергії або інформаційного потоку. Елементи grid відображаються на вузли на основі того факту, що можливо моделювати їх поведінку з використанням динамічних рівнянь. Вузли кібер-атак $A_1$, $A_2$, $A_3$, $A_4$, $A_5$, $A_6$ впливають на сигнали датчиків $s_1(t)$, $s_2(t)$, $s_{11}(t)$, $s_3(t)$, $s_4(t)$, $s_5(t)$, $s_6(t)$ на виходах кабелів 1, 2, 3, 10, 11, 12.

Кожен вузол має асоційований стан $x$ (що складається з відповідних системних напруг і струмів), регульований рівняннями динамічної системи, які моделюють фізику об'єкта (для випадку елементів енергосистеми) або функціональну або обчислювальну обробку (для випадку кібер-елементів).). Влучний вислів для $f$ залежить від ребер асоційованого вузла. Вузли можуть бути згруповані, щоб сформувати динамічні агенти для подання взаємодій в Smart Grid, як показано на рис. 3.2, на основі функціональності або для балансування порядку підсистеми.

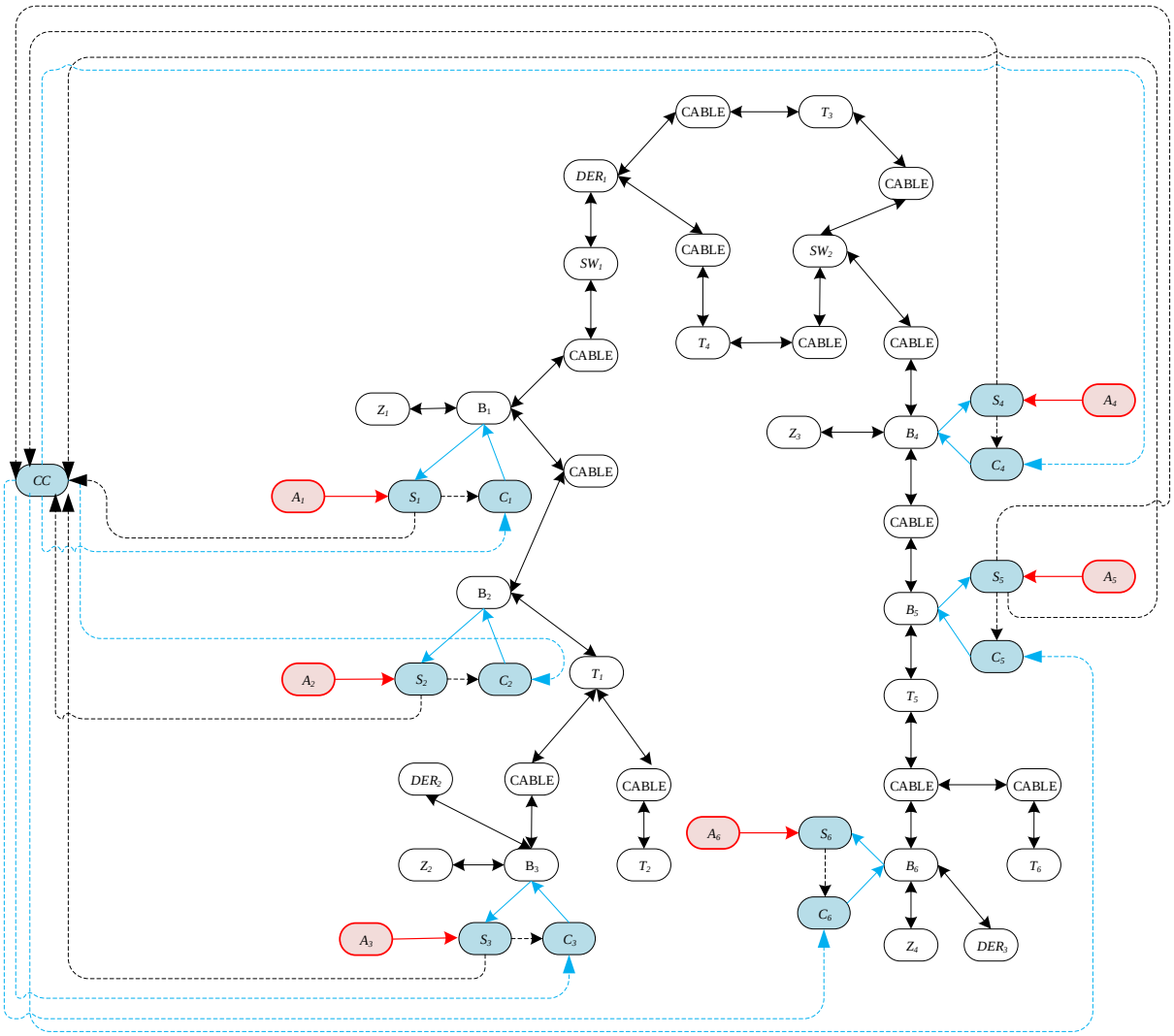


Рисунок 3.2 – Електричний і кібер-граф для системи з рис.3.1.

Вузли складаються з $DER_1$, $DER_2$, $DER_3$ - генераторів, автоматичних вимикачів $B_i$, кабелів, блоків $SW_i$, трансформаторів $T_i$ і акумуляторів / конденсаторів $Z_i$ електричної мережі та центру управління *cc*, датчиків $s_i$ і органів управління приводами кібер мережі. Графічний вузол «складовий кабель» представляє три фізичні кабеля, підключених до вузлів системи тестування розподілу вузлів. Краї представляють залежності стану для динамічного моделювання. Кібер-граф відрізняється заштрихованими вузлами і пунктирними краями. Атаки $A_1$, $A_2$, $A_3$, $A_4$, $A_5$, $A_6$ націлені на датчики $s_1$, $s_2$, $s_3$, $s_4$, $s_5$, $s_6$.

Для створення об'єктної моделі ГЕС заснованої на схемі 3.1, використовується мова моделювання кібербезпеки (CySeMoL), яку можна використовувати для оцінки кібербезпеки корпоративних архітектур [2]. Цей інструмент графа атак моделює архітектуру даної системи (служби, операційні системи, мережі, персонал і т. д.) І вказує задані характеристики (якщо в операційній системі включений брандмауер хоста і т. д.).

CySeMoL відображає як атаки і захист кількісно пов'язані між собою. Дана структура моделювання та механізму розрахунку призначена для оцінки кібербезпеки системних архітектур рівня підприємства.

P$^2$AMF є прогнозуючої, ймовірнісної структурою моделювання архітектури, яка призначена для того, щоб забезпечити моделювання і розрахунок уразливості системи-систем і визначити зв'язок атак і захистів. P2AMF є розширенням Object Constraint Language для ймовірнісної оцінки і прогнозування властивостей системи. P$^2$AMF здатна виражати невизначеності об'єктів, відносин і атрибутів в моделях уніфікованої мови моделювання (UML) і виконувати імовірнісні оцінки з урахуванням цих невизначеностей. P$^2$AMF було використано для створення моделі ГЕС для прогнозування доступності певного вузла при спробах несанкціонованих дій в системі.

У P$^2$AMF вводяться два види невизначеності.

По-перше, атрибути можуть бути стохастичними. Коли атрибути створюються, їх значення виражаються у вигляді імовірнісних розподілів. По-друге, існування об'єктів і відносин може бути невизначеним. Це може бути випадок, коли людина більше не знає, чи знаходиться конкретний вузол в роботі чи ні. Це випадок невизначеності існування об'єкта.

Імовірнісні аспекти розглядаються в режимі Монте-Карло: по-перше, користувач вказує бажану кількість вибірок. Після цього створюється набір об'єктних моделей, що відповідають обраному розміру вибірки. Стохастичні змінні моделі класів створюються зі значеннями примірників відповідно до їх відповідним призначеним розподілом. Це включає в себе існування класів і відносин, які створюються на частоті, яка відображається відповідними розподілами ймовірностей. Потім кожен оператор P2AMF перетворюється в правильний оператор OCL і може бути проаналізований аналізатором OCL. Після оцінки всіх зразків результати агрегируются і візуалізуються відповідно до дизайну моделі класу.

Основні активи даної архітектурної моделі, які зазнали атак, відображені в кібер-графі на рисунку 3.3. Він показує, які активи зображеної об'єктної моделі зловмисник має намір поставити під загрозу.

Вузли складаються з центру управління *cc*, датчиків $s_i$ і шаблонів *Operating System, Application Server, Web Application, Network Zone, SoftwareProduct, NetworkInterface*. Атаки $A_1, A_2, A_3, A_4, A_5, A_6$ націлені на датчики $s_1, s_2, s_3, s_4, s_5, s_6$.

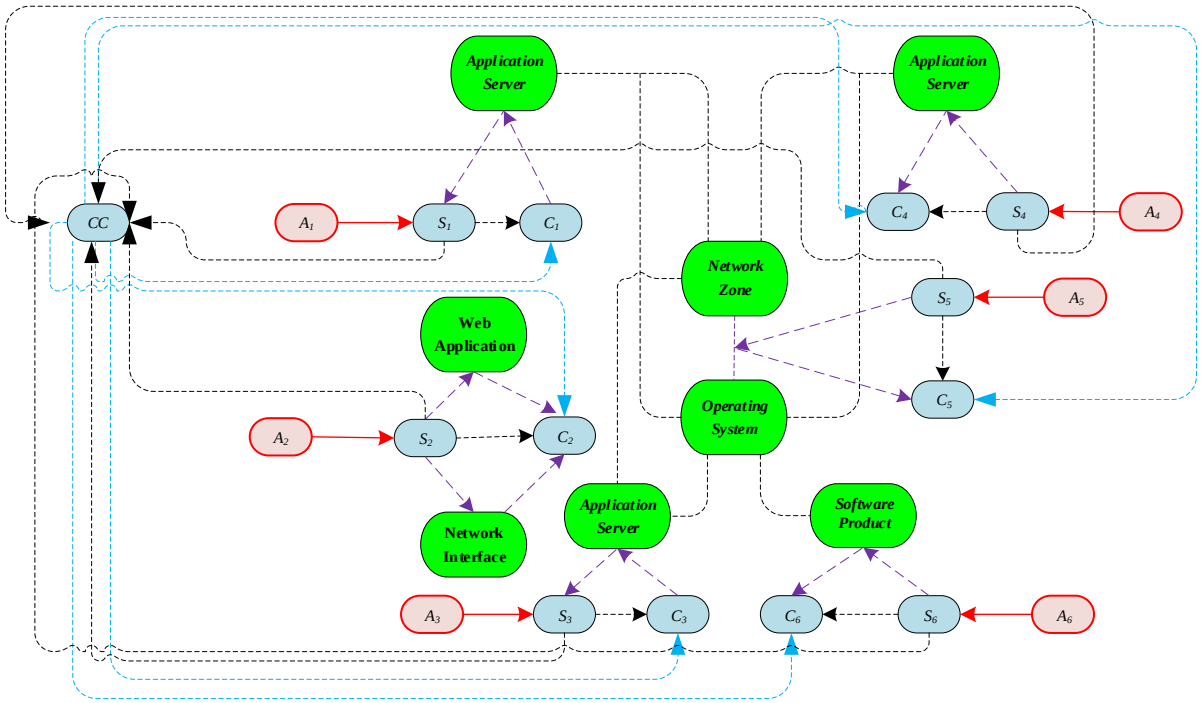


Рисунок 3.3. - Кібер-граф для системи з рис. 3.1.

### 3.4 Розробка моделі для аналізу кібербезпеки

Структура моделі створена в інструменті аналізу архітектури підприємства Object Modeler, який забезпечує зручну взаємодію для моделювання та аналізу, додаючи об'єкти і малюючи зв'язки між ними.

Коли розрахунки завершені, результати представляються користувачеві шляхом колірного кодування всіх шаблонів і кроків атаки за шкалою від 0%: зелений - 50%: жовтий - 100%: червоний. Тут ймовірність відноситься до ймовірності того, що один або кілька професійних тестерів проникнення успішно пройдуть етап атаки в об'єктної моделі за час, призначений для атаки. Ймовірності для шаблонів виводяться на основі оцінок кроків атаки, пов'язаних з ним, і обраного в даний момент колірного профілю.

На рис. 3.4 представлена модель ГЕС з можливими кроками атак і стан захисту системи, яка розроблена в середовищі CySeMoL [2].

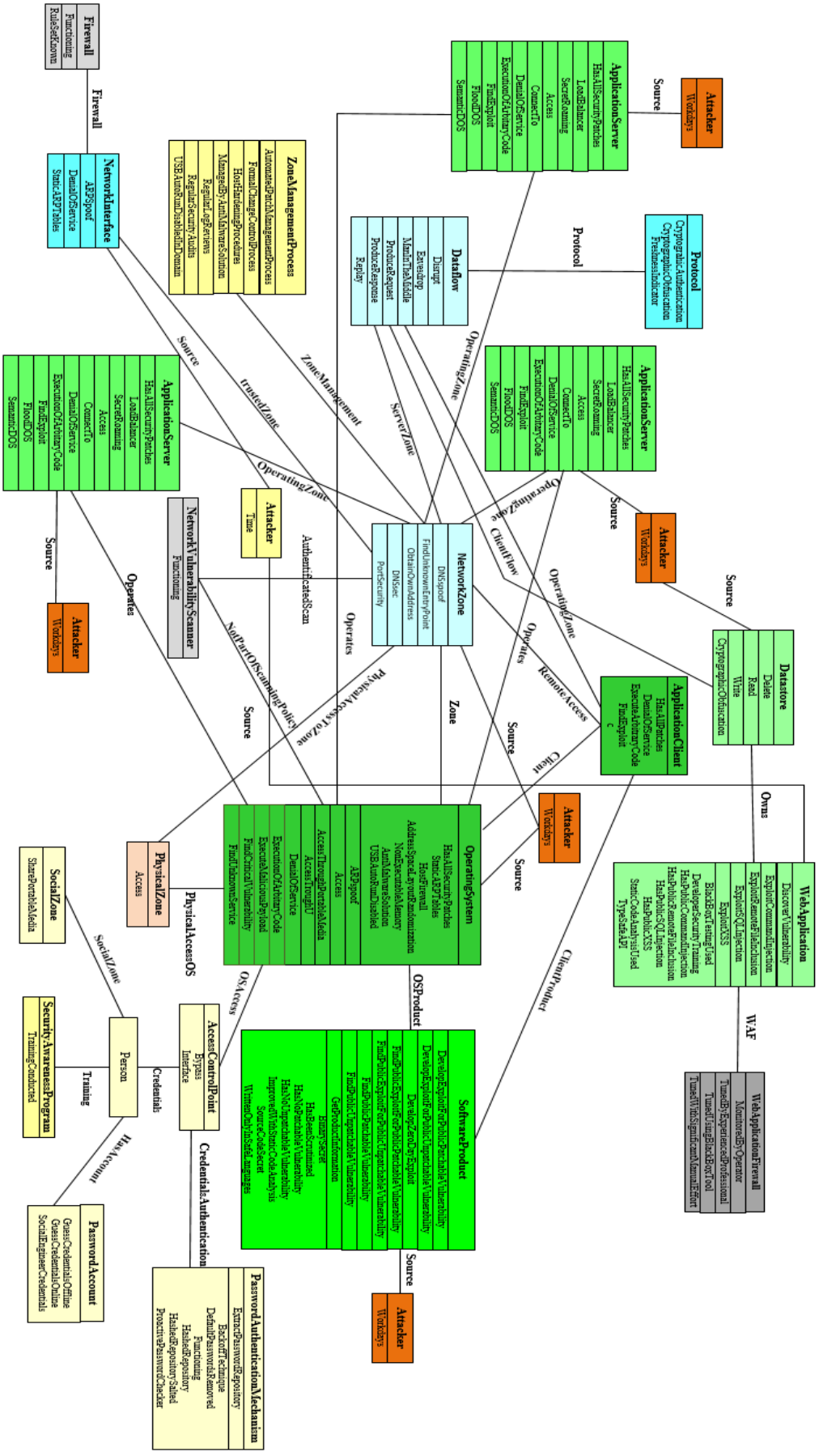


Рисунок 3.4 - Візуалізація моделі ГЕС класу CySeMoL до розрахунку

Для проведення розрахунків за ступенем серйозності уразливості спочатку було визначено параметри розрахунку моделі об'єкта.

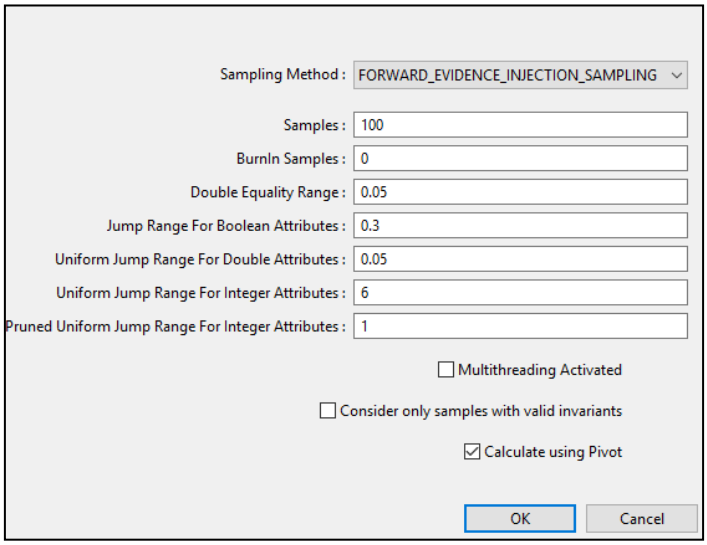


Рисунок 3.5 – Вікно конфігурації

У діалоговому вікні «Конфігурація», див. рис. 3.5, потрібно обрано метод вибірки, позначений як «FORWARD EVIDENCE INJECTION SAMPLING». Потім обрано кількість зразків, що відповідає часу і точності, необхідної для аналізу. Більша кількість зразків означає більш точні результати, але також і більше часу, необхідного для завершення розрахунку. Коли розрахунки завершені, результати представляються шляхом колірного кодування всіх шаблонів і кроків атаки за шкалою від 0%: зелений - 50%: жовтий - 100%: червоний. Тут ймовірність відноситься до ймовірності того, що один або кілька професійних тестерів проникнення успішно пройдуть етап атаки в об'єктної моделі за час, призначений для атаки.

Ймовірності для шаблонів виводяться на основі оцінок кроків атаки, пов'язаних з ним, і обраного в даний момент колірного профілю, див. рис. 3.6.

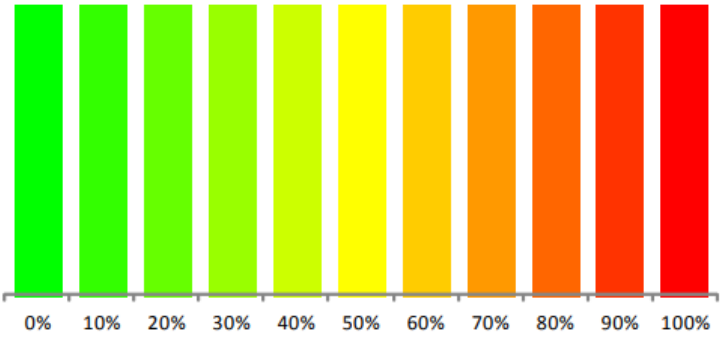


Рисунок 3.6 - Кольоровий профіль ймовірності етапів атаки

Зразковим колірним профілем є «Середнє», яке означає, що колір отриманий на основі середнього значення ймовірності для всіх відповідних етапів атаки. Іншим профілем є «Доступ», який розглядає тільки ті кроки атаки, які призводять до доступу активів (наприклад, операційної системи).

У CySeMoL існує 4 типи концепцій: Attacker, AttackStep, Defense і Asset. Кожен крок атаки і захисту пов'язаний з активом, який він ставить під загрозу або захищає. З'єднання між AttackSteps встановлюються автоматично в залежності від того, як підключили активи в об'єктної моделі, приклад показано на рисунку 3.7.

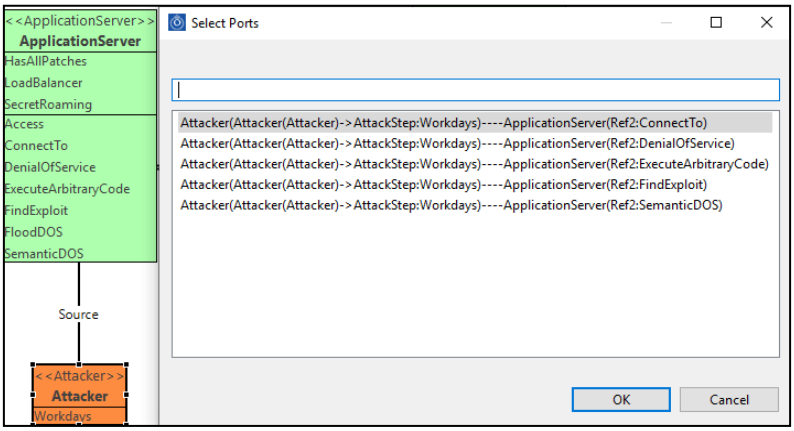


Рисунок 3.7 -Діалоговое вікно для вибору з'єднання

CySeMoL описує, як зловмисники можуть досягати різних кроків атаки в об'єктної моделі. Основною операцією Object Constraint Language для цієї мети є nextAttackWave, рекурсивна функція, яка намагається відвідати кожен AttackStep в об'єктної моделі (відвіданий масив відстежує ті, які були відвідані).

*Attacker*

Attacker може бути підключений до будь-якого класу, у якого є крок атаки. Підключення Attacker до етапу атаки в класі позначає вихідний вектор атаки. Цей конкретний крок атаки завжди оцінюється як TRUE, незалежно від властивостей об'єктної моделі.

Attacker має один атрибут - Час. Тут вказується, скільки робочих днів зловмисник повинен витратити на кожен крок атаки для об'єктної моделі. В обчислювальному відношенні ймовірність того, що кожен крок атаки в об'єктної моделі дорівнює TRUE, оцінюється щодо кількості робочих днів, зазначених для будь-яких змодельованих зловмисників. Приклад атакуючого зображено на рисунку 3.8.

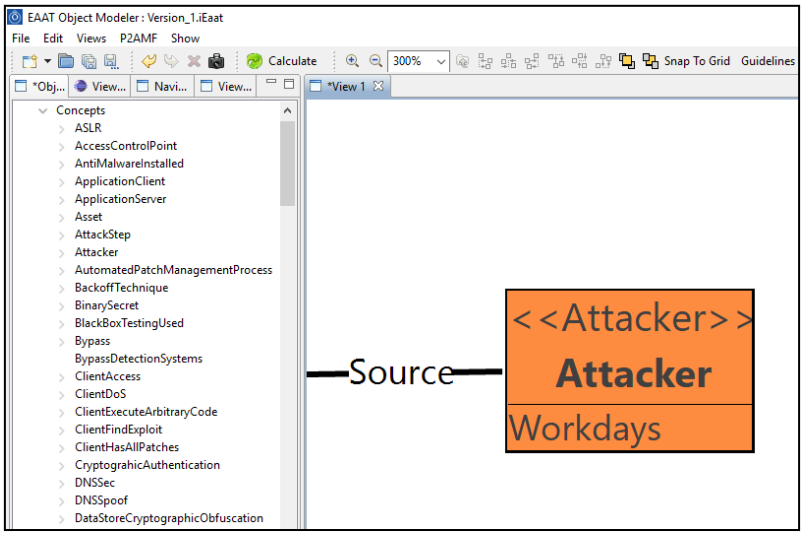


Рисунок 3.8 - Представлення атакуючого

*Operating System*

Operating System - це набір програмного забезпечення, який управляє апаратними ресурсами комп'ютера і надає загальні служби для комп'ютерних програм. У CySeMoL будь-яке додаткове програмне забезпечення для операційних систем, повинна бути представлена через класи ApplicationClient і ApplicationServer, і тільки «обов'язкова» базова функціональність (наприклад, реалізація стека TCP / IP) повинна розглядатися як частина класу OperatingSystem.

ApplicationClient або ApplicationServer повинен бути підключений до ОС, яка забезпечує його виконання. Тут ApplicationServer може діяти як термінал для своїх основних служб (наприклад, telnet, SSH, VNC або RDP) або надавати тільки специфічні для додатка функціональні можливості (наприклад, HTTP або FTP-сервер). ОС повинна бути підключена до SoftwareProduct.

Підключення до NetworkZone означає, що ОС має IP-адресу в цій мережі.

Підключення до PhysicalZone означає, що зловмисник має фізичний доступ до машини з ОС. AccessControlPoint описує засоби логічного доступу до вмісту ОС. DataStore - це база даних, розташована в ОС. ОС може бути захищена однією або декількома системами виявлення вторгнень (IDSSensors) або системами запобігання вторгнень (IPS). ОС може бути підключена до NetworkVulnerabilityScanner (наприклад, Nessus або Qualys Guard), що вказує або на те, що ОС аналізується за допомогою перевірки з перевіркою достовірності, перевірки без перевірки автентичності, або взагалі не використовується (остання використовується, коли NetworkZone є частиною політики сканування , але конкретної системи в зоні не повинно бути).

*HasAllSecurityPatches* вказує, чи реалізовані в системі всі виправлення безпеки програмного забезпечення. Стан захисту за замовчуванням вказується наступним чином:

Якщо ОС підключена до NetworkZone, яка, в свою чергу, підключена до ZoneManagementProcess, то стан за замовчуванням HasAllSecurityPatches залежить від стану ZoneManagementProcess.FormalPatchAndUpdatingProcess.

Якщо ОС або NetworkZone, підключена до ОС, підключена до NetworkVulnerabilityScanner (а ОС зображена як частина сканування), то стан захисту за замовчуванням залежить від типу сканування, яка призначена. ANS або UNS згідно з даними без аутентифікації. Якщо жоден з цих сценаріїв не застосовується, за замовчуванням стан HasAllSecurityPatches - FALSE.

*Static ARP Tables*

StaticARPTables включає в себе наявність в ОС статичних таблиць протоколу дозволу адрес (ARP). Таблиці ARP відображають логічні IP-адреси на фізичні MAC-адреси в широкомовному домені ОС. Стан за замовчуванням цього захисту - False.

*HostFirewall* дозволяє всі потоки даних з / в ОС і будь-яке на ній ПО, що використовується. Він служить для блокування служб, які невідомі моделюючому пристрою (OperatingSystem.FindUnknownService). Стан за замовчуванням цього захисту TRUE.

*Address Space Layout Randomization*

Мета AddressSpaceLayoutRandomization (ASLR) - ввести випадковість в адреси пам'яті, використовувані даним програмним модулем. Це призведе до того, що клас методів експлойта зазнає невдачі з вимірною ймовірністю, а також дозволить їх виявити, так як невдалі спроби, швидше за все, приведуть до аварійного завершення завдання атакуючого.

*Non Executable Memory*

NonExecutableMemory - це функція призначена для запобігання виконання додатком або службою коду з області нездійсненною пам'яті. Якщо в ОС реалізована і працює не виконуюча пам'ять, то ймовірність успіху для певного типу експлойтів повинна бути менше (атаки переповнення буфера). За замовчуванням цей захист має значення TRUE, так як більшість сучасних ОС і устаткування підтримують її.

*Anti Malware Solution*

AntiMalwareSolution - це програмне забезпечення, що використовується для запобігання, виявлення, видалення і повідомлення про шкідливі програми. Якщо ОС підключена до NetworkZone, яка, в свою чергу, підключена до ZoneManagementProcess і ZoneManagementProcess.ManagedByAntiMalwareSolution має значення TRUE, тоді стан AntiMalwareSolution за замовчуванням дорівнює TRUE, в інших випадках це False.

*USB AutoRun Disabled*

USB AutoRun Disabled автозапуску. Якщо він відключений, це збільшить складність поширення шкідливого ПЗ на основі USB.

OperatingSystem.Access позначає, чи може зловмисник керувати вмістом ОС як адміністратор. У CySeMoL є два способи виконати це: або діючий суб'єкт успішно виконує OperatingSystem.ExecuteMaliciousPayload, чи OperatingSystem.AccessThroughUI. Попереднє включає установку шкідливого ПО, яке забезпечує віддалений доступ до ОС. Останній включає обхід PasswordAuthenticationMechanism для AccessControlPoint ОС або ApplicationServer, який діє в якості терміналу для нього. Якщо який-небудь з цих кроків атаки має значення True, цей крок атаки має значення True, інакше, це False.

*Denial of Service* (Відмова в обслуговуванні)

Цей крок атаки групує всі атаки, спрямовані на ОС, і намагається викликати відмову в обслуговуванні (DoS). У CySeMoL, по суті, є два способи викликати DoS для ОС: або за допомогою OperatingSystem.Access, або з OperatingSystem. Execute Malicious Payload.

*Find Unknown Service* (Знайти невідомий сервіс)

Якщо зловмисник може знайти служби, невідомі адміністратору, що працюють на хості, можна атакувати їх, щоб отримати на них привілеї. Оскільки невідомі служби можуть мати більше дірок в безпеці, вони представляють собою серйозні проблеми безпеки. На OperatingSystem.FindUnknownService впливають три змінні:

– чи має ОС включену функцію HostFirewall (HF),

– чи виконали адміністратори мережі посилення захисту, наприклад, видалили непотрібні служби (ZoneManagementProcess.HostHardeningProcedures, HHP)

– чи визначали мережеві адміністратори формальний процес управління змінами (ZoneManagementProcess.FormalChangeManagementProcess, FCMP)

*Find Critical Vulnerability* (Знайти критичну уразливість)

На цьому етапі атаки з'ясовується, чи може зловмисник отримати критичну уразливість для бінарного сервісу, що працює в операційній системі. Щоб це було успішним, зловмисникові необхідно знайти невідомий сервіс в ОС (OperatingSystem.FindUnknownService) і використовувати цей сервіс. CySeMoL враховує п'ять різних способів отримання експлойта зловмисників (всі вони знаходяться в SoftwareProduct):

– FindPublicExploitForPatchableCritical Vulnerability - публічний експлойт може бути випущений для виправлення уразливості;

– DevelopExploitForPatchableCritical Vulnerability - зловмисник може розробити експлойт для виправлення уразливості;

– FindPublicExploitForUnpatchableCritical Vulnerability - публічний експлойт може бути випущений для уразливості, що не підлягає виправленню;

– DevelopExploitForUnpatchableCritical Vulnerability - зловмисник може розробити експлойт для уразливості, що не підлягає виправленню;

– DevelopZeroDayExploit - зловмисник може розробити експлойт для уразливості нульового дня, виявленої зловмисником.

Який тип експлойта є життєздатним, залежить від того, чи має ОС HasAllSecurityPatches чи ні.

*Execution of Arbitrary Code in Unknown Service* (Виконання довільного коду в невідомому сервісі)

Якщо зловмисник може знайти FindCriticalVulnerability, він може спробувати використовувати його для перенаправлення потоку управління програми на деякий код, обраний зловмисниками. Три ймовірності захисту впливають на ймовірність ExecutionOfArbitraryCodeinUnknownService:

– AddressSpaceLayoutRandomization (ASLR),

– NonExecutableMemory (NX)

– IntrusionPreventionSystems (IPS).

*Access Through Portable Media* (Доступ через портативні носії)

Ця змінна вказує на можливість отримання доступу до ОС за допомогою портативних носіїв. У CySeMoL AccessThroughPortableMedia має значення False, якщо USBAutoRunDisabled має значення True. Це також залежить від того, чи є користувач ОС частиною SocialZone з іншими користувачами, чиї комп'ютери були зламані, і можуть використовувати SharePortableMedia. Якщо немає, то цей крок атаки False.

*Access Through UI* (Доступ через призначений для користувача інтерфейс)

Цей крок атаки включає в себе, чи може зловмисник отримати доступ до ОС через деякий інтерфейс входу в неї. У CySeMoL цей крок атаки дорівнює TRUE, якщо зловмисник може фізично зв'язатися з машиною і обійти свій локальний механізм аутентифікації (PhysicalZone.Access = TRUE і ApplicationControlPoint.Bypass = TRUE) або зловмисник може обійти будь-який механізм віддаленого доступу в ОС.

*ARP spoof* (ARP оману)

Цей атрибут вказує, чи можна отруїти таблиці ARP в ОС. Якщо таблиці ARP ОС отруєні, це може бути використано для перехоплення трафіку, що йде із зовнішнього зони в одну з внутрішніх зон. Мережевий інтерфейс буде використовувати свої таблиці ARP, щоб визначити, з якого MAC-адресу повинен бути перенаправлений вхідний пакет IP. Якщо зловмисник може скомпрометувати таблицю ARP, агент загрози може змусити ці IP-пакети

потрапити на будь-який іншу MAC-адресу. Агент загрози може потім змінити дані, перш ніж пересилати їх за адресою, вказаною відправником. Статична таблиця ARP (StaticARPTables) є превентивним контрзаходом проти цього кроку атаки. Якщо цей захист True, ARPSpoof False. Якщо статичні таблиці ARP не функціонують, зловмисник може виконати цю атаку з будь-якої мережевої зони, через яку відповідний мережевий інтерфейс маршрутизує трафік (тобто це True).

*Execute Malicious Payload*

– Цей крок атаки стосується того, чи здатний агент загрози виконати будь-яке шкідливе ПЗ в системі. У CySeMoL це може бути досягнуто за допомогою восьми методів:

– ApplicationClient.ExecutionOfArbitraryCode - якщо в ОС є клієнтська програма, яка була скомпрометована в результаті успішного виконання довільного коду;

– WebApplication.ExploitCommandInjection - якщо в ОС є серверний додаток, на якому запущено веб-додаток, який було використано в результаті атаки Command Injection;

– WebApplication.ExploitRemoteFileInclusion - якщо в ОС є серверний додаток, на якому виконується веб-додаток, який було використано в результаті атаки з віддаленим включенням файлів;

– WebApplication.ExploitSQLInjection - якщо в ОС є серверний додаток, на якому виконується веб-додаток, який було використано при атаці SQL-ін'єкцією;

– OperatingSystem.ExecutionOfArbitraryCodeInUnknownServices – якщо можливо виконати довільний код у невідомому сервісі на ОС;

– ApplicationServer.ExecutionOfArbitraryCode (Terminal) - якщо в ОС є додаток сервера терміналів, який було скомпрометовано успішним виконанням довільного коду;

– ApplicationServer.ExecutionOfArbitraryCode ((Operates) - якщо в ОС є нетермінальних серверний додаток, який було скомпрометовано успішним виконанням довільного коду;

– OperatingSystem.AccessThroughPortableMedia - якщо можливо впровадити шкідливий код через переносний носій.

Якщо один або декілька з цих кроків атаки мають значення True, то існує ймовірність того, що ExecuteMaliciousPayload буде True, інакше це False. Крім того, ця ймовірність залежить від наявності або відсутності п'яти захистів:

IDS.Functioning (с отношением HIDS) - якщо операційна система має систему виявлення вторгнень, засновану на хості, що відстежує її;

IDS.Functioning (с отношением NIDS) - якщо в мережевий зоні, підключеної до ОС, є мережева система виявлення вторгнень (NIDS), що відслідковує її;

IDS.Updated - якщо HIDS і / або NIDS повністю оновлені;

IDS. Tuned - якщо HIDS і / або NIDS добре налаштовані;

OperatingSystem.AntiMalwareSolution - якщо в ОС встановлене антивірусне ПЗ.

***Application Client*** (Клієнт додатка)

ApplicationClient - це ПЗ або частина ПО, яке безпосередньо використовується кінцевими користувачами для виконання функцій певного типу. ПО для роботи з документами, таке як Adobe Reader, або ПО для веб-браузера, таке як Firefox. ApplicationClient повинен бути підключений до OperatingSystem, яка забезпечує його виконання.

З'єднання з NetworkZone означає, що клієнт є комбінованим клієнт-серверним рішенням, яким можна віддалено взаємодіяти, не маючи доступу до основних функцій ОС. AccessControlPoint описує засоби логічного доступу до вмісту клієнта. Клієнт може бути захищений однією або декількома системами запобігання вторгнень (IPS).

*HasAllSecurityPatches* вказує, чи реалізовані на клієнті всі застосовані програмні виправлення безпеки.

Доступ означає, чи може зловмисник управляти контентом клієнта в якості його адміністратора. У CySeMoL для успіху цієї атаки зловмисник повинен обійти функцію входу клієнта (AccessControlPoint.Bypass). Необхідно, щоб зловмисник міг підключитися до самого клієнта. У CySeMoL це може бути досягнуто через доступ до ОС, яку виконує клієнт (OperatingSystem.Access), або якщо клієнт підключений до NetworkZone,.

*Denial Of Service* (Відмова в обслуговуванні)

Цей крок атаки групує всі атаки, спрямовані на сервер, і намагається викликати відмову в обслуговуванні (DoS). У CySeMoL це може бути виконано зловмисниками, які мають доступ до ОС, на якій розміщений клієнт.

*Find Critical Vulnerability* (Знайти критичну уразливість)

Цей крок атаки включає в себе можливість атакуючому отримати критичну уразливість для клієнта. Щоб це було успішним, зловмисникові необхідно мати можливість взаємодіяти з клієнтом (OperatingSystem.Access або якщо клієнт підключений до NetworkZone і знайти експлойт для клієнта.

*Execution Of Arbitrary Code* (Виконання довільного коду)

Якщо зловмисник може знайти FindCriticalVulnerability, він може спробувати використовувати його для перенаправлення потоку управління програми на деякий код, обраний зловмисниками.

***Application Server*** (Сервер додатків)

ApplicationServer - це ПЗ або частина ПО, яке відповідає на віддалені запити програмних клієнтів. Залежно від типу цього з'єднання сервер або діє як термінал для доступу до основних функціональних можливостях ОС, або як сервер, який просто працює з використанням ОС, щоб дозволити його виконання.

*Connect To* Server цей етап атаки стосується можливості підключення зловмисника до програмного забезпечення сервера. У CySeMoL це можливо, якщо зловмисник може досягти потоку даних, мережевий зони або ОС, до якої підключений сервер.

Access це означає, чи може зловмисник керувати вмістом сервера в якості адміністратора. У CySeMoL це може бути досягнуто шляхом обходу функції входу на сервер (AccessControlPoint.Bypass). Також необхідно, щоб зловмисник міг підключитися до самого сервера (ConnectToServer).

Відмова в обслуговуванні групує всі атаки, спрямовані на сервер, і намагається викликати відмову в обслуговуванні (DoS). У CySeMoL досить, щоб зловмисник зміг успішно виконати крок атаки ConnectToServer. Це було виявлено в ході опитування, що включає оцінку значущості змінних, які зазвичай включені до DoS серверного програмного забезпечення.

***Software Product***

SoftwareProduct є ПО, яке ще не було змінено чи оновлено за допомогою виправлень.

*Source Code Secret*

Якщо зловмисник отримує доступ до вихідного коду програмного продукту, його можна знайти в «білому ящику» і перевірити його на наявність вразливостей. Деякі програми з відкритим вихідним кодом, в цьому випадку легко отримати вихідний код. Інше ПЗ є закритим, тоді отримати вихідний код складніше. CySeMoL не розкладає кроки, які можуть бути зроблені для отримання вихідного коду продукту, проте це може бути введено.

*Binary Secret*

Якщо зловмисник має доступ до двійкового коду (машинного коду), можна провести тести «чорного ящика» і тим самим виявити вразливості. Якщо зловмисник не зможе отримати цей код, буде практично неможливо знайти нову уразливість в цьому ПО.

*Improved With Static Code Analysis*

Статичний аналізатор коду - це інструмент, який перевіряє вихідний код програмного забезпечення на наявність помилок або вразливостей в ньому.

*Written Only In Safe Languages*

Якщо була використана «безпечна» мова програмування, така як Java або Python, що виконує перевірку кордонів, тоді можливості виконання переповнення буфера зменшуються і з'являється можливість виявлення уразливості. Якщо використовується

«небезпечна» мова, така як C або C ++, ймовірність виявлення уразливості вище. Однак використання безпечного діалекту цих мов можливо, наприклад, Cyclone. Використання безпечних бібліотек для вбудовування небезпечного коду також включено в це визначення.

*Has Been Scrutinized*

Деякі програмні продукти були ретельно вивчені. Тобто вони були ретельно перевірені на уразливості. Дослідження показали, що частота виявлення вразливостей в програмних продуктах з часом зменшується.

*Has No Public Patchable Vulnerability*

Це відноситься до сценарію, в якому відомо, що в ПО немає доступних для виправлення вразливостей на відкритих форумах, таких як NVD, PacketStorm або Exploit DB.

*Has No Public Unpatchable Vulnerability*

Це стосується сценарію, в якому відомо, що в ПО немає недоступної для виправлення уразливості, доступної на будь-яких загальнодоступних форумах, таких як Національна база даних вразливостей (NVD), PacketStorm або Exploit DB.

*Get Product Information*

Цей крок атаки стосується того, чи може зловмисник успішно перевірити ПО, щоб визначити його властивості .Щоб досягти цього кроку атаки, зловмисникові необхідно:

– ApplicationClient.ProduceResponse - провести відповідь від клієнтського програмного забезпечення, підключеного до продукту.

– ApplicationServer.ConnectTo - підключити до сервера програмне забезпечення, підключеного до продукту.

– OperatingSystem.FindUnknownService - знайти невідоме програмне забезпечення в ОС, підключене до продукту.

*Find Public Patchable Critical Vulnerability*

Цей крок атаки стосується того, чи може зловмисник знайти виправлену критичну уразливість в будь-якому загальнодоступному домені. Щоб досягти цього кроку атаки, необхідно, щоб відповідна GetProductInformation була True.

*Find Public Unpatchable Critical Vulnerability*

Цей крок атаки стосується того, чи може зловмисник знайти виправлену критичну уразливість в будь-якому загальнодоступному домені. Щоб досягти цього кроку атаки, необхідно, щоб відповідна GetProductInformation була TRUE.

*Find Public Exploit For Patchable Critical Vulnerability*

Цей крок атаки стосується того, чи може зловмисник знайти експлойт для виправленої критичної уразливості в будь-якому загальнодоступному домені. Щоб досягти

цього кроку атаки, необхідно, щоб FindPublicUnpatchableVulnerability або FindPublicPatchableVulnerability були True. Таким чином, уразливість, яку не можна було виправити при її розкритті, може бути виправлена до публічного випуску експлойта. Якщо обидва вони False, то цей крок атаки False. Якщо один або обидва значення True, то ймовірність успіху залежить від того, чи є цільове ПО ОС чи ні.

*Develop Exploit For Patchable Critical Vulnerability*

Якщо вразливість виявлена, але експлойт не доступний, то досвідчений зловмисник може використовувати оприлюднену інформацію про цю уразливість і самостійно розробити для неї експлойт. Щоб досягти цього кроку атаки, по-перше, необхідно, щоб FindPublicPatchableVulnerability була True. Якщо True, то ймовірність успіху залежить від того, чи доступний вихідний код програми або патча для зловмисника (SourceCodeClosed). Наявність вихідного коду може допомогти зловмисникові виявити «глибокі» уразливості, які важко знайти за допомогою відладчика, однак він також може допомогти захисникам швидко усунути недоліки.

*Find Public Exploit For Unpatchable Critical Vulnerability*

Цей крок атаки стосується того, чи може зловмисник знайти експлойт для виправленої критичної уразливості в будь-якому загальнодоступному домені.

*Develop Exploit For Unpatchable Critical Vulnerability*

Якщо розкрита вразливість виявлена, але експлойт не доступний, то досвідчений зловмисник може використовувати оприлюднену інформацію про уразливість і самостійно розробити для неї експлойт.

Відмінність від кроку атаки DevelopExploitForPatchableCriticalVulnerability полягає в тому, що даний стосується вразливості, для якої немає випущеного виправлення програмного забезпечення, що пом'якшує його.

*Develop Zero Day Exploit*

Якщо немає доступної розкритої вразливості або зловмисник хоче використовувати щось, що невідомо, щоб бути уразливим в загальнодоступному домені, то він може спробувати виявити нову уразливість (часто звану нульовим днем).

В результаті моделювання системи захисту і можливих атак були виявлені і передбачені наслідки, які  ефективно допомагають керувати кібербезпекою своєї системи. Недостатньо усунути всі вразливості в системі - також необхідно зрозуміти, як ці уразливості пов'язані. Таким чином, особи, які приймають рішення на підприємстві, мають потребу в інструментах, які можуть допомогти в простій і зрозумілій оцінці кібербезпеки їх системи.

На рис. 3.9 представлена модель ГЕС з можливими кроками атак і стан захисту системи після розрахунку.

Наприклад, як видно на рисунку, кроки атаки Access, Denial of Servise, ExecuteArbitraryCode, FloodDOS, SemanticDOS на яких зловмисник може керувати вмістом сервера в якості адміністратора або викликати відмову в обслуговуванні, з імовірністю приблизно 81% при самих базових умовах об'єктної моделі.

Семантична різниця впливає на різні кроки атаки в CySeMoL. Наприклад, якщо IDSensor підключений до мережевого інтерфейсу, він перевірить трафік, що переходить від відповідних ненадійних зон до довірених зон, але не навпаки.

Приклад гістограми  для ApplicationServer представлено на рисунку 3.10.

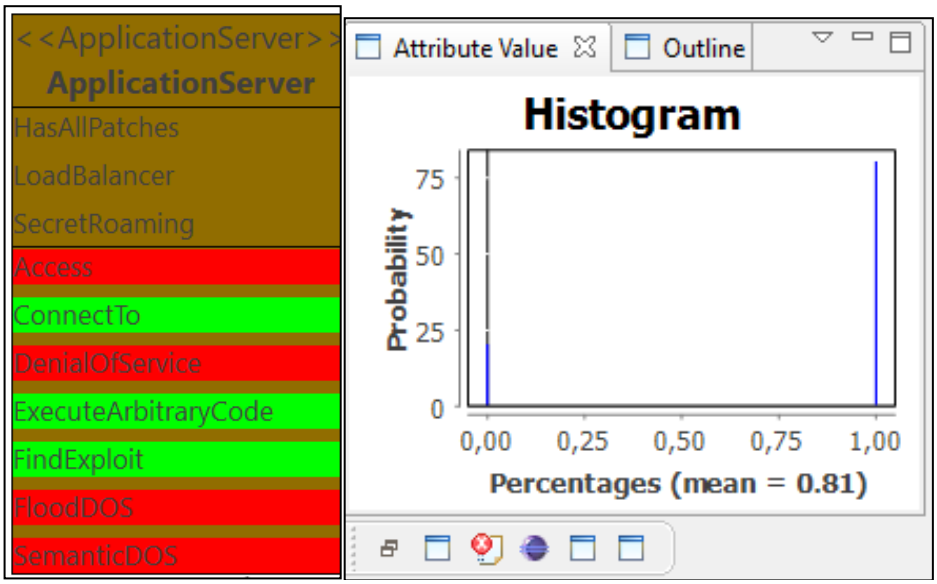


Рисунок 3.10 – Приклад гістограми об’єкта ApplicationServer

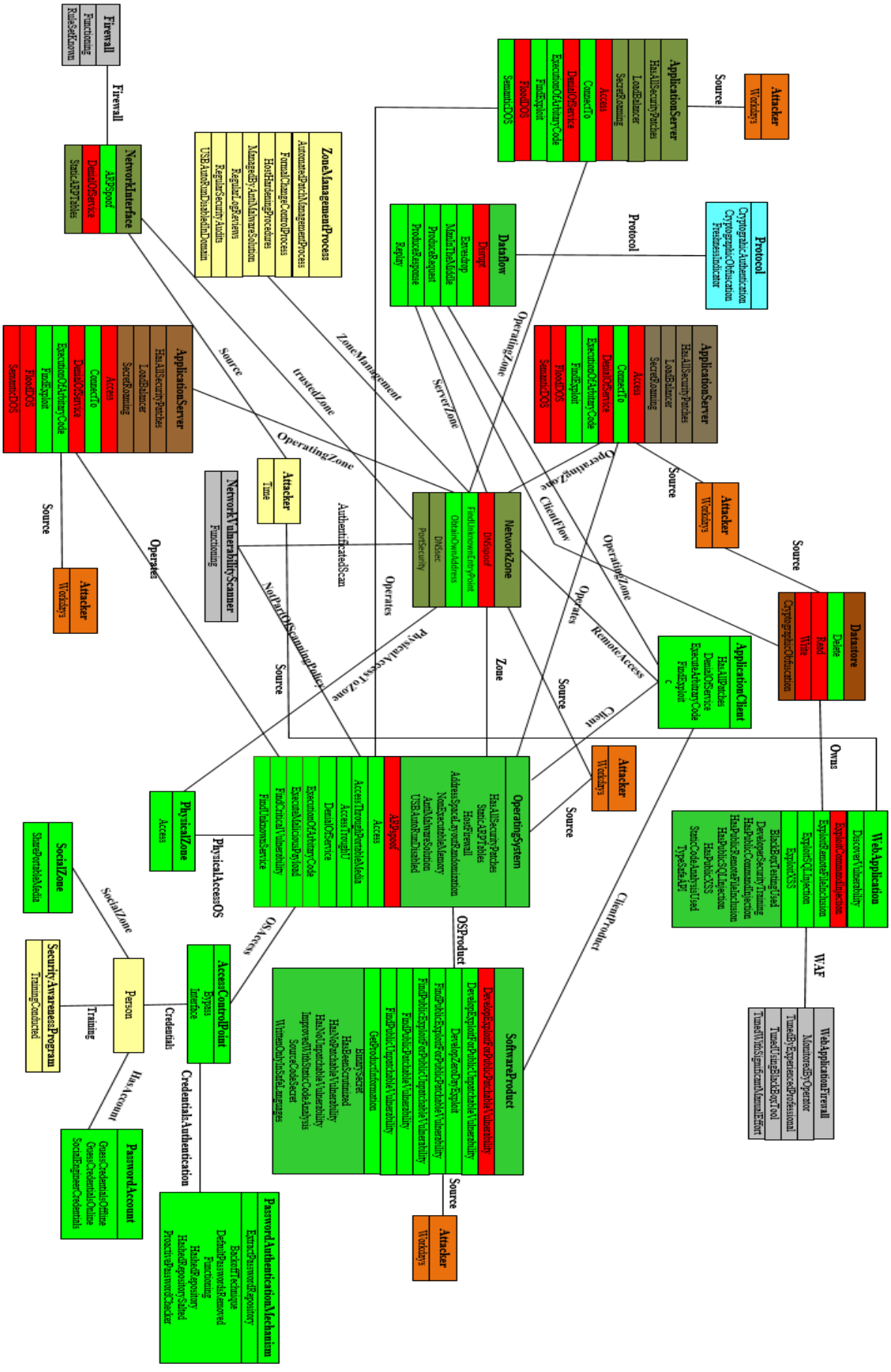


Рисунок 3.9 - Візуалізація моделі ГЕС класу CySeMoL після розрахунку

### 3.5 Висновки до розділу 3

Представлено етап синтезу моделі на основі графів в якому були використані динамічні системи для систематичного моделювання кібер і електричних мереж.

Побудовано лінійна схема системи живлення ГЕС, електричний граф і кіберграф.

В результаті розробленої моделі, що включає взаємодію об'єктів і атак був використаний інструмент аналізу архітектури підприємства Object Modeler, який використовується для побудови графіків атак і обчислення оцінок уразливості.

Використовуваний програмний інструмент Object Modeler на мові моделювання CySeMoL показав розрахунки і прогнози, які застерігають від атак зловмисників та визначають можливі вразливості.

Досліджено можливі кроки атак і їх властивості, впливаючи на систему.

### 3.6 Перелік посилань до розділу 3

1. D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos and K.L. Butler-Purry «Towards modelling the impact of cyber-attacks on a smart grid», 2011;

2. Hannes Holm, Mathias Ekstedt, Teodor Sommestad, Matus Korman «A Manual for the Cyber Security Modeling Language», 2013;

3. Методичні вказівки до виконання та захисту магістерської роботи за спеціальностями 122 "Комп'ютерні науки та інформаційні технології" (8.05010101 “Інформаційні управляючі системи та технології (за галузями)”, 8.05010102 “Інформаційні технології проектування”), 123 "Комп'ютерна інженерія" (8.05010201 "Комп'ютерні системи та мережі", 8.05010202 "Системне програмування") (для студентів денної та заочної форм навчання) / Уклад.: Скарга-Бандурова І.С., Рязанцев О.І., Барбарук В.М., Щербакова М.Є. – Сєвєродонецьк: Вид-во СНУ ім. В. Даля, 2016. – 80 с.

# РОЗДІЛ 4
# ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було використання інформаційних технологій для аналізу методів забезпечення кібербезпеки електроенергетичних мереж, оцінки ризиків вразливостей системи, прогнозування ймовірної структури моделювання архітектури, і як результат було розроблено математичну модель. За цією моделлю в подальшому розроблятиметься реальна система, яка значно полегшить процес виявлення вразливостей системи під час атак та запобігання їх в майбутньому. Так як в процесі проектування використовувалося ПК, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде використовуватися розроблена об'єктна модель для оцінки ризиків та аналізу кібербезпеки під час атак, розрахунку вразливостей системи, визначення зв'язків атак і захистів та прогнозування властивостей системи.

## 4.1 Загальні питання з охорони праці

В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу.

На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці.

### 4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Обов'язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені у [1].

### 4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [2].

Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [3].

## 4.2 Аналіз стану умов праці

Робота над створенням об’єктної моделі забезпечення оцінки кібербезпеки, розрахунок уразливості системи і визначення зв'язків атак і захистів проходитиме в побутовому приміщенні. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

### 4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 - Розміри приміщення

| **Найменування** | **Значення** |
|---|---|
| Довжина, м | 3 |
| Ширина, м | 3 |
| Висота, м | 2,5 |
| Площа, $м^2$ | 9 |
| Об'єм, $м^3$ | 22,5 |

Згідно з [4] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для зручності спільної роботи з іншими працівниками (обговорення ідей, з'ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов'язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог

пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

### 4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [5] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

| Найменування параметра | Фактичне значення | Нормативне значення |
|---|---|---|
| Висота робочої поверхні, мм | 750 | 680 ÷800 |
| Висота простору для ніг, мм | 730 | не менше 600 |
| Ширина простору для ніг, мм | 660 | не менше 500 |
| Глибина простору для ніг, мм | 700 | не менше 650 |
| Висота поверхні сидіння, мм | 470 | 400 ÷500 |
| Ширина сидіння, мм | 400 | не менше 400 |
| Глибина сидіння, мм | 400 | не менше 400 |
| Висота поверхні спинки, мм | 600 | не менше 300 |
| Ширина опорної поверхні спинки, мм | 500 | не менше 380 |
| Радіус кривини спинки в горизонтальній площині, мм | 400 | 400 |
| Відстань від очей до екрану дисплея, мм | 800 | 700 ÷800 |

### 4.2.3 Навантаження та напруженість процесу праці

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном,

не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи на ведені в [5].

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- для операторів персональних комп’ютерів тривалістю 15 хв через дві години роботи;

### 4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

#### 4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОМ з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання [6], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп'ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є:

– робоча напруга U=+220В +-5%;

– робочий струм I=2А;

– споживана потужність P=350 Вт.

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [5].

За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами, шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 - Аналіз небезпечних і шкідливих виробничих факторів

| Небезпечні і шкідливі виробничі фактори | Джерела факторів (види робіт) | Кількісна оцінка | Нормативні документи |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |
| - підвищена температура поверхонь обладнання | експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи | 2 | ДСН 3.3.6.042-99 [4] |
| - підвищений рівень шуму на робочому місці | -//- | 2 | ДСН 3.3.6.042-99 [4] |
| - підвищена або знижена вологість повітря | -//- | 2 | ДСН 3.3.6.042-99 [4] |
| - підвищена або знижена рухливість повітря | -//- | 1 | ДСН 3.3.6.042-99 [4] |
| - підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини | -//- | 4 | ГОСТ 12.1.030-81 [7]<br>ГОСТ 13109-97 [8] |

Продовження таблиці 4.3

| | | | |
|---|---|---|---|
| - недостатність природного світла | порушення умов праці (вимог до приміщень) | 2 | ДБН В.2.5-28:2015 [9] |
| - недостатнє освітлення робочої зони | порушення гігієнічних параметрів виробничого середовища | 3 | ДБН В.2.5-28:2015 [9] |
| - підвищена яскравість світла | порушення умов праці (організації місця праці - налагодження моніторів) | 1 | ДСанПіН 3.3.2.007-98[5] |
| - понижена контрастність | -//- | 1 | ДСанПіН 3.3.2.007-98[5] |
| | | | |
| - нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових) | - пошук інформації для постановки теми;<br>- пошук та аналіз аналогів і літератури;<br>- пошук наявних технологій, моделювання та аналіз алгоритмів;<br>- виконання роботи за темою диплома, тестування;<br>- оформлення роботи | 4 | НПАОП 0.00-1.28-10[6]<br>ДСанПіН 3.3.2.007-98[5] |
| - фізичні (статичне – сидіння) | порушення умов праці (організації місця праці - сидіння користувача, ) та організації робочого часу - безперервна робота) | 2 | НПАОП 0.00-1.28-10[6]<br>ДСанПіН 3.3.2.007-98[5] |

### 4.3.2 Пожежна безпека

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), надійно захищені діелектричними щитками та/або сітками з метою недопущення потрапляння працівника під напругу.

В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,

2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Згідно [10] таке приміщення, площею 9 м$^2$, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт.;
- повсть 1 1 м$^2$, кошму 2×1,5 м$^2$ або азбестове полотно 2×2 м$^2$ в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

### 4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення

обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

## 4.4 Гігієнічні вимоги до параметрів виробничого середовища

### 4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [11] і наведені в табл. 4.4:

Таблиця 4.4 - Норми мікроклімату робочої зони об'єкту

| **Період року** | **Категорія робіт** | **Температура $C^0$** | **Відносна вологість %** | **Швидкість руху повітря, м/с** |
|---|---|---|---|---|
| Холодна | легка-1 а | 22 - 24 | 40 – 60 | 0,1 |
| Тепла | легка-1 а | 23 - 25 | 40 – 60 | 0,1 |

### 4.4.2 Освітлення

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

*Розрахунок освітлення.*

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n , \quad (4.1)$$

де $S_b$ – площа віконних прорізів, м$^2$;

$S_n$ – площа підлоги, м$^2$.

$S_n = a \cdot b = 3 \cdot 3 = 9$ м$^2$,

$S_{вік} = 1/10 \cdot 9 = 0{,}9$ м$^2$.

Приймаємо 2 вікна площею $S = 0{,}9$ м$^2$ кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \quad (4.2)$$

де $E$ – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

$S$ – освітлювана площа, м$^2$; S = 9 м$^2$;

$Z$ – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ;

$Z$ = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

$K$ – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

$U$ – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

$M$ – число люмінесцентних ламп в світильнику – 2;

$F$ – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \times 9 \times 1.1 \times 1.5}{5400 \times 0.575 \times 2} = 0{,}7 \approx 1$$

Приймаємо освітлювальну установку, яка складається з 1 світильника, який складається з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

### 4.5 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40 м$^3$ на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

### 4.6 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

**Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).**

Загальний опір захисного заземлення визначається за формулою:

$$R_{ççï} = \frac{R_ç \cdot R_n}{R_n \cdot n \cdot \eta_ç + R_ç \cdot \eta_n} \quad (4.3)$$

де $R_з$ - опір заземлення, якими можуть бути труби, опори, кути і т.п., Ом;

$R_n$ - опір опори, яка з'єднує заземлювачі, Ом;

n - кількість заземлювачів;

$\eta_з$ - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; $\eta_з = 0,7$

$\eta_n$ - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; $\eta_n = 0,5$;

Опір заземлення визначається за формулою:

$$R_ç = \frac{\rho}{2\pi \cdot l}\left(\ln\frac{2 \cdot l}{d} + \frac{1}{2}\ln\frac{4 \cdot t + l}{4 \cdot t - l}\right) \quad (4.4)$$

де ρ - питомий опір ґрунту, залежить від типу грунту, Ом·м;

для піску - 400 ÷ 700 Ом·м; приймаємо ρ = 400 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3}\left(\ln\frac{2 \cdot 3}{0{,}05} + \frac{1}{2}\ln\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right) = 110, \text{ Ом}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_n = \frac{\rho}{2\pi \cdot L} \cdot \ln\frac{2 \cdot L^2}{b \cdot t_l} \quad (4.5)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

$t_1$ - глибина заземлення від рівня землі, м; $t_1 = 0,5$ м.

$$R_n = \frac{400}{2 \cdot 3{,}14 \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0{,}03 \cdot 0{,}5} = 5{,}99, \text{ Ом}$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_ç}{4 \cdot \eta_ç} = \frac{2 \cdot 110}{4 \cdot 0{,}7} = 79 \text{ øò} \qquad (4.6)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5{,}99}{5{,}99 \cdot 79 \cdot 0{,}7 + 110 \cdot 0{,}5} = 1{,}7, \text{ Ом}$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

### 4.7 Охорона навколишнього природного середовища

#### 4.7.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, а саме: Методи забезпечення кібербезпеки систем релейного захисту та автоматики в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища», Законом України «Про забезпечення санітарного та епідемічного благополуччя населення», Законом України «Про відходи», Законом України «Про охорону атмосферного повітря», Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», Водний кодекс України.

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які

утворюються, збираються, розміщуються, передаються на видалення (знешкодження), утилізацію, тощо в ІТ галузі.

В процесі діяльності розробника об’єктної моделі за допомогою ПК виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

Відпрацьовані люмінесцентні лампи - І клас небезпеки

Акумулятор для джерел безперебійного харчування -ІІІ клас небезпеки

Змінні носії інформації - IV клас небезпеки

Макулатура - IV клас небезпеки

Побутові відходи - IV клас небезпеки

### 4.7.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Наводяться вимоги зберігання виявлених за своєю роботою відходів відповідно до вимог [12].

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

- Відходи І класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

- Відходи ІІ класу небезпеки в залежності від агрегатного стану зберігаються в поліети-ленових мішках, бочках, сховищах та інших видах тари, яка запобігає поширенню шкідливих речовин;

- Відходи ІІІ класу небезпеки зберігаються в тарі, яка забезпечує локалізацію зберігання, дозволяє виконувати вантажно-розвантажувальні і транспортні роботи і виключає поширення в ОС шкідливих речовин;

- Відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і до-ставляють на місце утилізації або захоронення;

### 4.7.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишне середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України «Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються та наводяться у таблиці 4.5.

Таблиця 4.5 - Відомості про місце утворення та місце розташування відходів

| № з/п | Код та найменування відходів за ДК -005-96 | Технологічний процес або виробництво, де утворюються відходи / клас небезпеки | Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху) |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | 7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані (Відпрацьовані ртутьвмісні люмінесцентні лампи) | 1 | буд.78, кв. 63 |
| 2 | 7710.3.1.01 Макулатура паперова та картонна (Макулатура) | | буд.78, кв. 63 |
| 3 | Акумулятор для джерел безперебійного живлення | 3 | буд.78, кв. 63 |

### 4.8 Висновки до розділу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Були наведені розміри приміщення та значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри,

значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп'ютері.

А також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

### 4.9 Перелік посилань до розділу 4

1. НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві»

2. НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»

3. НАПБ Б.02.005-2003 «Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України»

4. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»

5. ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»

6. НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин»

7. ГОСТ 12.1.030-81 «ССБТ. Електробезпечність .Захисне заземлення. Занулення»

8. ГОСТ 13109-97 «Електрична енергія. Сумісність технічних засобів вієлектромагнітних. Норми якості електроенергопостачання загального призначення »

9. ДБН В.2.5-28:2015 «Природнє і штучне освітлення»

10. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою»

11. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»

12. ДСанПіН 2.2.7.029 «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення».

# ВИСНОВОК

Представлено структуру аналізу впливу, де увага сфокусована на етапі синтезу моделі, де кібер-фізичні, так і фізичні взаємозв'язки об'єктів grid моделюються як орієнтовані графи. Кожен вузол графа має асоційовану інформацію про стан, який регулюється рівняннями динамічної системи, які моделюють фізику взаємодії (для компонентів електричної мережі) або функціональність.

Основною вимогою для системи захисту є те, що вона може надійно виявляти будь-які несправності в зоні захисту. Захист і надійність захисту завжди є первинними вимогами поряд зі швидкістю, вибірковістю. Масивність Smart Grid і розширені можливості зв'язку роблять її більш схильною до кібератаки. Оскільки інтелектуальна мережа вважається важливою інфраструктурою, всі уразливості повинні бути ідентифіковані і повинні бути реалізовані достатні рішення для зниження ризиків до прийнятного рівня безпеки.

Інтелектуальна мережа вимагає комплексних рішень для кібербезпеки. Необхідна комунікаційна архітектура із захистом, вбудованою з самого початку. Інтелектуальне рішення для забезпечення безпеки мереж вимагає цілісного підходу, включаючи традиційні схеми, довірені обчислювальні елементи, механізми аутентифікації на основі галузевих стандартів. Тому для забезпечення інфраструктури інтелектуальних мереж зв'язку буде потрібно використання сучасних протоколів безпеки на основі стандартів. Щоб досягти поставленої мети, необхідно вжити декілька кроків: оптимізації для забезпечення максимальної надійності, доступності, ефективності та економічних показників, доступності, яка надає доступ до мережі для всіх користувачів мережі, особливо для поновлюваних джерел енергії і високоефективної місцевої генерації з нульовими або низькими викидами вуглецю, надійності, що забезпечує і поліпшує безпеку і якість поставок, відповідає вимогам епохи цифрових технологій зі стійкістю до небезпек і невизначеності

В результаті проведеного аналізу була побудована модель прогнозування імовірнісних атак на архітектуру підприємства. Ймовірності для шаблонів (активів) виводяться на основі оцінок кроків атаки, пов'язаних з ним, і обраного в даний момент колірного профілю.

Основною метою магістерської роботи було дослідження вразливостей Smart Grid та удосконалення і підвищення кібербезпеки електроенергетичних мереж за рахунок оцінки ризиків і властивостей використання розробленої моделей та методів для забезпечення прогнозування і аналізу атак і захисту. Були отримані наступні результати:

- отримано імовірні оцінки і прогнози властивостей системи
- визначено рамки оцінки для виконання
- створено об’єктну модель прогнозування та симуляції атак для системи ГЕС
- розраховано ймовірні атаки за ступенем серйозності уразливості
- представлено результати моделювання і варіанти захисту

**ДОДАТОК А**


СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ
Комплексна тема:
Smart Grid. Методи забезпечення кібербезпеки систем релейного захисту та автоматики
Smart Grid
Виконала студент групи КН-17дм: Старцева Юлія
Науковий керівник: проф. Кривуля Г.Ф.


Проблеми кібербезпеки Smart Grid
Основні проблеми кібербезпеки Smart Grid:
• Затримки
• Втрата потужності
• Якість і зміна напруги
• Управління захистом від замикань на землю
• Зміна конфігурації мережі
• Дизайн архітектури комунікацій Smart Grid:
○ Енергетичні послуги;
○ Велика сума даних
○ Зміна трафіка
○ Якість обслуговування і безпека
2

## Актуальність дослідження

**При дослідженні рішень для Smart Grid важливо розглянути безпеку для захисту важливих активів електроенергетичної системи.**

**Увага кібербезпеки пов'язана з системами інформаційних технологій, метою яких є захист інформації та інформаційних систем щодо несанкціонованого доступу, використання, модифікації або будь-яких дій, які можуть поставити під загрозу конфіденційність, цілісність або доступність інформації.**


3

## Мета роботи та постановка задачі

Підвищити кібербезпеку електроенергетичних мереж за рахунок оцінки ризиків і властивостей використання розробленої моделі та методів в програмному інструменті архітектури для забезпечення прогнозування і аналізу атак і захисту.

**Основні завдання**:

- аналіз методів і стандартів забезпечення кібербезпеки
- аналіз методів прогнозування ймовірного моделювання архітектури
- аналіз властивостей та ризиків моделей безпеки на моделях архітектури підприємства
- імовірна оцінка і прогнозування властивостей системи
- визначення та застосування рамки оцінки для виконання
- створення об’єктної моделі для прогнозування та симуляції атак
- розрахунок ймовірних атак за ступенем серйозності уразливості
- представлення результату моделювання

4

# Вимоги до кібербезпеки в Smart Grid

Вимоги безпеки Smart Grid можна розділити на три групи:

- Доступність даних
- Цілісність даних
- Конфіденційність даних

Для безпечної та надійної роботи енергосистеми оператори повинні контролювати систему, оскільки вона проходить через різні режими роботи.

Різні інтелектуальні електронні пристрої використовуються для контролю стану системи.

Ці дані вимірювань можуть бути пошкоджені зловмисником або можуть бути відсутніми через несправність датчика. Оператори енергосистем повинні мати впевненість у даних вимірювань. З цієї причини стан оцінки широко використовується операторами енергосистеми для обчислення станів системи. Алгоритми оцінки стану можуть виявити будь-які погані дані та забезпечити високу точність оцінки за допомогою обмеженого вимірювання.

Структурний підхід до забезпечення систем ICT, таких як Smart Grid, вимагає, щоб результати оцінки ризику входили до системи управління безпекою та ризиками.

Стандарти для інтеграції розподілених енергетичних ресурсів і зберігання в системах передачі та розподілу, які належним чином регулюють перешкоди, які вони можуть сформувати при увімкненні та вимкненні (запобігання можливим каскадним впливам на умови спрацьовування), будуть необхідними для забезпечення стабільності та надійності інтелектуальної мережі. Для цього потрібні належні стандарти для моделювання таких ресурсів.

5

# Класифікація атак

В Smart Grid є чотири основні типи кібератак:

- Атака пристрою
- Атака даних
- Атака приватного життя
- атака доступності мережі

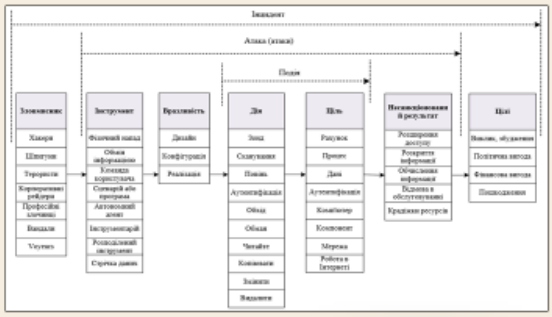

Рисунок 1 – Тактика атаки на аварію

Таблиця 1 – Основні види кібератак в Smart Grid

| Назва | Опис |
|---|---|
| Атака пристрою | Він спрямований на компроміс (контроль) мережевого пристрою. Часто це перший крок складної атаки |
| Атака даних | Він намагається змагально вставити, змінити або видалити дані в мережевому трафіку, щоб ввести Smart Grid в оману, щоб приймати неправильні рішення |
| Атака конфіденційності | Вона спрямована на вивчення / виведення особистої інформації користувачів, аналізуючи дані про використання електроенергії |
| Атака на доступ до мережі | Він спрямований на використання або придушення комунікаційних та обчислювальних ресурсів інтелектуальної мережі та призвести до затримки або невдачі зв'язку. |

6

## Атаки відмови в обслуговуванні в енергосистемах

Прикладний рівень. Атаки нижнього рівня фокусуються в основному на пропускної здатності каналів зв'язку, комп'ютерів або маршрутизаторів.

Мережевий і транспортний рівні. Ці два рівня повинні забезпечувати контроль надійності для доставки інформації по багато перехідних комунікаційних мереж. DoS-атаки на обох рівнях можуть серйозно погіршити наскрізну продуктивність зв'язку, таку як атаки з розподіленим трафіком і поширення хробака в Інтернеті.

Рівень MAC. Рівень MAC відповідає за надійний зв'язок точка-точка, а також за справедливість. В Smart Grid спуфінг являє собою відносно небезпечну загрозу на рівні MAC. Він націлений на доступність і цілісність.

Фізичний шар. Глушіння каналу є одним з найбільш ефективних способів запуску DoS-атак фізичного рівня, особливо для бездротового зв'язку.

| Рівень зв'язку | Атаки в енергосистемах |
|---|---|
| Прикладний рівень | - |
| Мережа | Рух затоплення |
| Транспортний шар | Буферне затоплення |
| Рівень MAC | ARP-спуфінг |
| Фізичний шар | Глушіння на підстанціях |

Таблиця 2 – Атаки відмови в обслуговуванні в енергосистемах

7

## Види вразливостей

Існує 4 основні класи вразливостей, які створюють значні ризики і відкривають двері для різних кібератак:

Клас 1: Люди, політика і процедура.

Клас 2: Уразливості програмного забезпечення та програмно-апаратних засобів.

Клас 3: Уразливості платформи.

Клас 4: Мережа.

8

# Моделі кібер втручань в Smart Grid

Кібервтручання в основному пов'язані з «Атаками хибного введення даних» і «Атаками перерозподілу навантаженням».

Велика кількість досліджень проводиться для запобігання введеня помилкових даних, які можна розділити на три категорії:

1) Аналіз вразливості оцінки стану
2) Аналіз наслідків
3) Розробка контрзаходів

9

# Моделі атак на перемикання та мережеві атаки

Розрізняють два типи команд перемикання:

1. Команди автоматичного перемикання: це команди, якими обмінюються між IED / Агентами, щоб усунути помилки короткого замикання, і вони зазвичай обмінюються по локальній мережі (LAN).

2. Команди ручного перемикання: це команди, відправлені системним оператором в центрі управління з глобальної мережі (WAN).

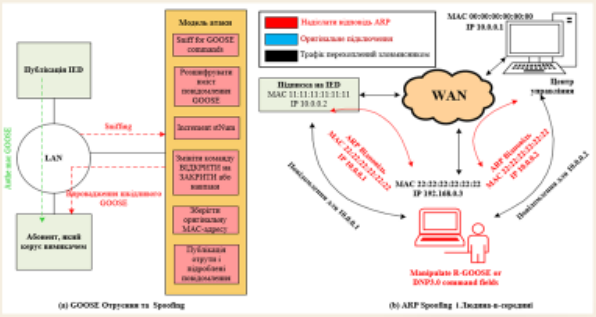


Рисунок 2 – (а) Процедура зараження GOOSE і Spoofing; (б) зараження ARP і R-GOOSE і DNP3.0 Атака «Людина в центрі».

| ARP зараження людина-в-середині | Відкритий з'єднувальний шар системи | Мережа | Можливі атаки |
|---|---|---|---|
| GOOSE | Layer 2 Data Link (MAC) | LAN | Зараження і спуфінг GOOSE |
| R- GOOSE | Layer 3 Network (IP) | LAN/WAN | ARP зараження людина-в-середині |
| DNP3.0 | Layer 4 Transport (TCP/IP) | LAN/WAN | ARP зараження людина-в-середині |

Таблиця 3 – Класифікація команд перемикання і можливих атак

10

# Синтез моделі динамічних систем на основі графів

На етапі синтезу даної моделі були використані динамічні системи для систематичного моделювання кібер і електричних мереж. Використання графів полегшує включення складних залежностей усередині і між кібер і електричними компонентами. Цей етап визначає відносну точність аналізу впливу Smart Grid і визначає можливі інструменти аналізу, що дозволяють отримати уявлення про уразливість і стратегії зміцнення системи.

Розроблено загальний і системний підхід до моделювання системи Smart Grid з використанням динамічного системного підходу на основі графів.

У дослідженні використано схему лінійної системи живлення ГЕС та побудовано до неї граф.

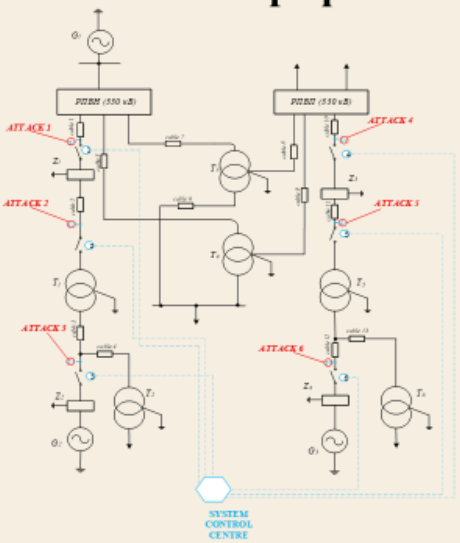


Рисунок 3 – Лінійна схема системи живлення ГЕС.

11

# Синтез моделі динамічних систем на основі графів

Кожен вузол має асоційований стан $x$ (що складається з відповідних системних напруг і струмів), регульований рівняннями динамічної системи, які моделюють фізику об'єкта (для випадку елементів енергосистеми) або функціональну або обчислювальну обробку (для випадку кібер-елементів).).

Влучний вислів для $f$ залежить від ребер асоційованого вузла. Вузли можуть бути згруповані, щоб сформувати динамічні агенти для подання взаємодій в Smart Grid, як показано на рис. 4, на основі функціональності або для балансування порядку підсистеми.

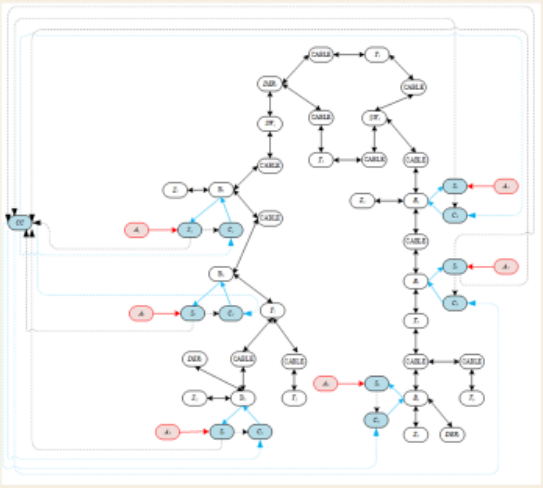

Рисунок 4 – Електричні і кібер-граф для системи ГЕС

12

# Розробка моделі для аналізу кібербезпеки

Структура моделі створена в інструменті аналізу архітектури підприємства Object Modeler, який забезпечує зручну взаємодію для моделювання та аналізу, додаючи об'єкти і малюючи зв'язки між ними.

Коли розрахунки завершені, результати представляються користувачеві шляхом колірного кодування всіх шаблонів і кроків атаки за шкалою від 0%: зелений - 50%: жовтий - 100%: червоний.

Ймовірність відноситься до ймовірності того, що один або кілька професійних тестерів проникнення успішно пройдуть етап атаки в об'єктної моделі за час, призначений для атаки. Ймовірності для шаблонів виводяться на основі оцінок кроків атаки, пов'язаних з ним, і обраного в даний момент колірного профілю.

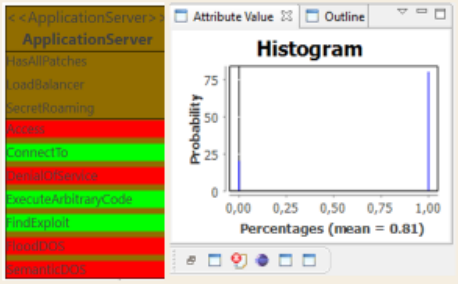


Рисунок 5 – Приклад гістограми об'єкта ApplicationServer

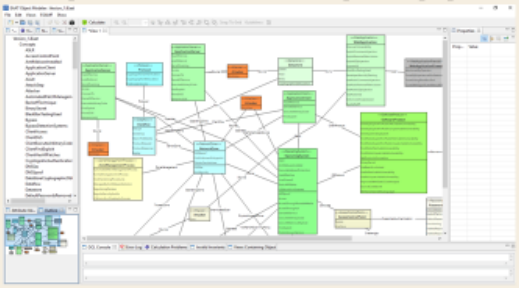

Рисунок 6 – Фрагмент вікна Object Modeler



# Результати моделювання

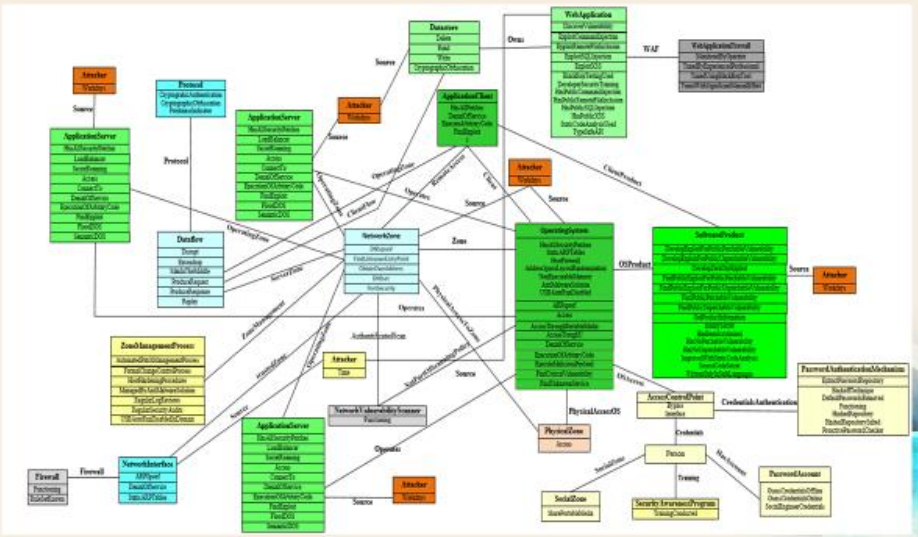

Рисунок 7 - Візуалізація моделі ГЕС класу CySeMoL до розрахунку

# Результати моделювання

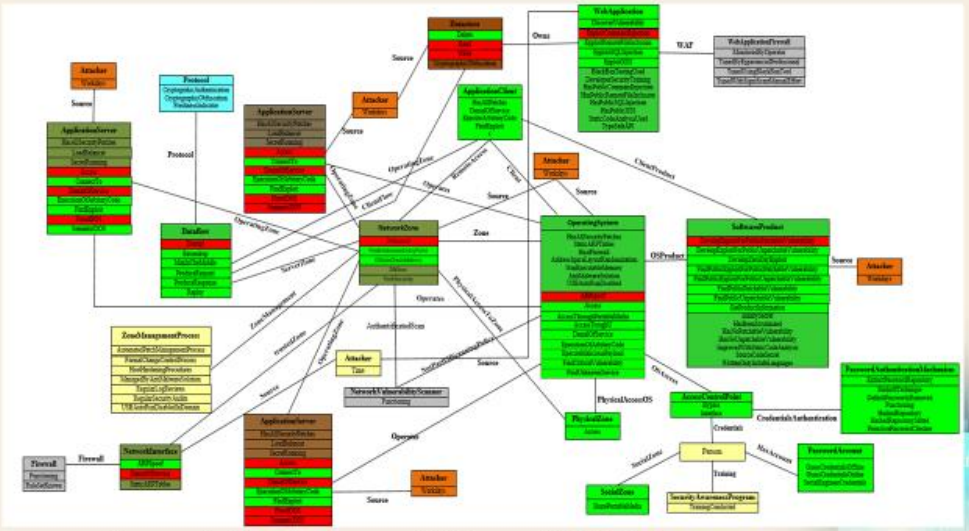

Рисунок 8 - Візуалізація моделі ГЕС класу CySeMoL після розрахунку

15

# Висновок

Основною вимогою для системи захисту є те, що вона може надійно виявляти будь-які несправності в зоні захисту. Захист і надійність захисту є первинними вимогами поряд зі швидкістю, вибірковістю. Масивність Smart Grid і розширені можливості зв'язку роблять її більш схильною до кібератаки. Smart Grid вважається важливою інфраструктурою, всі уразливості повинні бути ідентифіковані і повинні бути реалізовані достатні рішення для зниження ризиків до прийнятного рівня безпеки.

Для забезпечення інфраструктури інтелектуальних мереж зв'язку буде потрібно використання протоколів безпеки на основі стандартів.

Необхідно вжити декілька кроків: оптимізації для забезпечення максимальної надійності, доступності, ефективності та економічних показників, доступності, яка надає доступ до мережі для всіх користувачів мережі, особливо для поновлюваних джерел енергії і високоефективної місцевої генерації з нульовими або низькими викидами вуглецю, надійності, що забезпечує і поліпшує безпеку і якість поставок, відповідає вимогам епохи цифрових технологій зі стійкістю до небезпек і невизначеності

В результаті проведеного аналізу була побудована модель прогнозування імовірнісних атак на архітектуру підприємства. Ймовірності для активів виводяться на основі оцінок кроків атаки, пов'язаних з ним, і обраного в даний момент кольорового профілю.

16