ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО–КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Автоматизовані методи моніторингу для виявлення кіберзагроз в системах критичної інфраструктури»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
Освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

_____ *Максим ЗАЙЦЕВ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД–42
Максим ЗАЙЦЕВ
Ім'я, ПРІЗВИЩЕ
Керівник: Ігор БУЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО–КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Зайцев Максим Ігорович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Автоматизовані методи моніторингу для виявлення кіберзагроз в системах критичної інфраструктури
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно–комунікаційних технологій від «24» лютого 2025р. № 56
2. Строк подання кваліфікаційної роботи «5» червня 2025р.
3. Вихідні дані до кваліфікаційної роботи: науково–технічна література; міжнародні стандарти: SO/IEC 27001, IEC 62443, ISA/IEC 62443; керівництво з безпеки для ICS: NIST SP 800–82; фреймворки: MITRE ATT&CK; сучасні рішення: SIEM, EDR, XDR, UEBA;
4. Зміст розрахунково–пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи моніторингу кіберзагроз в системах критичної інфраструктури
2. Аналіз автоматизованих методів виявлення кіберзагроз
3. Застосування фреймворків та моделей для автоматизованого виявлення кіберзагроз
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02–28.03.2025	Виконано
2	Обробка матеріалу	29.03–05.04.2025	Виконано
3	Розробка теоретичної частини	06.04–10.04.2025	Виконано
4	Розробка фреймворку	11.04–20.04.2025	Виконано
5	Висновки за результатами аналізу	21.04–06.05.2025	Виконано
6	Оформлення пояснювальної записки	07.05–08.05.2025	Виконано
7	Розробка презентації	09.05–11.05.2025	Виконано
8	Передзахист	27.05–29.05.2025	Виконано
9	Здача в деканат	02.06–05.06.2025	Виконано

Здобувач вищої освіти _____ Максим ЗАЙЦЕВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 69 стор., 32 рис., 5 табл., 30 джерел.

Мета роботи – підвищення ефективності виявлення кіберзагроз у системах критичної інфраструктури за рахунок впровадження автоматизованих методів моніторингу.

Об'єкт дослідження – процес моніторингу кіберзагроз у системах критичної інфраструктури.

Предмет дослідження – автоматизовані методи моніторингу для виявлення кіберзагроз в системах критичної інфраструктури.

Короткий зміст роботи: У роботі досліджено актуальні загрози для об'єктів критичної інфраструктури та визначено особливості побудови систем моніторингу у таких середовищах. Проаналізовано сучасні автоматизовані підходи до виявлення аномалій та кіберзагроз, їх переваги та обмеження.

Розглянуто архітектурні рішення для реалізації безперервного моніторингу, описано принципи збору, агрегації та аналізу даних у режимі реального часу.

Запропоновано підходи до вдосконалення існуючих систем спостереження з урахуванням специфіки критичної інфраструктури, а також оцінено перспективи їх розвитку.

КЛЮЧОВІ СЛОВА: КРИТИЧНА ІНФРАСТРУКТУРА, КІБЕРЗАГРОЗИ, АВТОМАТИЗОВАНИЙ МОНІТОРИНГ, SIEM, MITRE ATT&CK, SPLUNK, WAZUH, ПОВЕДІНКОВИЙ АНАЛІЗ, СИГНАТУРНИЙ МЕТОД, МАШИННЕ НАВЧАННЯ, ВИЯВЛЕННЯ ВТОРГНЕНЬ, КОРЕЛЯЦІЯ ПОДІЙ, БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ.

ЗМІСТ

ВСТУП…… 9
1 ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ КІБЕРЗАГРОЗ В СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ……..…… 10
1.1 Поняття та складові критичної інфраструктури……..... 10
1.2 Основні типи кіберзагроз для критичних об’єктів…… 11
1.3 Стандарти і нормативна правова база в галузі кібербезпеки критичної інфраструктури……... 21
1.4 Традиційні та сучасні методи моніторингу…… 23
2 АНАЛІЗ АВТОМАТИЗОВАНИХ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ……. 36
2.1 Архітектура системи автоматизованого моніторингу кібербезпеки…... 36
2.2 Типи та функціональні рішення автоматизованих систем моніторингу кіберзагроз…….. 41
2.3 Застосування фреймворку MITRE ATT&CK……..…….. 47
2.4 Автоматизовані методи виявлення кіберзагроз…… 59
3 ЗАСТОСУВАННЯ ФРЕЙМВОРКІВ ТА МОДЕЛЕЙ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ…… 56
3.1 Аналіз сучасних інструментів автоматизованого виявлення кіберзагроз……...……...….. 56
3.2 Застосування MITRE ATT&CK Navigator для моделювання загроз…... 59
ВИСНОВКИ…… 75
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ…….. 77
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ(Презентація)…….. 80

ВСТУП

У сучасному цифровому світі питання забезпечення кібербезпеки набуває особливої актуальності, особливу роль у цій архітектурі займають об’єкти критичної інфраструктури — системи, безперебійне функціонування яких є життєво важливим для національної безпеки, економічної стабільності та добробуту суспільства.

У зв’язку з цим забезпечення кібербезпеки критичної інфраструктури стає пріоритетним напрямом як для окремих держав, так і для міжнародних організацій. Одним із ключових викликів сучасності є те, що зростання цифровізації супроводжується зростанням кіберзагроз. Хакерські атаки, шкідливе програмне забезпечення, цілеспрямовані кампанії (APT–групи), соціальна інженерія та інші форми кіберзлочинності — усе це створює реальні ризики для стабільного функціонування критичних об’єктів.

Класичні методи захисту (наприклад, міжмережеві екрани, антивірусні рішення) вже не можуть гарантувати належний рівень безпеки. Натомість фокус зміщується у бік проактивного виявлення загроз, аналізу аномальної поведінки та кореляції подій у режимі реального часу. У цьому контексті особливе значення набувають автоматизовані методи моніторингу, які дозволяють обробляти великі обсяги даних, виявляти потенційні інциденти без участі людини та швидко реагувати на кіберзагрози.

Автоматизовані системи моніторингу активно впроваджуються у всьому світі. Вони забезпечують централізований збір, обробку та аналіз подій безпеки, використовують сигнатурні та поведінкові моделі, алгоритми машинного навчання, корелюють дані з таксономіями загроз, забезпечують реагування на інциденти. Однак для систем критичної інфраструктури ці рішення повинні бути адаптовані до особливостей технологічного середовища, специфіки OT–сегментів (Operational Technology), використання застарілого обладнання та обмежень щодо оновлень і сканування.

Особливої уваги потребує і питання побудови безпечної архітектури моніторингу, адже самі засоби моніторингу можуть стати ціллю для зловмисників. Відсутність цілісного бачення загроз, несинхронізованість між відомчими системами та обмеженість фінансових ресурсів часто стають бар'єрами для впровадження комплексних рішень в галузі кібербезпеки. Тому виникає потреба в дослідженні ефективних, гнучких та доступних методів моніторингу, що можуть бути масштабованими та адаптованими під конкретні умови.

1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ КІБЕРЗАГРОЗ В СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та складові критичної інфраструктури

Критична інфраструктура (КІ) — це сукупність об’єктів, систем, мереж і послуг, які мають вирішальне значення для функціонування держави, її економіки, сфери охорони здоров’я, громадської безпеки та загального добробуту населення. Її порушення або знищення може спричинити серйозні наслідки для суспільства, включно з загрозами національній безпеці або стабільності економіки[1].

Згідно з чинним законодавством, зокрема проєктом Закону України №5219 від 09.03.2021 року, об’єктами критичної інфраструктури вважаються ті суб’єкти, чия діяльність здійснюється у межах відповідних секторів і виконує життєво важливі функції або забезпечує надання послуг, переривання яких може мати негативні наслідки для безпеки держави та життєдіяльності населення. До таких секторів належать, зокрема, урядування та надання ключових адміністративних послуг, енергозабезпечення, водопостачання, охорона здоров’я, транспорт, телекомунікації, інформаційні технології, продовольча безпека та інші[2].

Усередині цих секторів критичні об’єкти класифікуються за рівнем важливості на чотири категорії критичності. Найвищий рівень — це об’єкти загальнодержавного значення, функціонування яких впливає на стабільність інших елементів КІ і порушення яких може призвести до криз на рівні держави. Об’єкти другої категорії мають регіональне значення, і збої у їх роботі спричиняють кризові ситуації регіонального масштабу. До третьої категорії відносять об’єкти, порушення діяльності яких матиме наслідки на місцевому рівні, а до четвертої — ті, що пов’язані з локальними збоями та функціонують у межах обмеженої території або спільноти.

У сучасних умовах захист критичної інфраструктури потребує не лише

фізичної охорони чи технічної безпеки. Одним із ключових понять у цій сфері є стійкість — здатність об’єкта протистояти загрозам, оперативно реагувати на інциденти, забезпечувати безперервність функціонування та відновлюватись після збоїв. Досягнення стійкості вимагає комплексного підходу, що передбачає впровадження систем постійного моніторингу, оцінки ризиків, тестування готовності до надзвичайних ситуацій, а також активне використання автоматизованих методів виявлення та реагування на кіберзагрози.

1.2 Основні типи кіберзагроз для критичних об’єктів

Критична інфраструктура — це комплекс об’єктів, систем і послуг, які мають ключове значення для безперебійного функціонування держави та безпеки громадян. Серед них — енергетика, зв'язок, охорона здоров’я, транспорт, державне управління. Їх порушення через кіберзагрози може призвести до серйозних соціально-економічних наслідків.

Основні типи кіберзагроз (рис.1.1), що становлять небезпеку для об’єктів критичної інфраструктури можна поділити[3]: шкідливе програмне забезпечення, програми-вимагачі, DDoS–атаки, атака «Людина посередині» (MitM), безфайлові та фішингові атаки.

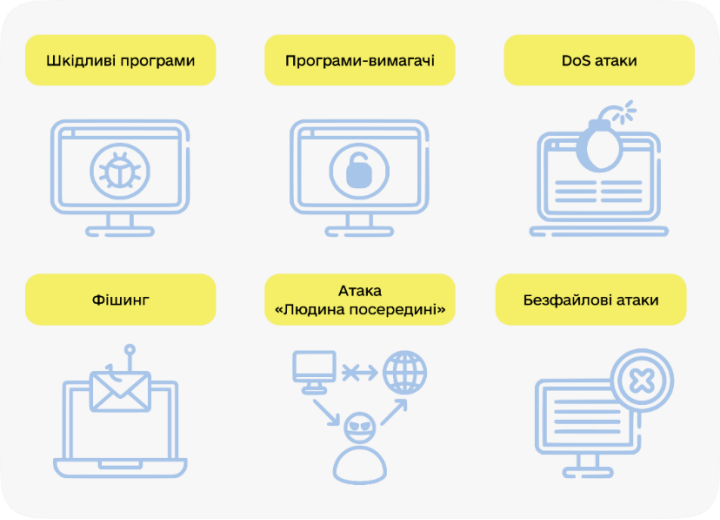


Рисунок 1.1 – Схема типових кіберзагроз

Шкідливе програмне забезпечення (або Malware) — це загальний термін для програм, які виконують шкідливі дії на заражених пристроях: викрадення даних, спотворення або знищення інформації, встановлення бекдорів. Перша зареєстрована успішна кібератака на енергетичну систему з виведенням її із ладу сталась 23 грудня 2015 року [4], вона отримала назву «Black Energy» (рис. 1.2). Як результат зловмисники отримали доступ до SCADA–систем і вивели з ладу електропостачання.

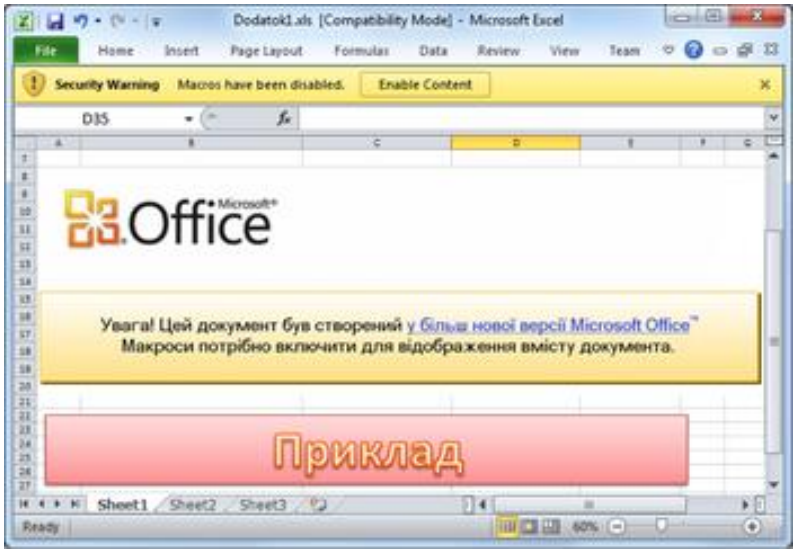


Рисунок 1.2 – Скриншот відкритого документу, зараженого троянською програмою BlackEnergy

Програми-вимагачі – це тип шкідливого програмного забезпечення, який спеціально розроблений для шифрування даних на комп'ютерах чи серверах жертв із метою вимагання викупу. Кіберзлочинці, які стоять за цими атаками, вимагають оплату за розшифрування файлів, зазвичай у криптовалюті, що значно ускладнює їхнє відстеження.

Головна небезпека вірусів-вимагачів полягає в їхній універсальності та руйнівному потенціалі. Вони однаково ефективно вражають як приватних користувачів, так і компанії будь-якого масштабу. Для бізнесу шантажист може паралізувати операційну діяльність, заблокувати доступ до критичних даних і

поставити під загрозу конфіденційну інформацію клієнтів, співробітників чи партнерів. Це призводить до значних репутаційних втрат та фінансових збитків, які можуть бути катастрофічними. Крім прямого економічного впливу, вірус-вимагач завдає шкоди довірі до цифрових інструментів і технологій. Навіть експерти з кібербезпеки часто не можуть відновити файли без втручання зловмисників, що ще більше підкреслює небезпеку цього типу атак.

Відома кібератака на Colonial Pipeline, яка за оцінками преси, вважається «найуспішніша кібератака на нафтову інфраструктуру в історії Америки»[5]. Тоді зловмисники зашифрували IT–системи одного з найбільших трубопроводів у США (рис. 1.3), що спричинило дефіцит пального у низці штатів.

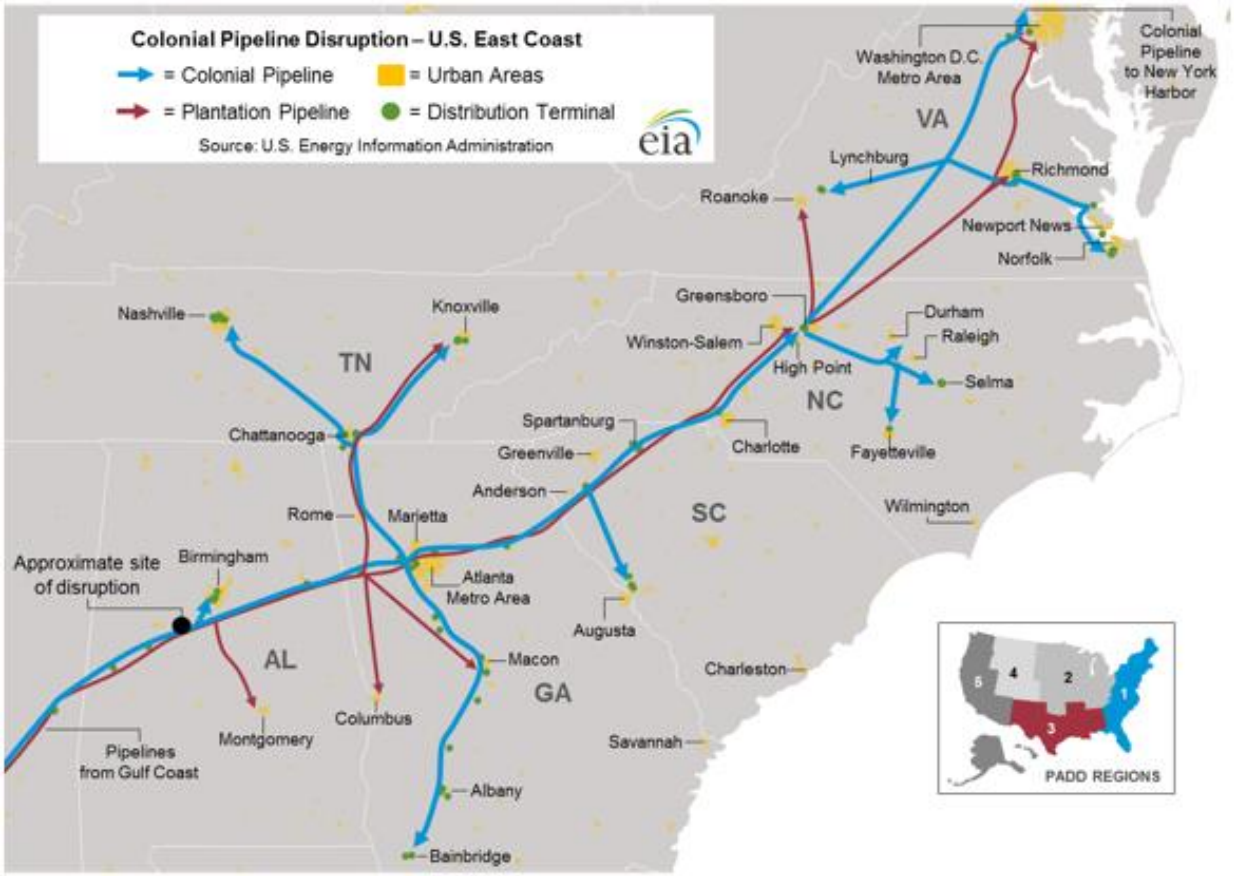


Рисунок 1.3 – Детальна схема масштабів трубопроводу, на яку зловмисники зробили кібератаку

DDoS–атаки – це один із найпоширеніших і найнебезпечніших видів

кіберзагроз, спрямований на порушення доступності інтернет-ресурсів або онлайн-платформ шляхом перевантаження їх фальшивим трафіком. В основі такої атаки лежить навмисне створення надмірного навантаження на сервер чи мережеву інфраструктуру, внаслідок чого ресурси не можуть обробити запити легітимних користувачів. Відмова в обслуговуванні відбувається через масове надсилання однотипних або зманіпульованих запитів, які імітують звичайну активність, але насправді є складовою деструктивного впливу.

Для здійснення таких атак зловмисники зазвичай використовують розподілену мережу інфікованих пристроїв, об'єднаних у так звану ботнет-мережу(рис.1.4). До неї можуть входити комп'ютери, мобільні телефони, веб-камери, маршрутизатори або інші пристрої, що мають підключення до Інтернету та були раніше заражені шкідливим програмним забезпеченням. Усі ці пристрої, керовані віддалено зловмисником, одночасно надсилають запити на цільовий сервер. У результаті такого масового навантаження сервер не витримує обсягу трафіку, що призводить до його сповільнення, збоїв або повної недоступності для звичайних користувачів.

Залежно від мети зловмисників, DDoS-атаки можуть бути короткостроковими або тривалими, мати на меті суто економічну шкоду або ж виступати елементом політичного чи інформаційного тиску. В окремих випадках ці атаки супроводжуються вимогою викупу за припинення трафіку, що класифікується як шантаж або кібервимагання. Зокрема, в останні роки помітним є зростання використання DDoS-атак у геополітичному контексті. Так, з початком повномасштабного вторгнення РФ в Україну, державні та комерційні ресурси в Україні регулярно зазнавали потужних DDoS-атак, які координувалися як державними, так і псевдодержавними хакерськими угрупованнями. Такі атаки мали на меті виведення з ладу інформаційних систем, дестабілізацію роботи урядових платформ, обмеження доступу громадян до сервісів електронного урядування та фінансових установ.

Типи DDoS-атак можуть відрізнятися як за рівнем мережевої моделі, на який спрямовано вплив, так і за технічними характеристиками самого навантаження.

Найбільш поширеними є атаки на мережевому рівні (наприклад, за допомогою протоколів UDP чи ICMP), а також атаки на рівні застосунків, що імітують поведінку звичайного користувача, наприклад, надсилаючи численні HTTP-запити на вебсайт. Особливо небезпечними є сценарії, в яких атаки використовують слабкі сторони поширених мережевих сервісів, що дозволяє зловмисникам здійснювати так звані рефлексивні або ампліфікаційні атаки — коли з невеликого початкового запиту формується багаторазово збільшений трафік у відповідь, спрямований на жертву.

Наслідки DDoS-атак можуть бути критичними: тимчасова або довготривала недоступність ресурсів спричиняє фінансові втрати, падіння репутації, переривання надання послуг, а в окремих випадках — параліч функціонування важливих секторів економіки чи державного управління. Особливо чутливими до таких атак є системи онлайн-банкінгу, електронного документообігу, державні реєстри, платформи цифрової ідентифікації тощо.

Для протидії DDoS-атакам необхідно впроваджувати багаторівневі засоби захисту, які включають фільтрацію аномального трафіку, обмеження кількості з’єднань, інтеграцію із системами виявлення вторгнень, а також використання послуг спеціалізованих платформ захисту (таких як Cloudflare, Imperva або Akamai). Важливим є також постійний моніторинг мережевого трафіку, регулярне тестування стійкості інфраструктури до перевантажень та використання розподілених систем доставки контенту (CDN), які дозволяють зменшити вразливість окремих вузлів.

У сучасних умовах DDoS-атаки залишаються однією з найреальніших загроз для організацій будь-якого масштабу, і їх успішне відбиття вимагає як технічної готовності, так і організаційної обізнаності персоналу щодо ознак і наслідків подібних атак.

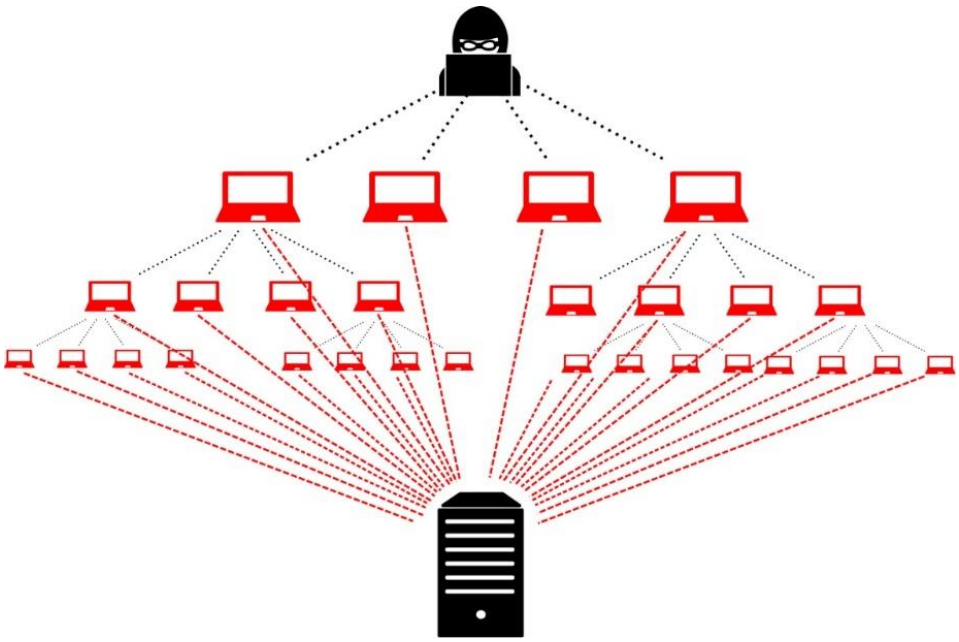


Рисунок 1.4 – Типова структура DDoS–атаки

Яскравий приклад відбувся у лютому 2022 року українські державні сервіси та банки (ПриватБанк, Ощадбанк) стали об’єктами масованих DDoS–атак, що були частиною гібридної війни. Клієнти державних банків повідомляли про перебої в роботі мобільних додатків, були проблеми із запуском та проведенням платежів[6].

Атака «Людина посередині» (MitM) – цей тип атак є розповсюдженим та руйнівним. Суть атаки man-in-the-middle доволі проста: злочинець таємно перехоплює трафік з одного комп’ютера та відправляє його кінцевому одержувачу, попередньо прочитавши та змінивши на свою користь. Атаки MITM надають можливість робити такі дії як підміна криптовалютного гаманця для викрадення коштів, перенаправлення браузера на шкідливий вебсайт або ж просто пасивний збір інформації з метою її подальшого злочинного використання. Найбільш очевидний спосіб, коли хтось може це зробити, коли ви користуєтесь незашифрованою, загальнодоступною мережею Wi-Fi, як у аеропортах чи кафе. MITM–атаки трапляються і на мережевому рівні (рис. 1.5).[7]

Особливу небезпеку такі атаки становлять у публічних незашифрованих Wi-Fi мережах, де зловмисник може непомітно перехопити трафік користувача, наприклад, у кафе чи аеропорту. В таких умовах дуже просто створити фальшиву точку доступу, яка імітує легітимну мережу, або використати слабкі сторони

протоколів маршрутизації для перехоплення інформації.

Наслідки MitM-атак можуть бути серйозними: від викрадення конфіденційних даних до повного контролю над сеансом користувача. У контексті об’єктів критичної інфраструктури це може призвести не лише до втрати даних, а й до прямого впливу на роботу систем управління технологічними процесами. Тому розуміння механізмів дії таких атак і впровадження відповідних засобів захисту є ключовими завданнями у сфері кібербезпеки .[8]

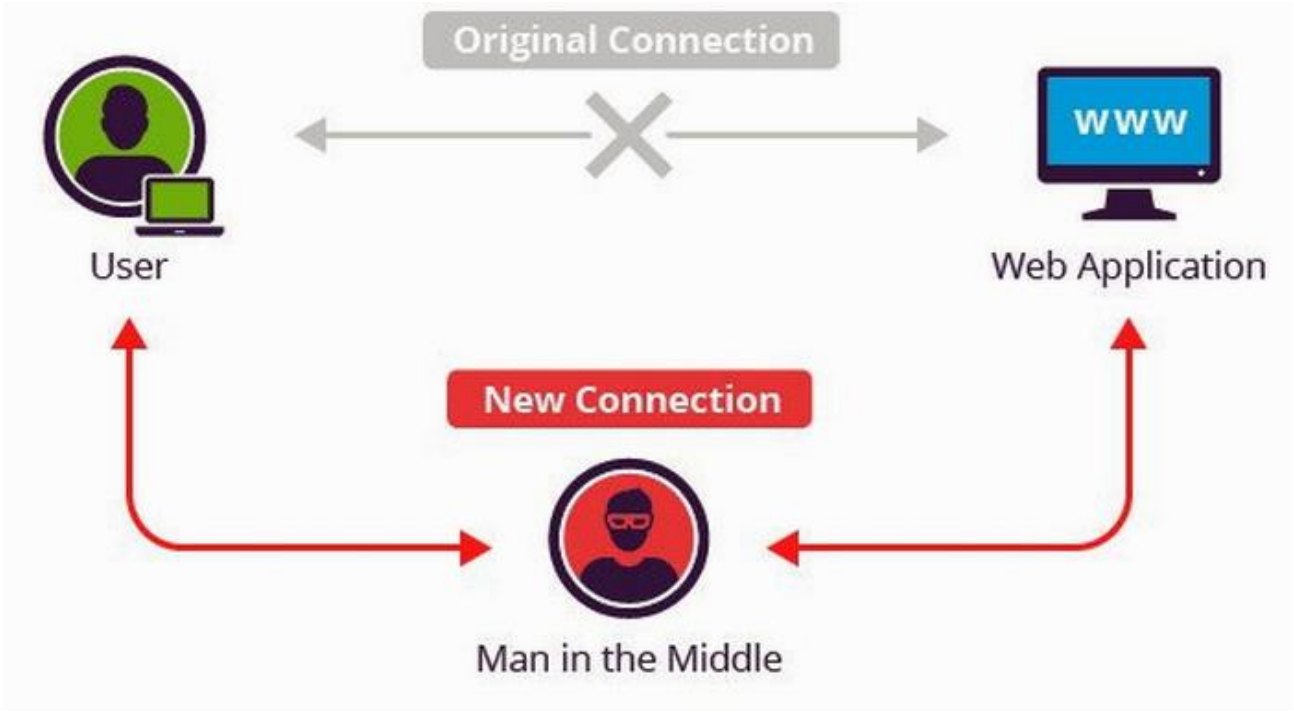


Рисунок 1.5 – Схематичний принцип атаки типу Man–In–The–Middle

Безфайлові атаки – ці атаки не залишають файлів на диску, а працюють безпосередньо в оперативній пам’яті. Шкідлива програма призначена для отримання несанкціонованого доступу до пристрою, мережі чи даних з ціллю їх експлуатації або заподіяння шкоди. Існують різні типи шкідливих програм, як–от віруси, хробаки, програми–вимагачі, шпигунське ПЗ, рекламні програми та трояни. Кожна з них по–своєму проникає в комп'ютерні системи й спричиняє збої в роботі. Наслідки зараження шкідливими програмами бувають абсолютно різними: від появи дратівливої реклами до блокування роботи всієї мережі. Незначне зараження рекламним ПЗ призведе лише до відображення банерів на вашому екрані. А от

зараження програмою–вимагачем може заблокувати доступ до всієї системи, доки не заплатити викуп у розмірі тисяч доларів. У гіршому випадку кібератака призведе до масових витоків даних, розкриття конфіденційної інформації та псування репутації компанії, що зазнала атаки.

Навіть незначне зараження, наприклад, рекламним програмним забезпеченням, може викликати постійне відображення банерів чи небажаної інформації на екрані користувача. У той же час потрапляння програми-вимагача в систему здатне заблокувати повний доступ до файлів і процесів, ставлячи користувача перед вибором: втратити дані або сплатити чималий викуп. У найгірших випадках зараження шкідливим ПЗ призводить до масштабних витоків даних, втрати комерційної таємниці, викрадення персональної інформації або серйозної шкоди репутації організації.

Одним з основних каналів доставки шкідливого ПЗ залишаються фішингові атаки (рис 1.6). Це особлива форма соціальної інженерії, яка полягає в обмані користувача з метою добровільної передачі конфіденційних даних. Зловмисники створюють правдоподібні повідомлення або вебсайти, які імітують офіційні сервіси, що спонукає жертву до введення логінів, паролів, платіжної інформації чи іншої важливої інформації. Часто фішинг реалізується через електронні листи, SMS-повідомлення або повідомлення в соціальних мережах, які пропонують нібито привабливу можливість, послугу чи вигоду. Такий психологічний тиск примушує користувача самостійно надати зловмиснику все необхідне для атаки.

Усі ці форми загроз підкреслюють необхідність високого рівня інформаційної гігієни, сучасних технічних засобів захисту та підвищеної пильності з боку користувачів — як на рівні побутового застосування, так і в контексті безпеки критичних інформаційних систем.

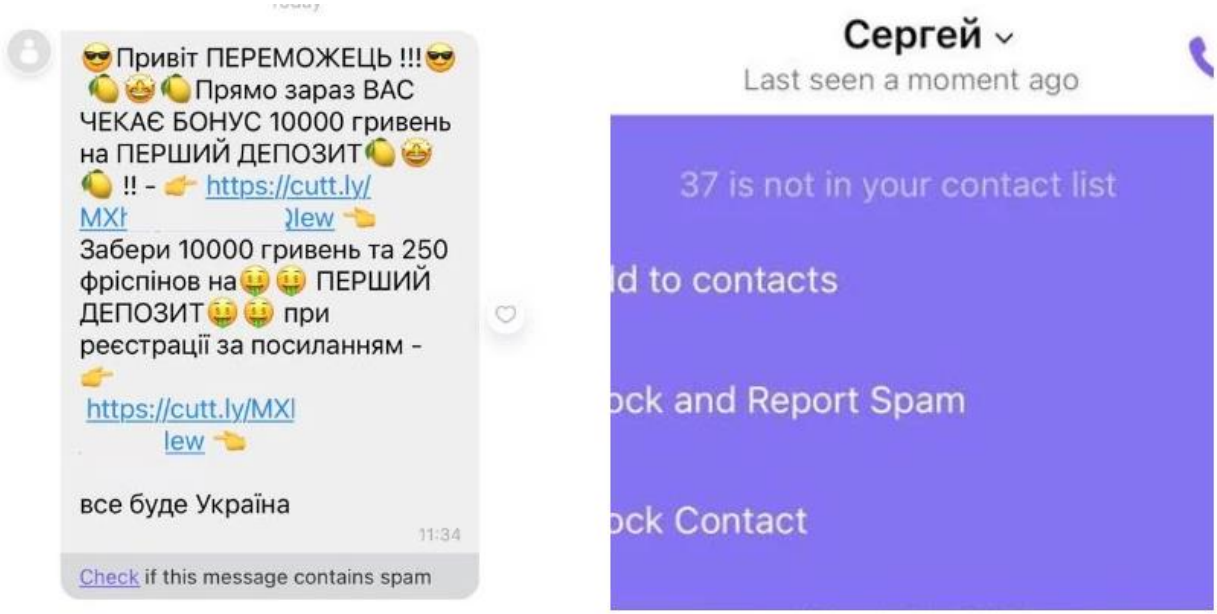


Рисунок 1.6 – Приклад фішингу, спамне повідомлення про виграш з російського номера телефону від «Сергія»

Інтерес зловмисників може викликати будь–яка інша конфіденційна інформація. Шахраї «вивуджують» дані користувачів під різними пристойними приводами: перевірка авторизації на сайті, необхідність «відписатися» від спаму в електронній пошті, оплата покупки за низькою ціною або з великою знижкою, необхідність встановити новий додаток.

Найпопулярніші серед шахраїв схеми онлайн-фішингу:

– розсилка підроблених електронних листів, з проханням підтвердити логін і пароль. Зловмисники можуть заспамити повідомленнями мільйони адрес електронної пошти протягом декількох годин. Для цього бази попередньо купуються. Однак за такі дії передбачена кримінальна відповідальність, а сервери, з яких розсилається спам, обчислюють і банять, тому цей спосіб повільно відходить у минуле;

– шахраї створюють електронні листи з підробленим рядком «Mail From:», використовуючи недоліки в поштовому протоколі SMTP. Коли відвідувач відповідає на фішингові повідомлення, лист з відповіддю автоматично пересилається шахраям електронною поштою;

– фішингові схеми популярні при проведенні інтернет–аукціонів. При

цьому товари виставляються на продаж через легальний інтернет–аукціон, однак кошти перераховуються через підроблений вебвузол;

– фіктивні благодійні організації, які звертаються з проханням про пожертвування.

Статистичний аналіз фішингових атак, що використовують бренди відомих компаній в Україні у 2022 році

У 2022 році в кіберпросторі України спостерігалася активізація фішингових атак, спрямованих на заволодіння коштами, платіжними реквізитами та обліковими даними користувачів онлайн-банкінгу. Зловмисники активно використовували бренд-джекінг, імітуючи комунікацію від імені відомих українських компаній з метою введення в оману потенційних жертв.

Аналіз зафіксованих фішингових кампаній у досліджуваному періоді виявив тенденцію до експлуатації довіри громадян до популярних торгових марок. Зокрема, фіксувалися численні випадки розповсюдження шахрайських повідомлень, що імітували надання фінансової допомоги або цінних призів від таких компаній, як: ОККО (псевдо-акції з паливними субсидіями), Київстар (грошові виграші), АТБ (обіцянки продуктових чи фінансових бонусів).

Результати статистичного аналізу фішингових атак засвідчують, що найбільш експлуатованими брендами стали:

1. єДопомога – ініціатива викликала широкий інтерес, що зробило її легкою ціллю для шахраїв;
2. Дія – зловмисники маскували фішингові сайти під офіційні портали цифрових послуг;
3. ПриватБанк – наймасовіше представлений банк в Україні;
4. Ощадбанк – ціль через соціальні виплати;
5. OLX – зловживання довірою під час онлайн-продажів.

Ці бренди (рис.1.7) об’єднує широка впізнаваність, часте використання в повсякденному житті та асоціація з фінансовими транзакціями, що робить їх особливо привабливими для атак соціальної інженерії. Зловмисники свідомо експлуатують довіру користувачів до цих сервісів, створюючи фішингові

повідомлення, які виглядають максимально переконливо. Це ускладнює виявлення шахрайства, особливо для нетехнічних користувачів, які часто не перевіряють достовірність отриманої інформації. Успішні фішингові кампанії на основі таких брендів свідчать про необхідність посилення цифрової грамотності населення та впровадження більш жорстких механізмів автентифікації та перевірки комунікацій.[9]

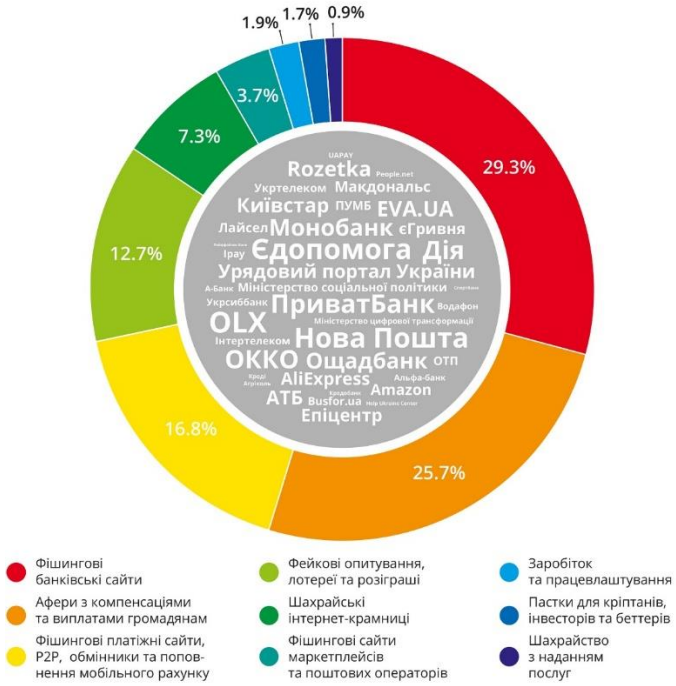


Рисунок 1.7 –Найпопулярніші бренди серед кібермародерів у 2022 році

1.3 Стандарти і нормативна правова база в галузі кібербезпеки критичної інфраструктури

Забезпечення кібербезпеки критичної інфраструктури базується на чітко визначених стандартах, регуляторних документах і законодавчих нормах, які формують вимоги до політик безпеки, процедур реагування на інциденти, а також контролю за виконанням заходів захисту. Об’єкти критичної інфраструктури часто обробляють інформацію, що має статус державної, службової або комерційної таємниці, тому підходи до захисту повинні бути системними та відповідати

визначеним стандартам.

Для впровадження ефективних механізмів кіберзахисту, а також систем управління інформаційною безпекою, використовують як національні, так і міжнародні нормативно–правові документи. Серед ключових:

SO/IEC 27001 — найвідоміший у світі стандарт для систем управління інформаційною безпекою (СУІБ) (рис.1.8). Він визначає вимоги, яким повинна відповідати СУІБ. Зі зростанням кіберзлочинності та постійною появою нових загроз, управління кіберризиками може здаватися складним або навіть неможливим. Стандарт ISO/IEC 27001 допомагає організаціям усвідомлювати ризики та проактивно виявляти й усувати слабкі місця[10].



Рисунок 1.8 – Логотип організації ISO зі стандартом 27001

IEC 62443 — це міжнародна серія стандартів, розроблених Міжнародною електротехнічною комісією (IEC) для кібербезпеки в системах промислової автоматизації та управління (IACS). Основною метою IEC 62443 є захист промислового середовища від ескалації кіберзагроз.

Ці кіберзагрози можуть порушити роботу в усіх галузях промисловості, що використовують IACS, включаючи автоматизацію будівель, медичне обладнання, виробництво та розподіл електроенергії, транспорт та переробну промисловість, таку як хімічна, нафтогазова[11].

IEC 62443 забезпечує структуровану основу для вирішення цих проблем та впровадження індивідуальних заходів кібербезпеки для IACS. ISA/IEC 62443 пропонує комплексний підхід до виявлення та зменшення вразливостей у

промислових мережах, підтримуючи цілісність, доступність та конфіденційність критично важливих систем.(рис.1.9)

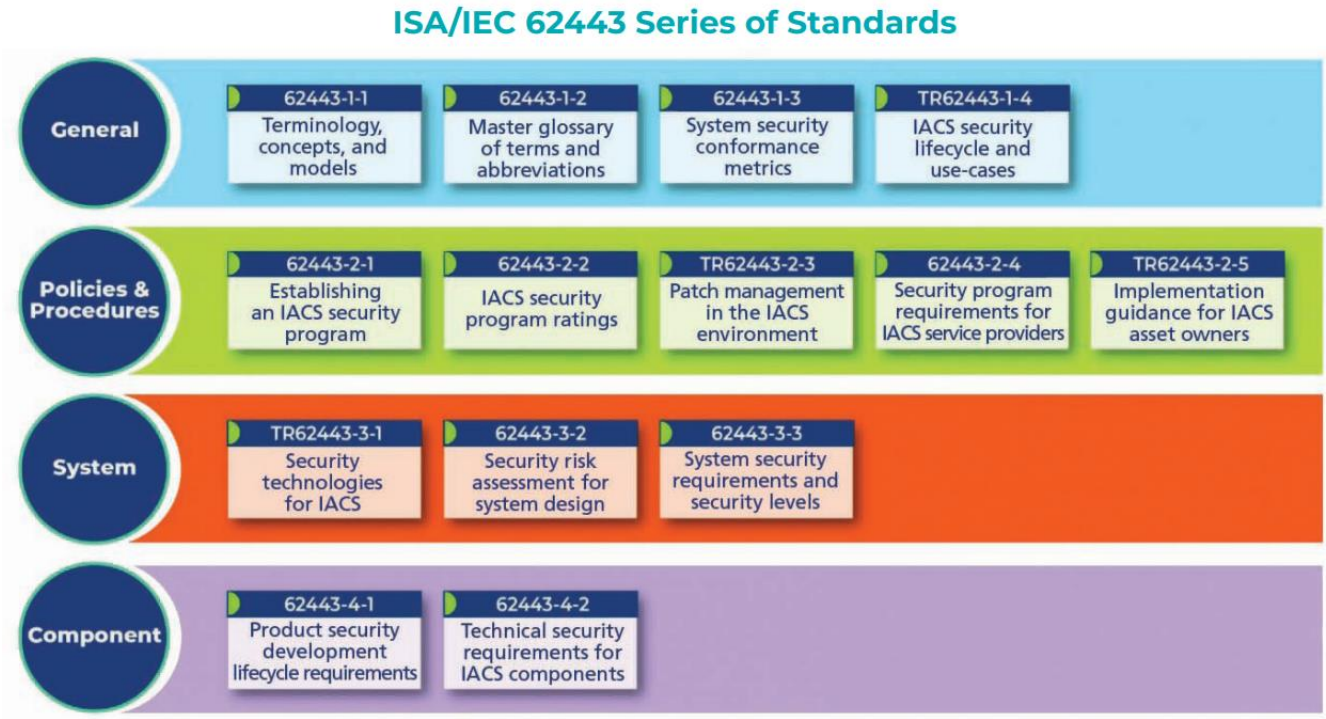


Рисунок 1.9 – Серія стандартів ISA/IEC 62443

NIST SP 800–82 — керівництво з безпеки для ICS від Національного інституту стандартів і технологій (США), містить практичні рекомендації щодо аналізу ризиків, впровадження засобів контролю та реагування на інциденти.

1.4 Традиційні та сучасні методи моніторингу

Моніторинг інформаційної безпеки є ключовим елементом забезпечення кіберзахисту критичних об’єктів інфраструктури. Залежно від рівня технологічного розвитку та потреб організацій, використовуються як традиційні (рис.1.10), так і сучасні (рис.1.14) підходи до виявлення кіберзагроз.



Рисунок 1.10 – Схема традиційних методів моніторингу

Логування та аналіз журналів подій є одним із найбільш традиційних, проте досі актуальних методів моніторингу інформаційної безпеки. Суть цього підходу полягає у систематичному зборі та аналізі логів — даних, які генеруються комп'ютерними системами, додатками, мережевими пристроями та іншими елементами IT-інфраструктури. Ці журнали подій є важливим джерелом інформації для виявлення операцій системи, поведінки користувачів, виявлення інцидентів безпеки та встановлення вразливих місць. Завдяки ретельному аналізу логів можна отримати глибше розуміння функціонування всієї інфраструктури, оптимізувати її продуктивність і своєчасно реагувати на потенційні загрози.

Процес аналізу журналів включає декілька важливих етапів. Першим із них є збір даних із численних джерел — від вебсерверів і баз даних до мережевих міжмережевих екранів і систем керування додатками. Далі виконується нормалізація, тобто уніфікація даних, яка дозволяє зіставити журнали з різних джерел у єдиному форматі. Для підвищення інформативності здійснюється збагачення даних, наприклад, додавання геолокаційної інформації за IP-адресами

або класифікація записів відповідно до індикаторів загроз. Після цього відбувається власне аналіз логів, який може виконуватися вручну, автоматизовано або з використанням машинного навчання. Результати цього аналізу дозволяють виявляти підозрілі дії, аномалії та потенційно шкідливу активність. Особливо важливим є етап кореляції, коли події з різних джерел об’єднуються для побудови повної картини загроз. Для полегшення сприйняття інформації широко застосовуються інструменти візуалізації, які перетворюють текстові логи у графіки, дашборди та звіти. Кінцевою метою всього цього процесу є виявлення атак або порушень безпеки та оперативне реагування на них.

Доповненням до логування виступають системи виявлення вторгнень (IDS), які забезпечують моніторинг мережі або хостів з метою фіксації аномальної активності. IDS можуть реалізовувати виявлення на основі підписів — за допомогою відомих шаблонів атак, на основі аномалій — шляхом зіставлення поведінки з нормативною моделлю, або на основі репутації — шляхом аналізу надійності джерел трафіку. Виявлена підозріла активність, як правило, реєструється або передається до адміністратора чи SIEM-системи.

На відміну від IDS, системи запобігання вторгненням (IPS) не лише виявляють шкідливу активність, але й здатні автоматично вживати заходів для її нейтралізації. Вони можуть блокувати підозрілий трафік у режимі реального часу, зупиняти виконання небезпечних процесів або змінювати правила маршрутизації. Завдяки цьому IPS-системи забезпечують більш активний захист мережі, виконуючи роль своєрідного фільтра, що зменшує навантаження на інші системи безпеки.

У контексті кібербезпеки об'єктів критичної інфраструктури, інтеграція механізмів логування з IDS/IPS-рішеннями дозволяє створити багаторівневу систему виявлення та запобігання інцидентам. Такий підхід є надзвичайно ефективним для забезпечення безперервного моніторингу та своєчасної відповіді на складні та цілеспрямовані кіберзагрози (рис.1.11).

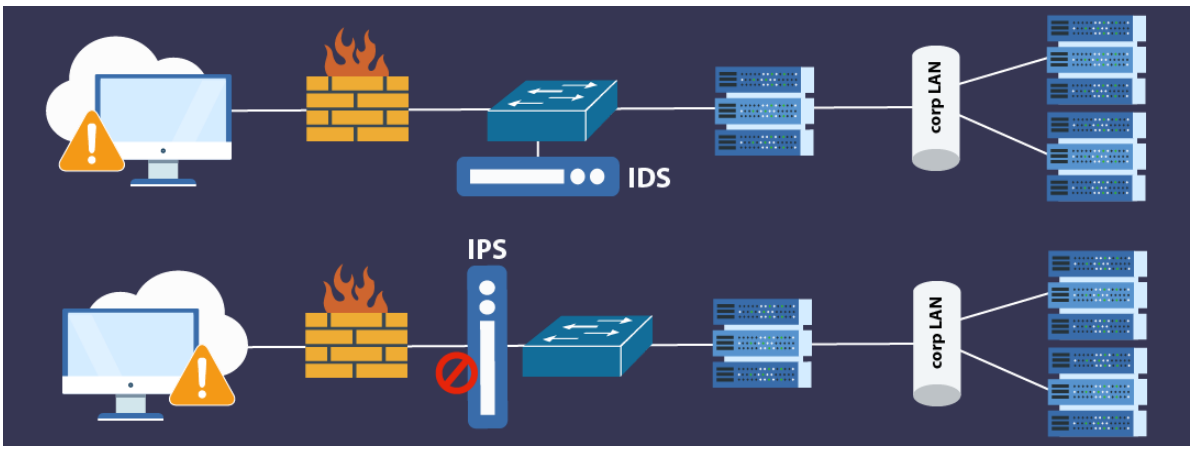


Рисунок 1.11 – Системи виявлення та запобігання вторгненням

Система запобігання вторгненням (IPS) встановлюється безпосередньо в потік мережевого трафіку між джерелом та призначенням, зазвичай розміщуючись одразу за брандмауером. Для виявлення загроз системи запобігання вторгненням використовують декілька методів:

– *базовані на сигнатурах.* Цей метод порівнює активність із сигнатурами відомих загроз. Недоліком цього методу є те, що він може зупинити лише раніше виявлені атаки і не зможе розпізнати нові;

– *базовані на аномаліях.* Цей метод здійснює моніторинг на предмет аномальної поведінки, порівнюючи випадкові зразки мережевої активності з базовим стандартом. Він є більш надійним, ніж моніторинг на основі сигнатур, але іноді може давати помилкові спрацювання. Деякі новіші та більш досконалі системи запобігання вторгненням використовують штучний інтелект та машинне навчання для підтримки моніторингу на основі аномалій;

– *базовані на політиках.* Цей метод менш поширений, ніж моніторинг на основі сигнатур або аномалій. Він використовує політики безпеки, визначені підприємством, і блокує дії, які порушують ці політики. Це потребує від адміністратора налаштування та конфігурації політик безпеки.

Після того, як IPS виявляє підозрілу активність, вона може вжити багато автоматичних дій, включаючи оповіщення адміністраторів, відкидання пакетів, блокування трафіку з адреси джерела або переривання з'єднання. Деякі системи запобігання вторгненням також використовують "honeypot" (пастку для

зловмисників) або підроблені цінні дані, щоб привабити атакуючих і не дозволити їм дістатися до цілей.(рис.1.12)

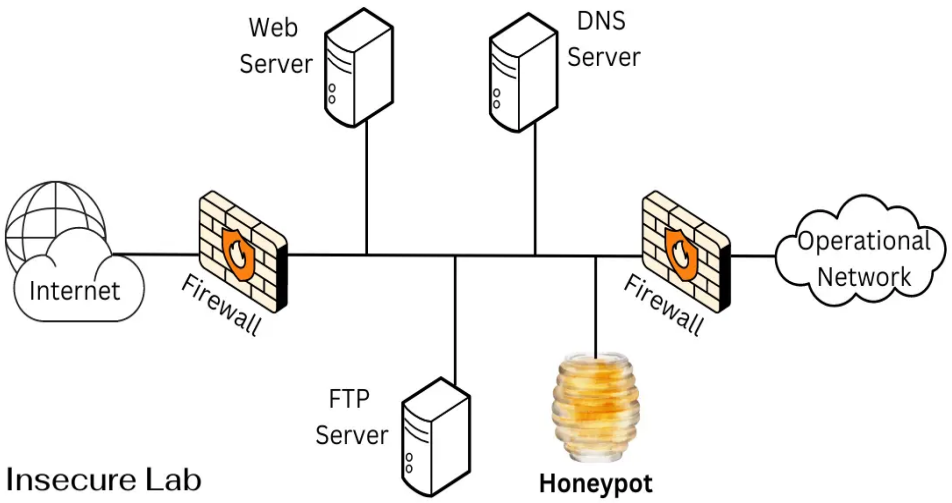


Рисунок 1.12– Приклад мережі з використанням Honeypot у кібербезпеці

Антивірусні програми та сигнатурне сканування – засновані на основі сигнатурного сканування є одним із найдавніших та найбільш поширених методів кіберзахисту, який широко використовується для виявлення відомого шкідливого програмного забезпечення. Цей підхід полягає у пошуку специфічних цифрових «відбитків» (сигнатур), які відповідають вже ідентифікованим зразкам вірусів, троянів, руткітів та інших форм malware.

Сигнатура — це унікальна послідовність байтів або хеш, який характеризує певну загрозу. База сигнатур постійно оновлюється постачальниками антивірусного ПЗ (як–от ESET, Avast, Bitdefender, Norton тощо), що дозволяє програмі зіставляти файли або процеси на комп’ютері з відомими зразками загроз. Як тільки антивірус знаходить збіг, файл позначається як шкідливий та ізолюється або видаляється (табл.1.1).

Таблиця 1.1 – Переваги та недоліки антивірусних програм

Переваги	Недоліки
Висока швидкість перевірки — дозволяє швидко виявляти вже відомі загрози.	Не виявляє нові або модифіковані загрози, які ще не мають сигнатур.
Низький рівень помилкових спрацювань — точне виявлення за відомими ознаками.	Неефективність проти безфайлових атак, які не залишають слідів у файловій системі.
Простота реалізації — зрілий, добре відпрацьований підхід, доступний для всіх ОС.	Потреба в постійному оновленні бази сигнатур, особливо критично в ізольованих системах.

Попри ці обмеження, антивірусне ПЗ залишається базовим рівнем захисту і є невід'ємною частиною багаторівневої системи безпеки, зокрема в критичній інфраструктурі. Воно ефективно усуває масові загрози, забезпечує відповідність політикам безпеки, а також може бути частиною ширших платформ захисту, наприклад, EDR (Endpoint Detection and Response).

У поєднанні з іншими методами, такими як поведінковий аналіз, машинне навчання, кореляція подій або фреймворки MITRE ATT&CK, сигнатурне сканування виконує роль першого фільтру безпеки, який дозволяє зменшити навантаження на системи виявлення складніших загроз.



Рисунок 1.14 – Схема сучасних методів моніторингу

Системи управління інформаційною безпекою та подіями (SIEM) є ключовими інструментами в арсеналі сучасної кібербезпеки, які забезпечують централізований збір, зберігання, аналіз та кореляцію подій безпеки з різних джерел. Їх основна мета — виявлення загроз у режимі реального часу, ефективне реагування на інциденти, розслідування подій та підготовка звітності для внутрішніх і зовнішніх контролюючих органів (рис.1.15).

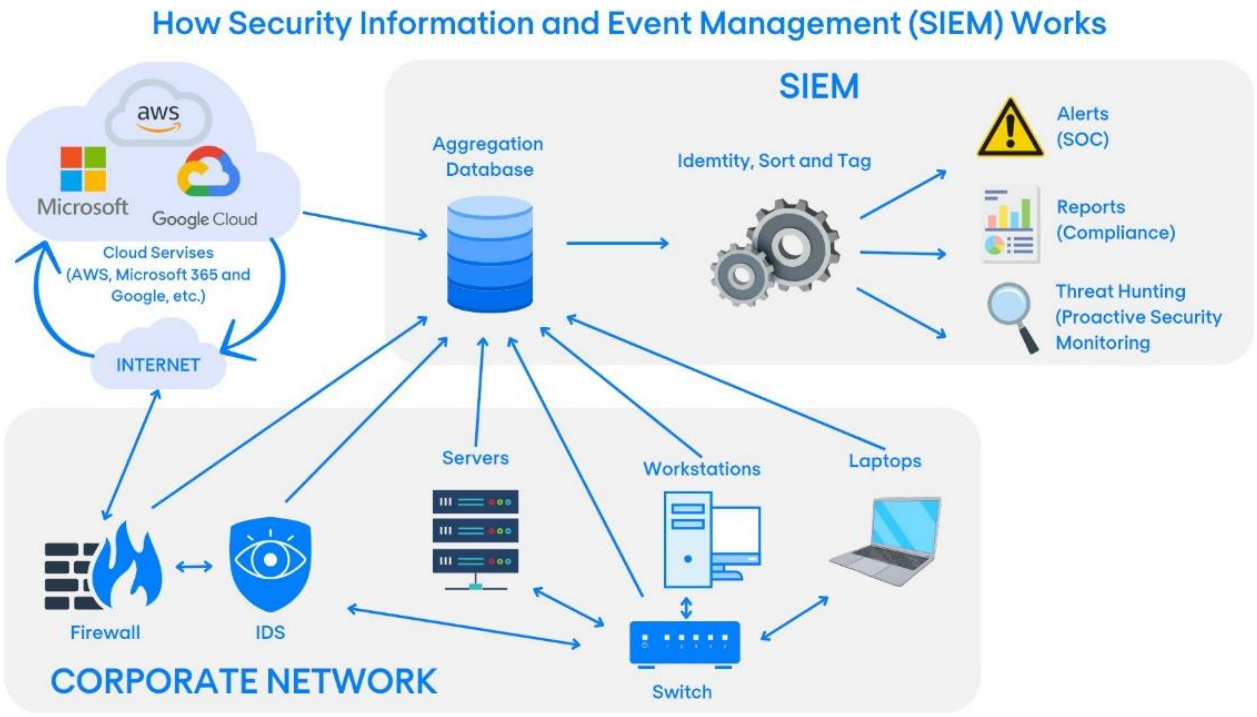


Рисунок 1.15– приклад схеми роботи SIEM рішення

Системи SIEM здатні обробляти величезні обсяги даних, що надходять із різних компонентів IT-інфраструктури — серверів, кінцевих пристроїв, мережевого обладнання, систем автентифікації, міжмережевих екранів, антивірусів тощо. Для цього використовуються агенти, які здійснюють первинну обробку та передачу логів у центральну систему. Крім того, сучасні SIEM-рішення можуть інтегруватися з хмарними платформами та іншими нестандартними джерелами інформації.

Однією з ключових переваг SIEM є здатність до кореляції подій — об’єднання на перший погляд незначних інцидентів у широку картину, яка вказує на потенційну загрозу. Це дозволяє виявляти складні, приховані атаки, що

залишають у журналах лише розрізнені сліди. Для цього використовуються алгоритми штучного інтелекту та машинного навчання, які аналізують поведінкові патерни, виявляють аномалії та пріоритезують події за критичністю.

SIEM-системи є висококонфігурованими: аналітики можуть налаштовувати власні правила виявлення загроз, задавати допустимі межі активності та автоматизувати відповідні дії. Це забезпечує гнучку інтеграцію в корпоративне середовище та тісну взаємодію з іншими засобами захисту, такими як IDS/IPS, EDR чи DLP.

Однак ефективне впровадження SIEM вимагає значних ресурсів. Потік даних, який генерується всіма компонентами інфраструктури, потребує високої пропускної здатності мережі, великої обчислювальної потужності та надійного сховища. Тому перед розгортанням необхідно ретельно оцінити готовність IT-інфраструктури.

SIEM забезпечує прозорість інформаційного середовища, дозволяючи аналітикам бачити цілісну картину кібербезпеки, відслідковувати вектори атак, визначати джерела компрометації та швидко вживати заходів. Компоненти системи допомагають не лише виявляти та локалізовувати інциденти, а й формувати детальні звіти для внутрішнього аналізу, аудитів і регуляторів. Такі звіти часто є необхідними для сертифікації інформаційної безпеки та дотримання міжнародних стандартів (наприклад, ISO/IEC 27001, GDPR, PCI DSS).

Найбільшого поширення SIEM-рішення набули у фінансовому секторі, на великих підприємствах, а також в організаціях із розгалуженою географічною структурою. Завдяки потужному функціоналу та здатності адаптуватися до специфіки конкретного бізнесу, вони відіграють провідну роль у побудові комплексної системи кіберзахисту. [12]

Безперервний моніторинг інформаційної безпеки (ISCM) — це процес постійного збирання, аналізу та оцінки даних щодо стану безпеки інформаційних систем, з метою своєчасного виявлення загроз, вразливостей і аномальної активності. Цей підхід є ключовим елементом у забезпеченні стійкої кібербезпеки, особливо в критичних інфраструктурних системах, де навіть короткочасний

інцидент може мати серйозні наслідки.

На відміну від періодичних перевірок, ISCM забезпечує реальний або майже реальний час реагування, що дозволяє виявляти загрози на ранніх етапах. Це досягається за рахунок автоматизованих засобів моніторингу, які інтегруються з усіма компонентами IT–інфраструктури — мережами, кінцевими точками, серверами, системами управління подіями тощо. Основна ідея полягає у створенні безперервного потоку даних, який аналітики безпеки або системи на основі машинного навчання можуть обробляти для прийняття оперативних рішень.

Ключовими перевагами ISCM є своєчасне виявлення нових вразливостей, оцінка відповідності стандартам безпеки, а також зниження часу на реагування на інциденти. Крім того, ISCM дає змогу підтримувати постійну видимість загального стану безпеки та адаптувати політики захисту до змін у середовищі або загрозах (рис. 1.16)

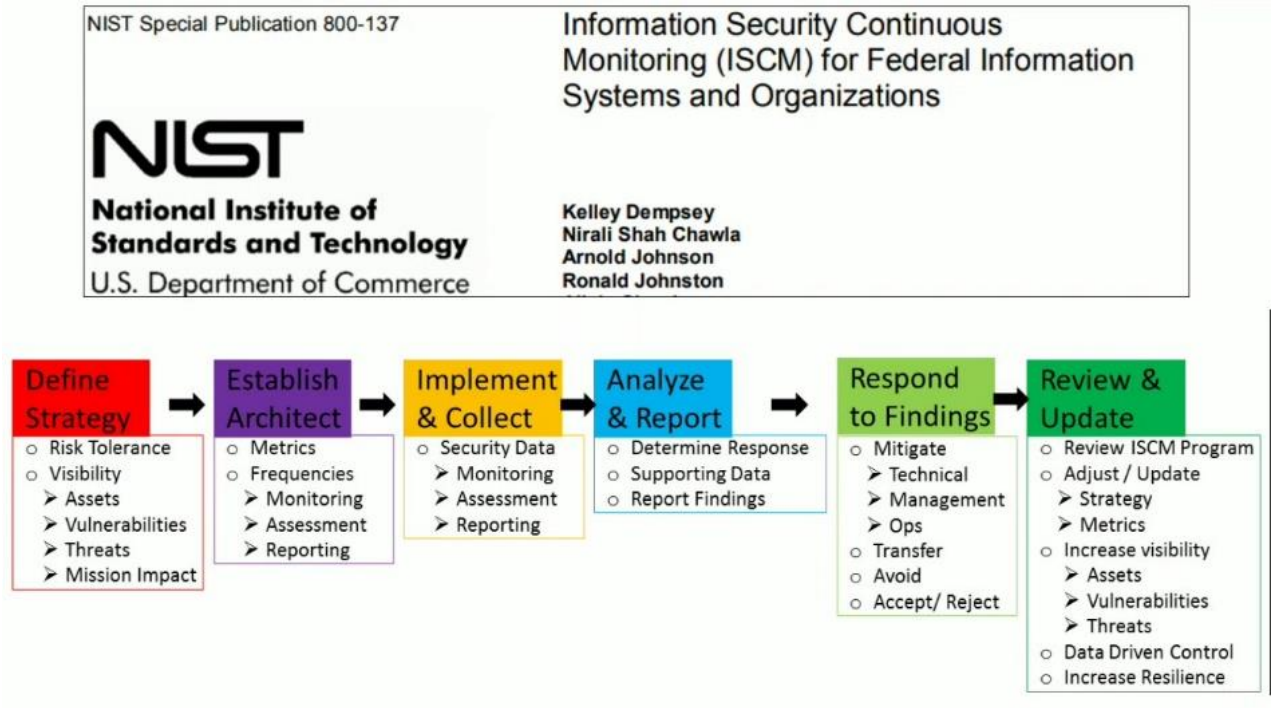


Рисунок 1.16 – Схема безперервного моніторингу безпеки в інформаційних системах

У межах національних і міжнародних практик ISCM часто є обов’язковим компонентом у рамках фреймворків управління ризиками, таких як NIST RMF

(Risk Management Framework), де підкреслюється важливість циклічного збору, оцінки та вдосконалення засобів безпеки.

Поведінковий аналіз та машинне навчання в сучасних системах кібербезпеки є потужними інструментами для виявлення складних та прихованих загроз, які можуть залишатися непоміченими при використанні лише традиційних підходів. Одним із найбільш ефективних рішень у цій сфері є технологія UEBA (User and Entity Behavior Analytics) — аналітика поведінки користувачів і об'єктів.

UEBA використовує методи машинного навчання та статистичної обробки даних для створення базових моделей нормальної поведінки кожного користувача, пристрою, облікового запису чи сервісу в системі. Ці моделі ґрунтуються на аналізі великої кількості параметрів: час входу в систему, геолокація, частота доступу до файлів, характер мережевої активності, використання привілеїв, послідовність команд тощо. Такий підхід дозволяє сформувати повноцінний поведінковий профіль для кожного суб'єкта в інфраструктурі.

Коли активність користувача або пристрою відхиляється від типового шаблону, система фіксує аномалію та повідомляє аналітиків безпеки або автоматично ініціює захисні дії. Наприклад, якщо співробітник, який зазвичай працює з бухгалтерськими файлами вдень, раптово починає завантажувати великі об'єми даних уночі з невідомої IP–адреси — така активність буде визнана підозрілою.

Основна перевага UEBA полягає в тому, що вона не покладається на попередньо відомі сигнатури загроз чи фіксовані правила. Замість цього вона виявляє нові, нульові або внутрішні атаки, включно з компрометацією облікових записів, lateral movement, зловживанням правами доступу, витоком даних, внутрішнім шахрайством тощо[13].

UEBA зазвичай інтегрується з SIEM–системами або працює як окремий модуль аналітики. У поєднанні з іншими засобами (ML–моделями, правилами кореляції, контекстною інформацією про ризики) вона забезпечує глибший рівень ситуаційної обізнаності та дозволяє організаціям реагувати на інциденти не лише швидше, а й точніше.

Технології XDR (Extended Detection and Response) – це еволюційний крок у сфері кібербезпеки, який спрямований на об’єднання, автоматизацію та покращення виявлення загроз і реагування на них в усій інфраструктурі організації. На відміну від ізольованих інструментів, таких як EDR, NDR чи класичні SIEM, XDR забезпечує централізований підхід до захисту всієї екосистеми – від кінцевих пристроїв до хмарних середовищ і мережевого трафіку[14].

Основна ідея XDR полягає в тому, щоб агрегувати дані з кількох джерел безпеки – зокрема з EDR (Endpoint Detection and Response), що відповідає за моніторинг активності на кінцевих точках (ПК, ноутбуки, сервери), NDR (Network Detection and Response), який аналізує мережевий трафік, та інших джерел, включаючи хмарні сервіси, поштові системи, ідентифікаційні сервіси тощо. Ці дані об’єднуються в єдиному середовищі для кращої кореляції, аналітики та швидкої реакції.

XDR використовує машинне навчання, поведінкову аналітику та автоматизовану обробку загроз, щоб не лише виявляти атаки, а й забезпечувати повний контекст подій, визначати причинно–наслідкові зв’язки та пропонувати рекомендовані дії або навіть виконувати автоматизовану реакцію.

На відміну від SIEM, який переважно орієнтований на збір та зберігання журналів, XDR зосереджується на практичній безпеці – виявленні, аналізі та реагуванні. Він мінімізує "шум" шляхом пріоритизація подій, скорочує час на виявлення та усунення загроз, а також забезпечує єдине вікно видимості (single pane of glass) для аналітиків.

У контексті критичної інфраструктури XDR особливо цінний тим, що дозволяє оперативно виявляти складні, багатоступеневі атаки (APT), забезпечує координовану відповідь на інциденти та знижує навантаження на команди реагування завдяки автоматизації та інтегрованій аналітиці.

Також варто розглянути, які типи XDR–рішень існують. Умовно їх можна розділити на два типи – Native та Open (рис.1.17)

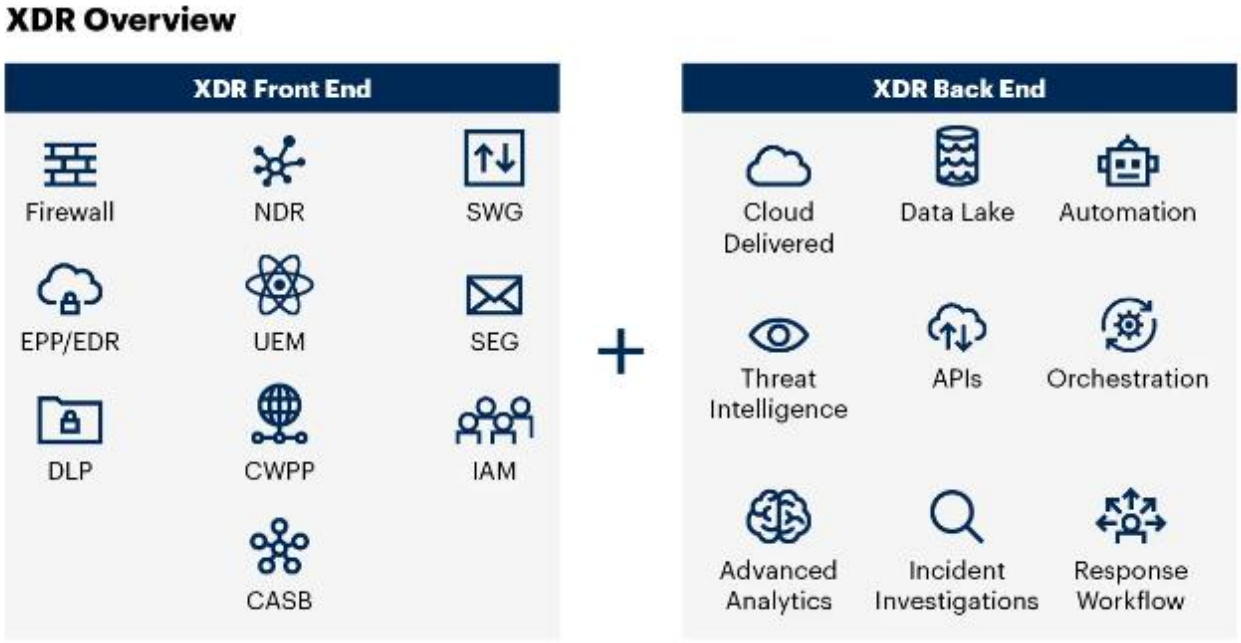


Рисунок 1.17 – Типи XDR

Native XDR повністю покладається на рішення від одного вендора, водночас жертвуючи інтеграціями з іншими постачальниками. Всі інтеграції та збиральники даних орієнтовані тільки на рішення свого виробника і жодним чином не можуть взаємодіяти зі сторонніми вендорами.

Своєю чергою, Open XDR орієнтований на інтеграцію зі сторонніми постачальниками, збирання даних та реагування на загрози, водночас він використовує широкий спектр рішень безпеки від різних вендорів. [15]

MITRE ATT&CK – надає уніфіковану структуру для опису поведінки противника, яка може бути використана в системах безпеки для побудови логіки кореляції, визначення слабких місць у захисті, розробки сценаріїв тестування та формування орієнтованих політик виявлення. База знань ATT&CK використовується як основа для розробки конкретних моделей та методологій загроз у приватному секторі, уряді та спільноті розробників продуктів і послуг кібербезпеки. Застосування ATT&CK дозволяє переходити від простого лог–аналізу до поведінкової аналітики, де кожна подія мапується на потенційну техніку або тактику атаки[16].

Основні складова фреймворку MITTRE ATT&CK (рис.1.18) включає в себе:

– матриці тактик і технік – цей блок підкреслює основну частину MITRE ATT&CK – ієрархічно організовані матриці, що описують тактики (високорівневі цілі зловмисників) та конкретні техніки (способи досягнення цих цілей);

– джерела даних – цей елемент відображає інформацію про типи даних, які можуть бути використані для виявлення та аналізу технік ATT&CK;

– імітація ризиків – цей блок представляє інформацію про можливі заходи безпеки для запобігання, виявлення або реагування на тактики та техніки ATT&CK;

– злочинні угруповання – цей елемент містить інформацію про відомі кіберзлочинні угруповання та їхні характерні тактики, техніки та процедури (TTPs);

– використовуване ПЗ – цей блок описує конкретне програмне забезпечення, яке зловмисники можуть використовувати для реалізації своїх технік;

– хакерські кампанії – цей елемент пов'язує різні тактики, техніки та угруповання для опису цілісних атак.



Рисунок 1.18 – Структурна схема складової фреймворку MITRE ATT&CK

2. АНАЛІЗ АВТОМАТИЗОВАНИХ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

2.1 Архітектура системи автоматизованого моніторингу кібербезпеки

У сучасному світі, де кіберзагрози стають дедалі витонченішими, критична інфраструктура — така як енергетика, транспорт, водопостачання, охорона здоров'я та банківська сфера — потребує надійних засобів захисту. Одним із ключових компонентів такого захисту є автоматизовані системи моніторингу кібербезпеки (ASMS) (рис.2.1), які забезпечують безперервне спостереження за станом інформаційних систем, своєчасне виявлення загроз та ефективне реагування на них.

Архітектура таких систем зазвичай складається з декількох взаємопов'язаних рівнів. На першому рівні розташовуються джерела даних, до яких належать мережеві пристрої, кінцеві точки, сервери, програмні додатки та журнали подій. Вони є первинними постачальниками інформації про події, що відбуваються в інформаційному середовищі підприємства. Для об'єктів критичної інфраструктури надзвичайно важливо, щоб дані з таких джерел передавалися захищеними каналами зв'язку, а самі джерела були ізольовані в окремих мережевих сегментах.

Другим важливим компонентом є система збору та агрегації даних, найчастіше представлена SIEM–платформою (Security Information and Event Management). Вона виконує збір інформації з усіх доступних джерел, її нормалізацію, фільтрацію та зберігання. SIEM забезпечує єдину точку спостереження для операторів кібербезпеки. На об'єктах з обмеженим доступом до інтернету, що характерно для критичної інфраструктури, часто застосовуються on–premise рішення, які не залежать від зовнішніх хмарних сервісів.

На третьому етапі відбувається аналіз та обробка даних, під час якого за допомогою механізмів кореляції виявляються зв'язки між подіями з різних джерел. Система здатна виявляти аномальну поведінку користувачів та пристроїв,

використовуючи моделі поведінкового аналізу (UEBA). Одним із найефективніших підходів у цьому напрямі є використання фреймворку MITRE ATT&CK, який дозволяє співвідносити виявлені активності зі знаними тактиками й техніками супротивника. У ряді випадків застосовується також машинне навчання для ідентифікації нових або невідомих загроз.

Завершальним компонентом архітектури є система реагування на інциденти, яка може працювати як у ручному, так і в автоматичному режимі. Вона здійснює блокування підозрілих облікових записів, ізоляцію заражених вузлів, сегментацію мережі та інші захисні дії. Для підвищення ефективності цієї функції часто використовується SOAR–платформа (Security Orchestration, Automation and Response), яка дозволяє автоматизувати процеси реагування відповідно до заздалегідь визначених сценаріїв (playbooks).



Рисунок 2.1 – Блок–схема системи автоматизованого моніторингу

2.2 Типи та функціональні рішення автоматизованих систем моніторингу кіберзагроз

У сучасних умовах захисту критичної інформаційної інфраструктури особливе місце займають автоматизовані системи моніторингу кіберзагроз (ASMS), що реалізують безперервне спостереження, аналіз та реагування на загрози в реальному часі. Залежно від завдань і архітектури, такі системи поділяються на кілька основних типів, кожен з яких має своє функціональне призначення (табл. 2.1) та технологічні особливості.

Одним із ключових типів ASMS є SIEM–системи (Security Information and Event Management), які поєднують функції збору, агрегації, кореляції та зберігання даних з подальшим аналізом подій безпеки. Вони забезпечують централізоване моніторинг середовища, що дозволяє швидко виявляти підозрілі активності та будувати зв’язки між розрізненими подіями. Типовими прикладами таких рішень є Splunk, IBM QRadar, ArcSight, ELK Stack (у поєднанні з Wazuh).

Іншим напрямом є EDR–системи (Endpoint Detection and Response), які фокусуються на кінцевих пристроях (endpoint) і дозволяють виявляти підозрілі процеси, зміни у файловій системі, спроби ескалації привілеїв тощо. Сучасні EDR–рішення, як–от CrowdStrike Falcon або Microsoft Defender for Endpoint, мають у своєму складі компоненти з автоматизованого реагування на загрози та вбудовану аналітику[17].

IDS/IPS–системи (Intrusion Detection/Prevention Systems) також є важливим елементом архітектури ASMS. Вони здійснюють глибокий аналіз мережевого трафіку для виявлення шкідливої активності в режимі реального часу. Zeek (раніше Bro) — це приклад сучасної IDS–системи з відкритим кодом, що дозволяє гнучко налаштовувати політики моніторингу [18].

Крім того, останніми роками активно розвиваються UEBA–рішення (User and Entity Behavior Analytics), що застосовують поведінковий аналіз користувачів і пристроїв. Вони виявляють аномалії, які не завжди фіксуються класичними

правилами сигнатурного типу. UEBA базується на машинному навчанні, статистичних моделях та профілюванні поведінки.

У свою чергу, SOAR–платформи (Security Orchestration, Automation and Response) є інструментом автоматизації рутинних процесів та реакцій на інциденти. Вони дозволяють реалізовувати сценарії реагування (playbooks), об’єднувати роботу SIEM, EDR та інших систем безпеки, прискорюючи цикл виявлення й реагування [19].

Таким чином, сучасні ASMS не є однорідними: це комплексні рішення, які поєднують функціональність кількох компонентів. У залежності від рівня загроз, типу організації та особливостей інфраструктури можуть використовуватись як спеціалізовані продукти, так і гібридні рішення, що інтегрують декілька функціональних типів в єдину екосистему моніторингу кібербезпеки.

Таблиця 2.1– Порівняльна таблиця функціональних можливостей SIEM, EDR, IDS/IPS та UEBA

Характеристика	SIEM (Security Information and Event Management)	EDR (Endpoint Detection and Response)	IDS/IPS (Intrusion Detection/Prevention System)	UEBA (User and Entity Behavior Analytics)
Основна функція	Збір, нормалізація, агрегація та аналіз журналів подій безпеки з різних джерел (мережі, кінцеві точки, програми тощо) для виявлення загроз, інцидентів та забезпечення відповідності.	Постійний моніторинг та збір даних на кінцевих точках (комп'ютери, сервери) для виявлення, аналізу та реагування на складні та приховані загрози.	Моніторинг мережевого трафіку на предмет підозрілої активності. IDS виявляє загрози та попереджає, IPS може автоматично блокувати або запобігати виявленим загрозам.	Аналіз поведінки користувачів та інших сутностей (наприклад, пристроїв, додатків) для виявлення аномалій, які можуть свідчити про внутрішні або зовнішні загрози.

Продовження таблиці

Характеристика	SIEM (Security Information and Event Management)	EDR (Endpoint Detection and Response)	IDS/IPS (Intrusion Detection/Prevention System)	UEBA (User and Entity Behavior Analytics)
Джерела даних	Журнали подій безпеки (логи), дані про мережевий трафік, інформація про вразливості, контекстні дані (активи, користувачі).	Детальні дані з кінцевих точок: процеси, мережеві з'єднання, файлова активність, реєстр, поведінка користувачів.	Мережевий трафік (пакети даних), журнали подій (деякі системи).	Журнали подій, дані про автентифікацію, активність користувачів у різних системах та програмах, мережевий трафік (у контексті поведінки).
Фокус виявлення	Широкий спектр загроз на рівні інфраструктури, кореляція подій для виявлення складних атак, відповідність вимогам.	Складні, цілеспрямовані атаки, шкідливе ПЗ, дії зловмисників на рівні кінцевих точок, пост–експлуатація.	Відомі сигнатури атак, аномалії в мережевому трафіку, спроби експлойтів.	Внутрішні загрози (інсайдери), скомпрометовані облікові записи, аномальна поведінка, що може свідчити про атаку.
Реагування на інциденти	Надання контексту для аналізу інцидентів, централізоване управління інцидентами, автоматизовані робочі процеси реагування (в деяких випадках).	Розширені можливості реагування на кінцевих точках: ізоляція, блокування процесів, видалення файлів, відновлення після атаки, збір криміналістичних даних.	Блокування або запобігання шкідливому трафіку (IPS), генерація сповіщень (IDS).	Надання контексту для розслідування аномалій, інтеграція з іншими системами безпеки для автоматизованого реагування.
Сфера застосування	Централізований моніторинг безпеки великих та складних IT–інфраструктур, забезпечення відповідності нормативним вимогам.	Організації, які стикаються зі складними та цілеспрямованими атаками, потребують глибокого розуміння активності на кінцевих точках та ефективного реагування.	Захист периметра мережі, виявлення та блокування відомих та потенційних мережевих атак.	Виявлення внутрішніх загроз, виявлення скомпрометованих облікових записів, аналіз поведінки користувачів для запобігання шахрайству та витоку даних.

2.3 Застосування фреймворку MITRE ATT&CK

У сучасних автоматизованих системах моніторингу кіберзагроз ключову роль відіграє не лише збір і обробка інформації, а й здатність інтерпретувати події в контексті відомих тактик і технік зловмисників. У цьому аспекті ефективним інструментом є фреймворк MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), який став стандартом у сфері кіберзахисту.

MITRE ATT&CK — це комплексна база знань, яка використовується для розуміння, класифікації та аналізу поведінки зловмисників у сфері кібербезпеки. Назва фреймворку розшифровується як *Adversarial Tactics, Techniques, and Common Knowledge* та включає систематизований опис тактик, технік і процедур (TTPs), що застосовуються у реальних атаках. Завдяки цьому організації можуть ефективніше розпізнавати потенційні загрози, формувати стратегії захисту й усувати вразливі місця у своїх IT-системах[20].

Фреймворк MITRE ATT&CK надає фахівцям спільну мову та уніфіковану структуру для аналізу та обміну інформацією про загрози. Він постійно оновлюється на основі аналізу реальних інцидентів, що робить його надзвичайно актуальним і корисним для організацій, які прагнуть до проактивного підходу в захисті інформаційної інфраструктури.

Завдяки глибокій деталізації TTP, MITRE ATT&CK сприяє моделюванню атак, оцінці поточних рівнів захисту та вдосконаленню механізмів виявлення загроз. Одним із ключових переваг фреймворку є його здатність покращувати взаємодію між командами безпеки — як у межах організації, так і між різними структурами. Це досягається за рахунок стандартизації опису кіберзагроз і підтримки сумісності з численними інструментами, рішеннями та платформами безпеки. У результаті, центри моніторингу безпеки (SOC) та команди реагування на інциденти можуть координувати дії ефективніше, швидше виявляти індикатори компрометації та впроваджувати цільові заходи реагування.

Крім того, MITRE ATT&CK також є цінним ресурсом для навчання та

програм підвищення обізнаності з безпеки. Важливість і вплив MITRE ATT&CK(табл.2.3):

- розуміння та моделювання поведінки учасників загрози;
- визначте вразливі місця та розставте пріоритети;
- розробка та оптимізація оборонних стратегій;
- посилення зв’язку та співпраці між командами безпеки;
- полегшення інтеграції між інструментами та рішеннями безпеки;
- покращення можливостей полювання на загрози.

Таблиця 2.3– Переваги впровадження MITRE ATT&CK у різних напрямках кіберзахисту

Площа	Ефект	Пояснення
Розвідка загроз	Розширений аналіз	Краще розуміти та аналізувати TTP учасників загроз.
Оборонні стратегії	Оптимізований захист	MITPE ATT&CK Розробка та впровадження механізмів захисту на основі.
Інструменти безпеки	Ефективна оцінка	Оцініть і порівняйте ефективність інструментів і рішень безпеки.
Освіта та обізнаність	Підвищення свідомості	Надання цінного ресурсу для програм навчання та підвищення обізнаності з кібербезпеки.

Але також в процесі моделювання загроз MITPE ATT&CK Під час використання фреймворку можна припуститися деяких типових помилок. Усвідомлення та уникнення цих помилок підвищує ефективність моделювання загроз і зміцнює безпеку організації. Однією з найпоширеніших помилок є недостатнє виділення часу та ресурсів на процес моделювання загроз. Швидкий і поверхневий аналіз може пропустити важливі вектори загрози.

Ще одна велика помилка полягає в тому, що розглядати моделювання загроз як одноразову діяльність і нехтувати його регулярним оновленням. Оскільки ландшафт загроз постійно змінюється, моделі загроз також повинні йти в ногу з цими змінами. Також поширеною помилкою є незалучення до процесу

моделювання загроз людей з різних відділів і сфер знань. Об’єднання різних точок зору, таких як експерти з кібербезпеки, мережеві адміністратори та розробники додатків, дає змогу більш комплексно та ефективніше моделювати загрози.

Неправильне розуміння фреймворку та його неправильне застосування також є поширеною помилкою. Поверхневе використання без розуміння всіх тонкощів фреймворку може призвести до неповної або неправильної класифікації загроз. Тому що, MITPE ATT&CK Надзвичайно важливо пройти адекватну підготовку та правильно застосовувати структуру. У наведеному нижче списку є деякі важливі речі, яких слід уникати:

– ігнорування інформації про загрози;

– не адаптація захисних стратегій на основі результатів моделювання загроз;

– недостатньо докладні сценарії загроз;

– нездатність визначити потенційні поверхні атаки. [21]

Матриці MITRE ATT&CK складаються з двох сутностей: тактик та технік. Тактики визначають мету, якої атакуючі хочуть досягти шляхом використання певних технік та процедур, які також називають підтехніками. Все це разом позначається абревіатурою TTP (Tactics, Techniques and Procedures). Кожна тактика або техніка має унікальний ідентифікатор, який використовується для простоти роботи з матрицею. Зокрема, тактики позначаються кодом виду "TAXXXX", де XXXX – цифрове позначення номера тактики. Наприклад, TA0043 – розвідка (рис.2.1), а TA0007 – пересування інфраструктурою.

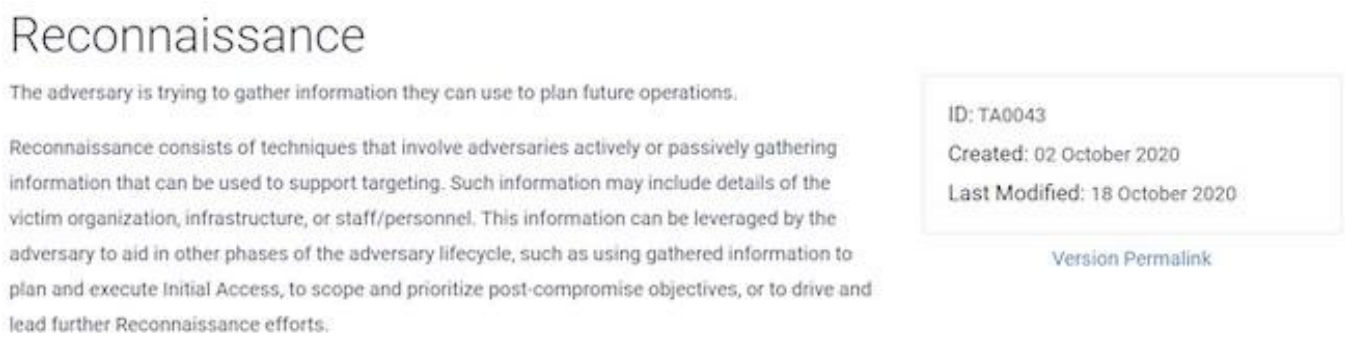


Рисунок 2.1 – Картка тактики TA0043

Ідентифікатори технік мають вигляд TVVVV.YYY, де VVVV — цифрове позначення номера техніки, а YYY — цифрове позначення підтехніки. Наприклад, T1055.012 (рис.2.2) "Впровадження в порожній процес" відноситься до техніки T1055 "Впровадження коду в процеси".



Рисунок 2.2– Картка техніки T1055.012

Для кожної техніки та підтехніки на сайті MITRE є детальний опис принципу її використання зловмисниками та програм, що застосовуються для цього, названі методи зниження ризику та способи відстеження спроб її реалізації (рис.2.3)

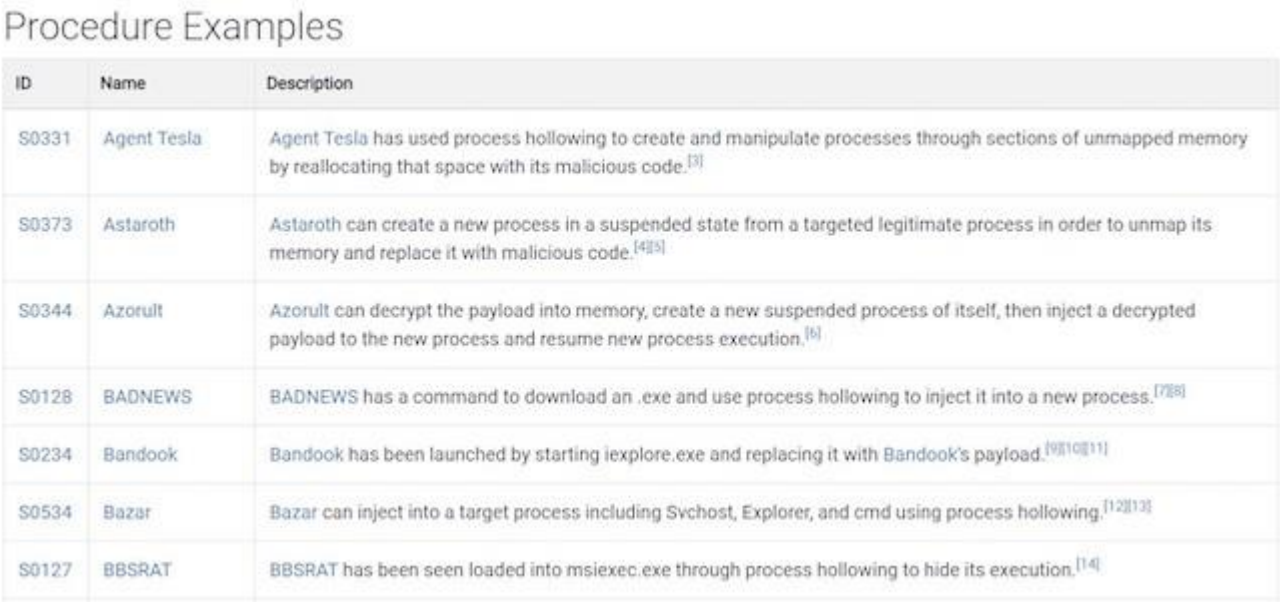


Рисунок 2.3 – Картка техніки T1055.012 з описом програм, що використовуються для її реалізації

Матриця MITRE ATT&CK є надзвичайно цінним джерелом знань для фахівців з інформаційної безпеки, оскільки містить детальний опис тактик, технік та процедур (TTPs), що використовуються зловмисниками. Вона слугує основою для аналізу, виявлення та протидії загрозам у контексті реальної інфраструктури. Однак уніфікованого підходу до її використання не існує — практичне застосування матриці залежить від доступних людських та технічних ресурсів організації[22].

Одним із найефективніших способів використання матриці є всебічне моделювання можливостей проникнення в інформаційну інфраструктуру підприємства. Такий підхід охоплює повний життєвий цикл атаки: від етапу розвідки до етапу впливу (наприклад, виведення системи з ладу або викрадення даних). Послідовно розглядаючи всі релевантні техніки та підтехніки, аналітики можуть залишити у фокусі лише ті, що потенційно застосовні до конкретної організаційної архітектури. Подальший аналіз зосереджується на ідентифікації вразливих місць та впровадженні відповідних заходів реагування, що дозволяє знизити ризики успішної реалізації відповідних сценаріїв атак.

Застосування такого підходу потребує скрупульозної, системної роботи та значних трудовитрат, однак дає змогу досягти високого рівня обізнаності про поточний стан безпеки. Жоден з можливих векторів атаки при цьому не залишається поза увагою, що особливо важливо для організацій із критичною інфраструктурою або підвищеними вимогами до кібербезпеки.

Для полегшення практичного використання матриці MITRE розробила спеціальний інструмент — MITRE ATT&CK Navigator (рис. 2.4). Цей вебзастосунок дозволяє інтерактивно працювати з матрицею, фільтрувати техніки за відповідністю до конкретних платформ, груп APT або програмного забезпечення, а також створювати власні шари (layers) із зазначенням рівня ризику, наявних заходів виявлення та відповідності контролям безпеки. Таким чином, ATT&CK Navigator сприяє візуалізації й аналізу ризиків, полегшуючи процес прийняття рішень щодо підвищення захищеності IT-інфраструктури[23].

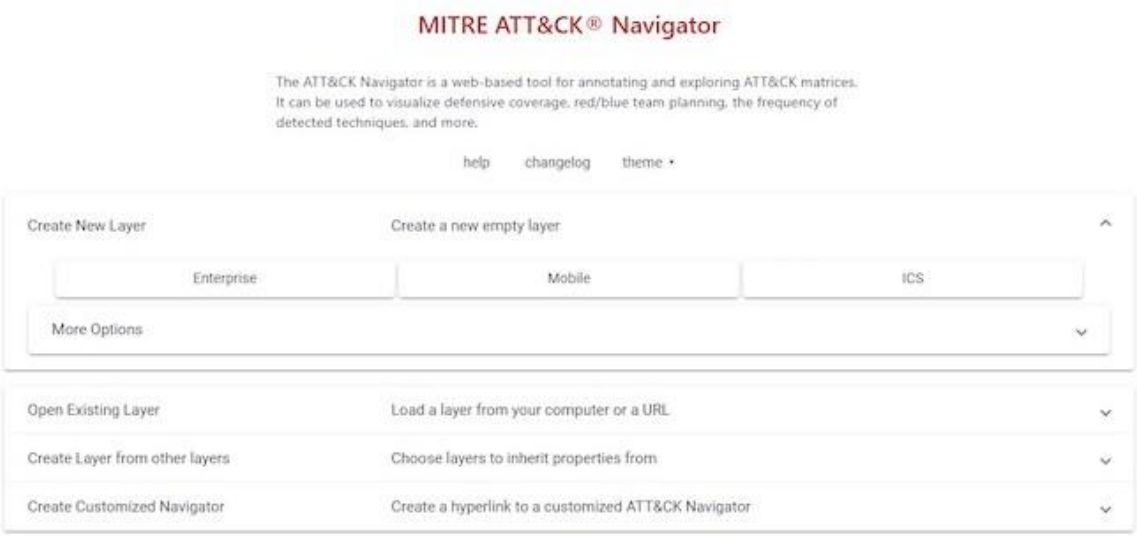


Рисунок 2.4 – Інтерфейс ATT&CK Navigator

Результат моделювання (рис.2.5) можна завантажити у форматі XLS, а шар, у якому відбувалося моделювання, – у форматі JSON.

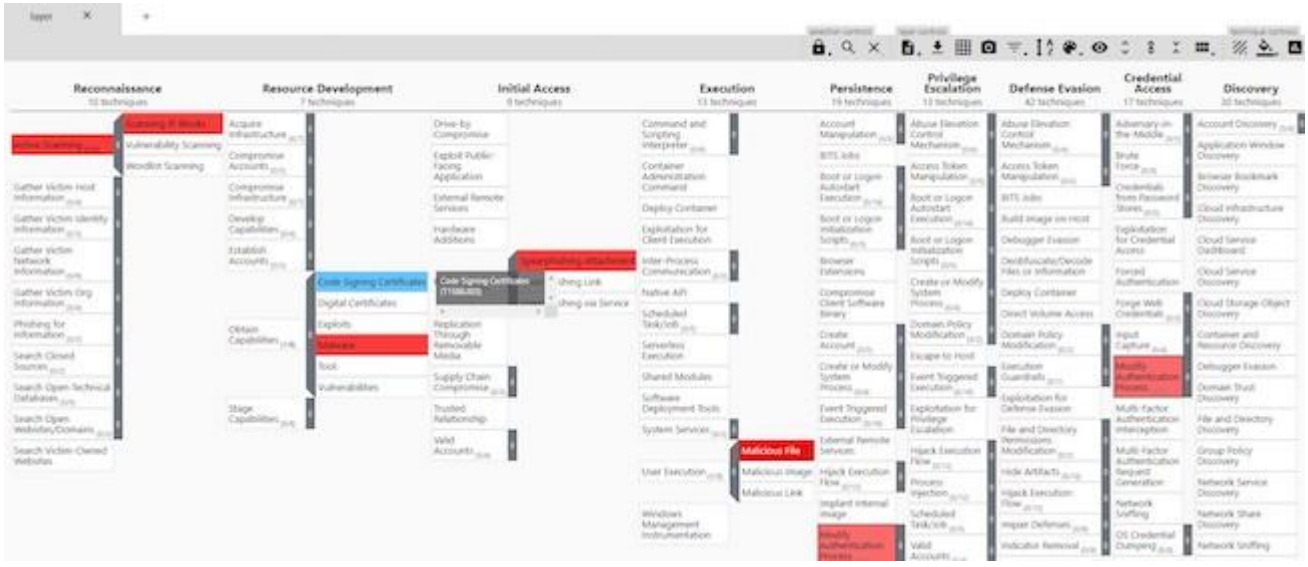


Рисунок 2.5 – Процес моделювання векторів кібератак за допомогою ATT&CK Navigator

2.4 Автоматизовані методи виявлення кіберзагроз

У сучасних умовах кіберзагрози стають дедалі складнішими, багаторівневими та цілеспрямованими. Це зумовлює необхідність використання автоматизованих методів для їх виявлення, які дозволяють не лише оперативно ідентифікувати загрози, але й здійснювати їх глибокий аналіз, класифікацію та в деяких випадках — автоматичне реагування.

Серед основних підходів, що застосовуються в автоматизованих методах виявлення, можна виділити:

Сигнатурний аналіз, є одним із найпоширеніших методів у кібербезпеці. По суті, це метод, який ідентифікує загрози, шукаючи відомі закономірності або «сигнатури» в даних або системній активності. Ці сигнатури попередньо визначені та зберігаються в базі даних, що дозволяє системам виявлення легко порівнювати вхідні дані з ними. Виявлення на основі сигнатур працює так, ніби це система безпеки, яка перевіряє вхідні дані на відповідність відомому шаблону загрози. Припустимо, що організація отримала фішинговий електронний лист, де шкідливе вкладення містить певний унікальний код, помічений під час попередніх атак. Система виявить цей код, тим самим одразу позначивши електронний лист як небезпечний, блокуючи його отримання. Такий підхід забезпечує швидку ідентифікацію та стримування таких загроз на основі встановлених сигнатур, що робить його важливим рівнем кібербезпеки.

Ось як працює процес виявлення на основі сигнатур (рис.2.6):

– Крок 1. Генерація сигнатури: Коли виявляється нова загроза, така як вірус або шкідливе програмне забезпечення, дослідники вивчають її поведінку та генерують унікальний відбиток пальця або сигнатуру. Це може бути певний шаблон коду або послідовність дій, які він виконує.

– Крок 2. База даних підписів: Цей підпис фактично зберігається в центральній базі даних. Інструменти безпеки, такі як антивірусне програмне забезпечення або системи виявлення вторгнень перевіряють цю базу даних на

наявність загроз.

– Крок 3. Сканування та зіставлення: Коли дані або дії проходять через систему, цей інструмент безпеки сканує їх та намагається зіставити зі збереженими сигнатурами. У разі збігу система позначає їх як шкідливі.

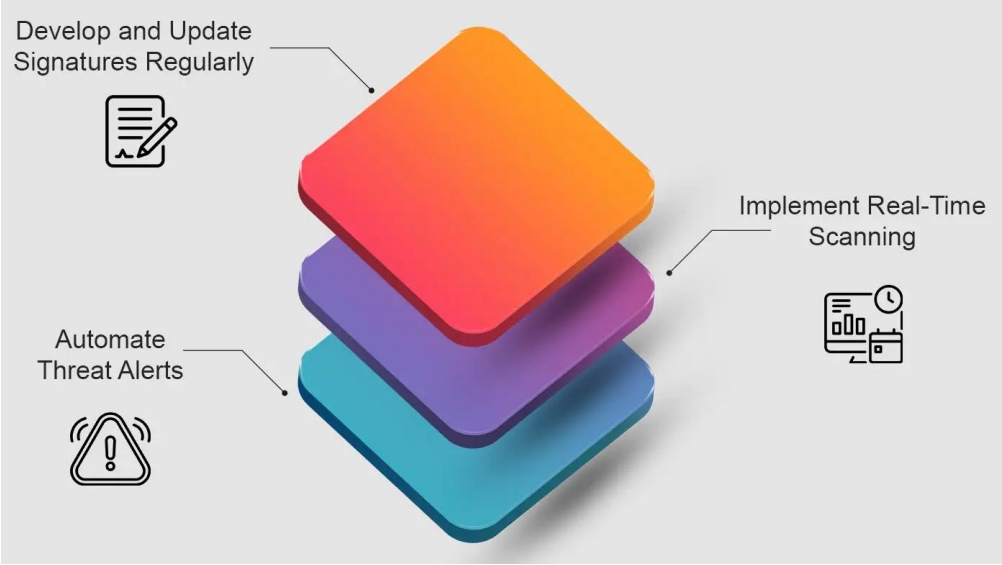


Рисунок 2.6 – Схема процесу виявлення на основі сигнатур

Сценарій: Компанія отримує підозрілий файл електронною поштою. Антивірусне програмне забезпечення компанії сканує файл та ідентифікує вбудований у нього унікальний рядок шкідливого коду. Цей код відповідає відомому підпису, що зберігається в базі даних, який був доданий після аналізу дослідниками аналогічного шкідливого програмного забезпечення. Система негайно поміщає файл у карантин, запобігаючи його виконанню та потенційному пошкодженню систем компанії. Така швидка реакція демонструє ефективність виявлення на основі сигнатур у запобіганні тому, щоб відомі загрози стали причиною пошкодження.

Виявлення на основі сигнатур є надійним інструментом протягом десятиліть, а його переваги полягають у точності та простоті. Але заглибимося в те, чому цей метод досі є наріжним каменем сучасної кібербезпеки (табл.2.4).

Таблиця 2.4– Аналіз сильних і слабких сторін Signature-based Detection

Аспект	Переваги Signature–based Analysis	Недоліки Signature–based Analysis
Швидкість і точність	Дуже швидке виявлення відомих загроз завдяки точним сигнатурам	Не може виявити нові, невідомі загрози або модифіковане шкідливе ПЗ
Точність (False Positives)	Низький рівень хибнопозитивних спрацювань	Поліморфне або метаморфне ПЗ може обходити сигнатурне виявлення
Простота реалізації	Простий у впровадженні та інтеграції в існуючі системи безпеки	Потребує регулярного обслуговування, оновлення бази сигнатур
Історична перевіреність	Випробуваний роками метод, широко підтримується	Не справляється з атаками нульового дня або складними атаками (APT)
Залежність від оновлень	Дає високу ефективність при актуальній базі сигнатур	Без постійних оновлень втрачає ефективність
Підхід до загроз	Ефективний щодо вже відомих атак	Реактивний: не попереджає, а лише виявляє загрози, які вже ідентифіковані

Виявлення на основі сигнатур працює значною мірою шляхом зіставлення файлів, поведінки або шаблонів з базою даних відомих загроз.

Зіставлення рядків:

– сканує файли або потоки даних на наявність певних послідовностей символів, що відповідають відомим сигнатурам шкідливого програмного забезпечення;

– практична порада: регулярно оновлюйте свою базу даних сигнатур, щоб переконатися, що вона містить найновіші шаблони загроз.

Виявлення на основі хешу:

– кожен файл або фрагмент шкідливого програмного забезпечення має унікальне «хеш–значення». Якщо хеш файлу збігається з відомим шкідливим файлом, він позначається як шкідливий;

– практична порада: переконайтеся, що ваша система регулярно сканує файли та порівнює їх з оновленими базами даних.

Поведінкові сигнатури:

– зосереджується на закономірностях у поведінці (наприклад, повторювані невдалі спроби входу, незвичайні передачі даних) та порівнює їх з відомими шкідливими діями;

– практична порада: відстежуйте тенденції поведінки з часом, щоб на ранній стадії виявляти будь–які аномалії.

Поведінкова аналітика передбачає вивчення тенденцій та моделей активності користувачів організації. У контексті кібербезпеки поведінкова аналітика зосереджується на поведінці користувачів у мережах та додатках, відстежуючи незвичайну активність, яка може свідчити про загрозу безпеці.

Зі зростанням складності та витонченості сучасних кіберзагроз, роль поведінкової аналітики в кібербезпеці також зростає. Вона пропонує додатковий рівень захисту, виявляючи аномалії, які традиційні заходи безпеки можуть пропустити.

Поведінкова аналітика виходить далеко за рамки простого збору даних. Вона включає глибокий аналіз активності користувачів та систем в організації, розкриваючи, як, коли та чому. Оцінка активності в режимі реального часу допомагає точно визначити закономірності, тим самим виявляючи аномалії використання або потенційно шкідливу поведінку.

Штучний інтелект (ШІ) та машинне навчання (МН) часто доповнюють поведінкову аналітику. ШІ/МН можуть просіювати величезні обсяги даних, щоб виявляти закономірності та порушення. Завдяки інтеграції ШІ/МН процеси поведінкової аналітики в організації отримують вигоду від автоматизації та ефективності.

Звичайно, поведінкова аналітика найкраще працює з різноманітними наборами даних. Це допомагає створити всебічне розуміння поведінки користувачів і системи. Типи даних, що використовуються в поведінковій аналітиці, включають:

– мережевий трафік;

– активність бази даних;

– активність користувачів;

– системні події.

Поведінкова аналітика починається з встановлення базової поведінки: стандартних дій, які вважаються нормальними в мережі організації. Після визначення базової лінії ваш механізм поведінкової аналітики може виявити відхилення від базової лінії, які можуть свідчити про загрозу безпеці або вразливість. Відхилення можна позначити на основі того, наскільки вони відрізняються від базової поведінки. [24]

Аналітика поведінки включає дії, які перетворюють дані з різних джерел на практичні висновки. Тепер давайте розглянемо, як це працює, збираючи необроблені джерела даних для запобігання потенційним кібератакам.

Крок 1. Збір та перетворення даних. Першим кроком бізнес-аналізу є збір необхідних даних, що стосуються проблемної сфери, та перетворення їх у відповідний формат для аналізу. Джерела даних включають:

– журнали мережевого трафіку;

– журнали доступу;

– записи про активність користувачів бази даних.

Наразі вилучення та перетворення даних можуть бути повністю автоматизовані та виконуватися в режимі реального часу.

Крок 2. Аналіз даних. Після перетворення даних у правильний формат, BA використовує неконтрольовані алгоритми машинного навчання для аналізу цих даних та виявлення аномалій, що відхиляються від нормальної поведінки.

Крок 3. Оповіщення та усунення несправностей. Коли процес виявляє аномалію в даних, він повідомляє про це команди безпеки за допомогою інтегрованої системи сповіщень. Вона надасть командам безпеки всю необхідну інформацію, щоб вони могли вжити необхідних заходів.

Кореляція подій є основоположною діяльністю для всіх цифрових практик: IT та мережевих операцій, управління IT–послугами, публікації/підписки та, безумовно, кібербезпеки.

Кореляція подій корисна в кількох сферах IT. Ось короткий огляд того, як працює весь процес кореляції IT–подій:

– агрегація. Збирає дані моніторингу з різних пристроїв, таких як програми та інструменти моніторингу, в одному місці для легкого доступу;

– фільтрація. Після збору даних вони уточнюються за допомогою фільтрації;

– дедуплікація. Виявляє дублікати записів та видаляє їх із наборів даних, щоб зберегти лише унікальні події;

– нормалізація. Нормалізуйте дані в узгоджений формат. Таким чином, штучний інтелект інструмента кореляції подій може інтерпретувати їх однаково, незалежно від походження;

– аналіз першопричини. Проаналізуйте, як події пов'язані між собою, щоб з'ясувати основну причину проблеми. Наприклад, ми можемо проаналізувати події з одного пристрою, щоб побачити, як вони впливають на інші пристрої в мережі[25].

– *Методи машинного навчання (ML)* — це підклас штучного інтелекту (ШІ), який об’єднує підходи та технології для створення алгоритмів, здатних самостійно навчатися на основі даних. На відміну від традиційних програм, які чітко прописані для виконання конкретних завдань, ML-моделі з часом покращують свою роботу, аналізуючи дані і виявляючи в них закономірності. Це дає змогу розв’язувати складні задачі, які важко або неможливо реалізувати звичайним програмуванням[26]. Існує багато типів алгоритмів машинного навчання (рис. 2.7), серед яких найпоширеніші:

– навчання з вчителем (Supervised learning). Алгоритм навчається на розмічених даних, де кожен приклад має відповідну мітку або клас;

– навчання без вчителя (Unsupervised learning). Алгоритм працює з даними без позначок і самостійно знаходить структури чи закономірності;

– напівкероване навчання (Semi-supervised learning) поєднує обидва підходи, використовуючи як розмічені, так і нерозмічені дані;

– навчання з підкріпленням (Reinforcement Learning, RL). Алгоритм вчиться приймати рішення, отримуючи «винагороду» або «штраф» залежно від своїх дій.

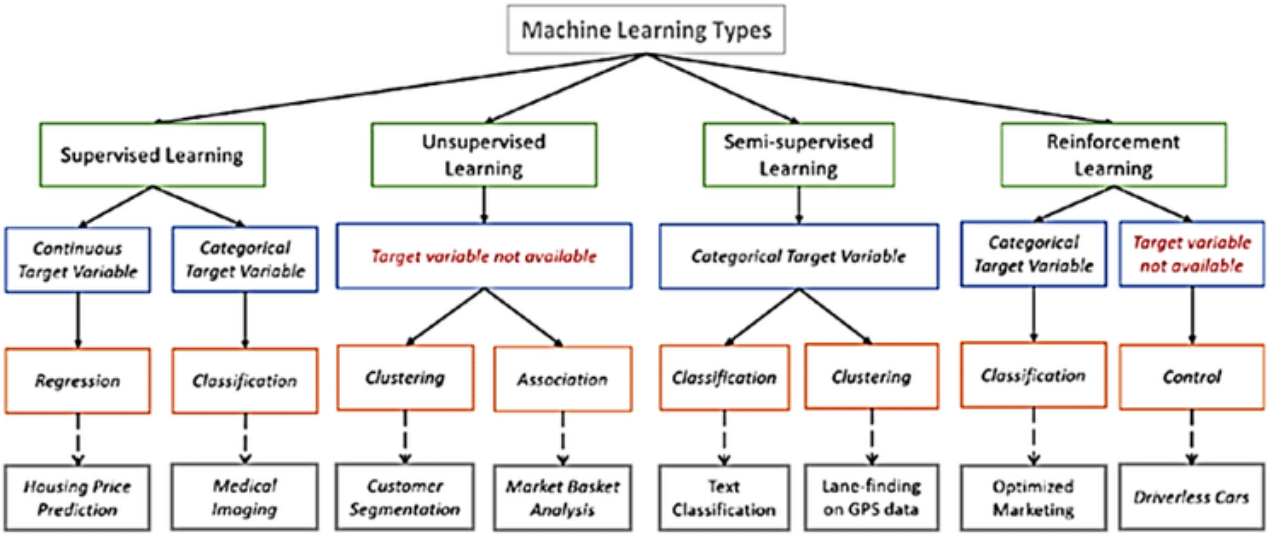


Рисунок 2.7 – Типи ML–алгоритмів

Сьогодні машинне навчання активно впроваджується у різноманітні сфери — від медицини та фінансових технологій до маркетингу та виробництва. Наведемо кілька прикладів, які демонструють, як ця технологія застосовується для розв’язання практичних завдань:

– Amazon, Netflix, Spotify застосовують ML для побудови рекомендаційних систем, що пропонують контент або товари на основі історії переглядів, покупок, вподобань та інших користувацьких даних;

– Google, Facebook використовують алгоритми машинного навчання для показу персоналізованої реклами з урахуванням інтересів, пошукової активності, демографії та поведінки користувачів у соцмережах;

– віртуальні помічники Apple Siri, Amazon Alexa, Google Assistant — використовують ML для розпізнавання природної мови, інтерпретації запитів і виконання завдань користувачів;

– IBM Watson застосовує ML для аналізу медичних зображень (рентген, МРТ), що допомагає лікарям у виявленні захворювань;

– Verily (підрозділ Alphabet) розробляє ML-алгоритми для діагностики хвороб на основі симптомів, медичної історії та результатів обстежень пацієнтів.

– Walmart використовує машинне навчання для прогнозування попиту на товари, що дозволяє ефективно керувати запасами та плануванням виробництва;

– Uber впроваджує ML для аналізу попиту на поїздки та оптимізації розподілу водіїв у реальному часі.

Ці приклади демонструють, наскільки широко машинне навчання інтегроване в сучасний бізнес. Завдяки постійному розвитку технологій, ML-системи стають дедалі продуктивнішими, дозволяючи вирішувати складніші задачі. Компанії, які ефективно застосовують машинне навчання, отримують значну конкурентну перевагу.

Однак важливо пам’ятати, що машинне навчання — не чарівна паличка. У межах побудови систем автоматизованого виявлення та аналізу кіберзагроз важливу роль відіграють інструменти, здатні збирати, обробляти та інтерпретувати події безпеки у реальному часі.

Розглянемо кілька популярних рішень, які активно застосовуються у практиці інформаційної безпеки:

Wazuh — платформа з відкритим кодом, що поєднує функції сигнатурного виявлення, поведінкової аналітики та кореляції подій. Інтегрується з іншими рішеннями, зокрема ELK Stack, і може використовуватися як повноцінна SIEM-система. Забезпечує збір логів, контроль цілісності файлів, виявлення вторгнень та відповідність політикам безпеки.

1. Zeek — мережевий аналізатор, орієнтований на поведінкове виявлення загроз. Забезпечує детальний аналіз мережевого трафіку, з можливістю створення кастомних політик для виявлення: аномальної активності, підозрілих з'єднань, потенційно шкідливих дій у режимі реального часу[27];

2. CrowdStrike Falcon — сучасна платформуа, яка поєднує функціональність EDR (Endpoint Detection and Response) і XDR (Extended Detection and Response). Вона використовує методи машинного навчання для виявлення як відомих, так і нових типів загроз, аналізу поведінки користувачів і пристроїв, а також забезпечення проактивного захисту на рівні кінцевих точок[28];

3. Splunk — платформа для збору й аналізу великих обсягів даних, яка може виступати як SIEM-система. Splunk дозволяє створювати гнучкі кореляційні правила, візуалізувати дані у вигляді дашбордів, а також автоматизувати процеси

виявлення інцидентів. Завдяки підтримці алгоритмів машинного навчання, платформа ефективно застосовується для виявлення складних та багатовекторних атак.

Таким чином, сучасні інструменти виявлення загроз забезпечують не лише реактивне, а й проактивне реагування на потенційні інциденти безпеки. Їх застосування є ключовим компонентом автоматизованих систем моніторингу, що дозволяє зменшити час виявлення атак, покращити точність детекції та забезпечити комплексний підхід до захисту інформаційних систем

3. ЗАСТОСУВАННЯ ФРЕЙМВОРКІВ ТА МОДЕЛЕЙ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

3.1 Аналіз сучасних інструментів автоматизованого виявлення кіберзагроз

Аналіз сучасних інструментів виявлення кіберзагроз дозволяє визначити практичну реалізацію автоматизованих методів, описаних в (п. 2.4). Обрані рішення демонструють здатність ефективно працювати з великими обсягами даних, здійснювати кореляцію подій, виявляти відхилення в поведінці користувачів та систем, застосовувати алгоритми машинного навчання, а також інтегруватися з іншими компонентами інформаційної інфраструктури. Такий підхід забезпечує оперативне реагування на загрози та підвищення загального рівня кіберзахисту організацій.

Wazuh – використовується широким колом організацій, включаючи CERN, Міністерство оборони Іспанії та Alfamart, для моніторингу безпеки, управління журналами та дотримання вимог. Його віддають перевагу освітні заклади, державні установи та телекомунікаційні компанії, такі як Wind Telecom, завдяки гнучкості відкритого коду та можливостям виявлення загроз у режимі реального часу.

Wazuh чудово справляється зі збором журналів з різних джерел, включаючи операційні системи, програми та мережеві пристрої. Він використовує передові методи парсингу для вилучення значущих даних, що дозволяє проводити комплексний аналіз безпеки та виявляти загрози.

Платформа забезпечує миттєві сповіщення про потенційні інциденти безпеки, що дозволяє швидко реагувати на загрози. Її можливості моніторингу в режимі реального часу забезпечують постійний контроль за активністю системи, допомагаючи підтримувати проактивний рівень безпеки.

Wazuh спрощує управління відповідністю, автоматизуючи створення звітів

для різних регуляторних стандартів. Він також сприяє ретельному аудиту, відстеженню змін у системі та діяльності користувачів для забезпечення дотримання політик та правил безпеки.

Щоб оцінити ефективність систем SIEM/EDR для підприємств, ми зосередимося на ключових функціях, які є вирішальними для комплексного управління безпекою. Ось порівняльна таблиця Wazuh з трьома іншими популярними системами SIEM/EDR (табл.3.1).

Таблиця 3.1 – порівняльна характеристика інструментів SIEM/EDR

Функція	Wazuh	Splunk
Збір та аналіз журналів	Комплексний	Екстенсивний
Оповіщення в режимі реального часу	Так	Так
Інтеграція розвідки загроз	Так	Так
Моніторинг цілісності файлів	Вбудований	Через доповнення
Звітність про відповідність	Екстенсивний	Комплексний
Масштабованість	Високий	Дуже високий
Інтеграція з хмарою	Сильний	Відмінно
Аналіз поведінки користувачів та сутностей (UEBA)	Обмежена	Розширений
Вартість	Відкритий код	Висока
Легкість розгортання	Помірний	Комплекс
Створення власного правила	Гнучкий	Висока гнучкість
Інтеграції зі сторонніми розробниками	Добре	Екстенсивний

Це порівняння підкреслює, що хоча Wazuh пропонує потужні функції, порівнянні з комерційними рішеннями, особливо в таких сферах, як збір журналів, сповіщення в режимі реального часу та звітність про відповідність, він може мати деякі обмеження в розширеній аналітиці та UEBA порівняно з більш усталеними комерційними продуктами. Однак його відкритий код та сильні основні функції роблять його привабливим варіантом для багатьох підприємств, особливо тих, хто шукає економічно ефективне рішення з хорошими можливостями налаштування. [29]

Splunk – це платформа для збору, зберігання, обробки та аналізу машинних даних, тобто логів. Наразі вона дуже популярна у США та Європі, а також

поступово виходить на інші ринки, включно з Україною. Головною перевагою Splunk є її здатність працювати з даними практично з будь-яких джерел, що значно розширює сферу застосування системи (рис. 3.1).



Рисунок 3.1 – Перелік інструментів інструмента Splunk

Splunk підтримує кореляційні правила, машинне навчання, створення дашбордів та автоматичних сповіщень. Завдяки потужним аналітичним функціям платформа ефективно виявляє складні, багатоетапні кіберзагрози. Splunk зазвичай (автоматично або через додаткові модулі) розбирає вхідні дані на поля та значення для подальшої обробки. Ця обробка здійснюється через SPL — спеціальну мову запитів Splunk, яка дозволяє створювати вибірки, таблиці, сортувати, фільтрувати, агрегувати інформацію, генерувати звіти, додавати обчислювальні поля, звертатись як до внутрішніх, так і зовнішніх довідників, будувати дашборди з різноманітними типами візуалізації та налаштовувати алерти (наприклад, для автоматичного створення заявок у Service Desk). Всі ці функції можна упакувати у власний додаток.

Основні відмінності або сильні сторони Splunk:

– архітектура в реальному часі: Splunk збирає, аналізує, моніторить і здійснює пошук по великих обсягах даних (до сотень терабайт на день) у реальному часі — все це в одній системі. Це дозволяє отримувати інформацію з тисяч різних джерел (фізичних, віртуальних, хмарних) без затримок. Крім того, пошук можна

виконувати не лише у реальному часі, а й по історичних даних за будь-який період, що робить систему універсальною для моніторингу, звітності та аналітики;

– універсальна платформа машинних даних. Splunk може індексувати будь-які машинні дані з часовою позначкою незалежно від формату і структури. Платформа здатна поєднувати машинні, бізнес- та користувацькі дані, що значно підвищує її гнучкість;

– схема на льоту. Для пошуку в Splunk не потрібно заздалегідь знати структуру даних. Досить вказати часовий проміжок і ключові слова, щоб швидко переглянути результати. Запити можна зупиняти, ставити на паузу або переглядати проміжні результати, що робить роботу з даними надзвичайно гнучкою;

– гнучка аналітика та звітність: Splunk надає широкі можливості для побудови аналітики, створення звітів і їх візуалізації. Крім внутрішніх даних, система може звертатись до зовнішніх довідників, таких як SQL-бази даних. Також можна розробляти власні модулі, що розширюють функціонал;

– масштабованість від робочого столу до підприємства. Завдяки технології MapReduce, Splunk забезпечує розподіл навантаження і горизонтальне масштабування. Це означає, що почати можна з одного сервера, а при зростанні обсягів даних додати нові вузли, які розподілять обробку. Технологія дозволяє працювати з великими обсягами даних без потреби в надпотужному обладнанні;

– швидкий запуск та результат. Впровадження Splunk відбувається за лічені години або дні, а не тижні чи місяці. Також процес масштабування і подальшої експлуатації системи відносно простий і швидкий. [30]

3.2 Застосування MITRE ATT&CK Navigator для моделювання загроз

Аналізуючи можливі вектори атак на пристрій доповненої реальності користувача, доцільно скористатися базою знань MITRE Mobile ATT&CK, яка спеціалізується на загрозах, притаманних мобільним платформам. Це особливо

актуально, оскільки більшість AR-пристроїв працюють на модифікованих мобільних операційних системах, таких як Android. Саме тому багато тактик і технік із цієї бази знань є релевантними для досліджуваної системи.

Однією з початкових тактик, які можуть бути використані зловмисниками, є Initial Access, тобто отримання первинного доступу до пристрою. У контексті AR-платформи це може бути досягнуто шляхом фішингових атак, встановлення шкідливих додатків або використання уразливостей у сторонньому програмному забезпеченні, що працює на пристрої. Наприклад, користувач може встановити AR-додаток, який не пройшов перевірку безпеки або вимагає надмірних дозволів, що відкривають зловмиснику доступ до чутливих функцій пристрою — таких як камера, мікрофон чи геолокація.

Після отримання початкового доступу можливе застосування тактик, пов’язаних з Privilege Escalation та Defense Evasion, які дозволяють атакувальнику підвищити рівень своїх привілеїв та приховати свою присутність у системі. Наприклад, це може бути досягнуто через експлуатацію уразливостей операційної системи пристрою або обходу системи контролю доступу до об’єктів доповненої реальності.

Також слід враховувати тактики з категорії Collection, які описують методи збору даних з пристрою. У випадку з AR-системами це може включати перехоплення аудіо або відео з камер і мікрофонів, зчитування координат руху користувача або взаємодій з навчальними об'єктами в доповненій реальності. Усі ці дані можуть бути надзвичайно чутливими, особливо якщо йдеться про освітні або корпоративні тренінги, які містять конфіденційну інформацію.

Ще одним важливим аспектом є Command and Control — встановлення зв’язку з віддаленим сервером для управління зараженим пристроєм. Зловмисники можуть використовувати шифровані канали або легітимні служби для прихованого передавання даних з пристрою. У поєднанні з техніками з тактики Exfiltration, це дозволяє їм отримувати доступ до особистих даних користувача або навіть до навчального контенту, розміщеного в системі.

Таким чином, вектор атаки на AR-пристрій користувача може включати послідовність дій: від фішингової атаки або встановлення шкідливого ПЗ, через ескалацію прав і приховування активності, до збору та виведення даних за межі системи. Модель MITRE ATT&CK дозволяє візуалізувати ці сценарії, виявляти найвразливіші точки та планувати відповідні заходи реагування та захисту.

Особливо важливим є виявлення саме тих технік, які на практиці можуть бути реалізовані проти конкретної конфігурації пристрою та програмного забезпечення, що використовується в освітньому середовищі з доповненою реальністю.

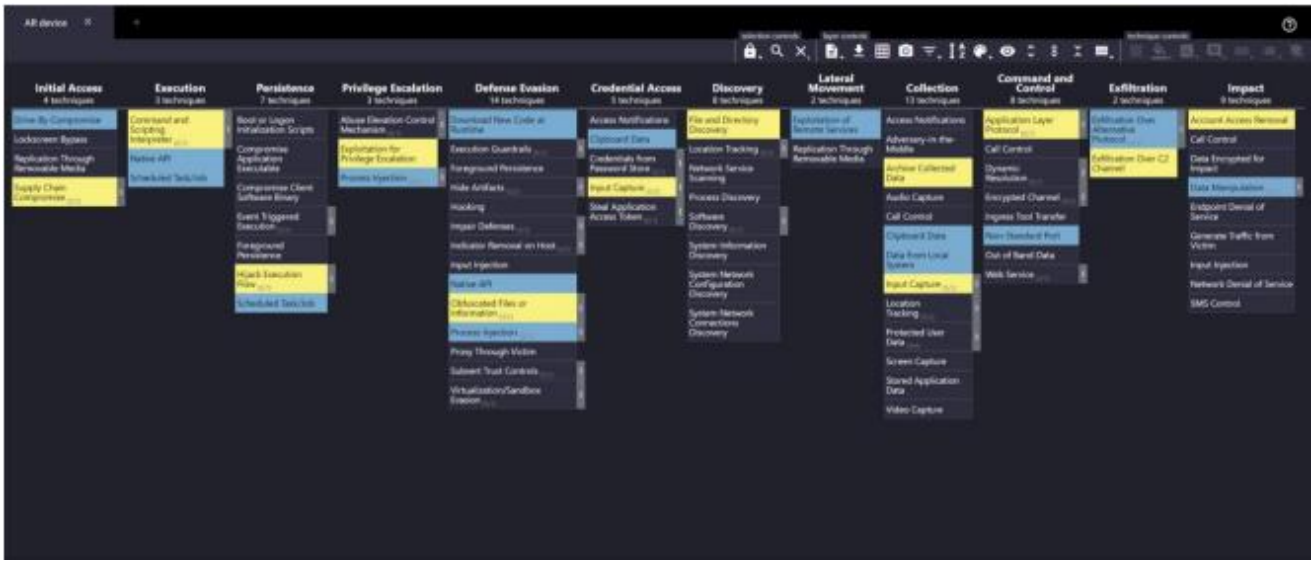


Рисунок 3.2 – Вектори атак на AR пристрої

Для глибшого розуміння потенційних сценаріїв компрометації AR-пристроїв у межах освітньої системи, побудованої на технологіях доповненої реальності, розглянемо два типові вектори атак, змодельовані на основі фреймворку MITRE ATT&CK. Кожен із них представляє послідовність технік, які зловмисник може використати для проникнення в систему, закріплення своєї присутності, збору інформації та її ексфільтрації (рис.3.2).

Перший вектор починається з компрометації ланцюга постачання (Supply Chain Compromise). У цьому випадку зловмисник отримує доступ до AR-пристрою ще на етапі виробництва або розробки програмного забезпечення — наприклад,

через заражене оновлення прошивки або модифікований драйвер для периферійного пристрою. Після цього запускається шкідливий код за допомогою інтерпретаторів команд і скриптів (Command and Scripting Interpreter). Це дозволяє виконати ініціальні інструкції без активації традиційних антивірусних захистів. Згодом відбувається перехоплення потоку виконання (Hijack Execution Flow) — техніка, яка дає змогу закріпити шкідливу присутність шляхом зміни шляху запуску довірених програм. Щоб отримати повний контроль над пристроєм, зловмисник виконує експлуатацію вразливостей для ескалації привілеїв (Exploitation for Privilege Escalation), що дозволяє йому діяти від імені системного користувача. Після закріплення в системі, важливим етапом є обфускація даних і дій (Obfuscated Files or Information) — приховування шкідливих компонентів від аналітичних засобів. На цьому етапі зловмисник може почати перехоплювати введення користувача (Input Capture), зокрема дані автентифікації чи взаємодію з AR-об’єктами. Для розширення атаки здійснюється сканування файлової системи (File and Directory Discovery) з метою виявлення цінної інформації або точок доступу. Зібрані дані зазвичай архівуються (Archive Collected Data) для подальшої ексфільтрації. Вивід здійснюється через протоколи прикладного рівня (Application Layer Protocol) — зокрема, HTTP або HTTPS(рис.3.3), що маскує зловмисну активність під звичайний вебтрафік.



Рисунок 3.3 – Порівняння структури протоколів HTTP та HTTPS

Важлива інформація передається через C2-канал (Exfiltration Over C2 Channel), встановлений заздалегідь, що дозволяє зловмиснику залишатися в системі непоміченим.

На завершальному етапі здійснюється видалення доступу до облікових записів (Account Access Removal), що унеможливлює відновлення контролю з боку законного користувача або адміністратора.

Другий вектор атаки імітує ситуацію, коли користувач випадково активує шкідливу активність, відвідавши скомпрометований вебресурс — так звану Drive-By Compromise. У результаті цього зловмисник отримує початковий доступ до системи. Для виконання шкідливого коду на пристрої використовуються виклики Native API, що дозволяє запускати код без створення нових процесів, мінімізуючи ймовірність виявлення засобами захисту.

Наступним кроком є створення Scheduled Task/Job — запланованого завдання або служби, яке забезпечує періодичне виконання зловмисного коду. Це гарантує стійкість атаки та дозволяє зловмиснику зберігати контроль над пристроєм навіть після його перезавантаження.

Для підвищення привілеїв застосовується Process Injection — техніка впровадження коду в довірені процеси системи, що дозволяє приховати шкідливу активність від механізмів виявлення.

У процесі атаки може бути реалізовано Download New Code at Runtime — динамічне завантаження нового коду під час виконання. Це дає змогу зловмиснику адаптувати поведінку шкідливого ПЗ до умов середовища.

Подальшим етапом є доступ до Clipboard Data, де можуть зберігатися тимчасові паролі, ключі чи інша конфіденційна інформація.

Після цього відбувається Exploitation of Remote Services — зловмисник використовує вразливості віддалених сервісів з метою горизонтального переміщення мережею, що дозволяє йому розширити доступ до інших компонентів інфраструктури.

Для збору цінної інформації застосовується техніка Data from Local System, що передбачає зчитування локальних конфігурацій, журналів, збережених облікових даних тощо.

Щоб уникнути виявлення, ексфільтрація даних здійснюється через Non-Standard Port або з використанням Exfiltration Over Alternative Protocol, зокрема таких протоколів, як DNS або FTP.

Це значно ускладнює фіксацію інциденту засобами моніторингу. Завершальним етапом є Data Manipulation — навмисна модифікація або знищення даних, що може порушити цілісність інформації, викликати збої в навчальному процесі або спричинити саботаж функціонування системи.

Для побудови моделі загроз, пов’язаних із базами даних, мережею та вебінтерфейсом користувача системи управління навчанням (LMS — Learning Management System), доцільно застосовувати фреймворк MITRE ATT&CK for Enterprise. Він дозволяє систематизовано моделювати потенційні сценарії атак, описуючи типові техніки, що застосовуються зловмисниками на різних етапах атаки — від початкового доступу до ексфільтрації даних.

Зокрема, при моделюванні загроз для LMS слід приділити особливу увагу сценаріям, спрямованим на базу знань системи, яка становить підвищену цінність як джерело навчального та особистісного контенту. За допомогою фреймворку MITRE ATT&CK можливо ідентифікувати ключові техніки, що використовуються під час збору, передачі та маніпуляцій із даними, а також візуалізувати вектори потенційних атак (рис. 3.4), орієнтовані на базу даних LMS.

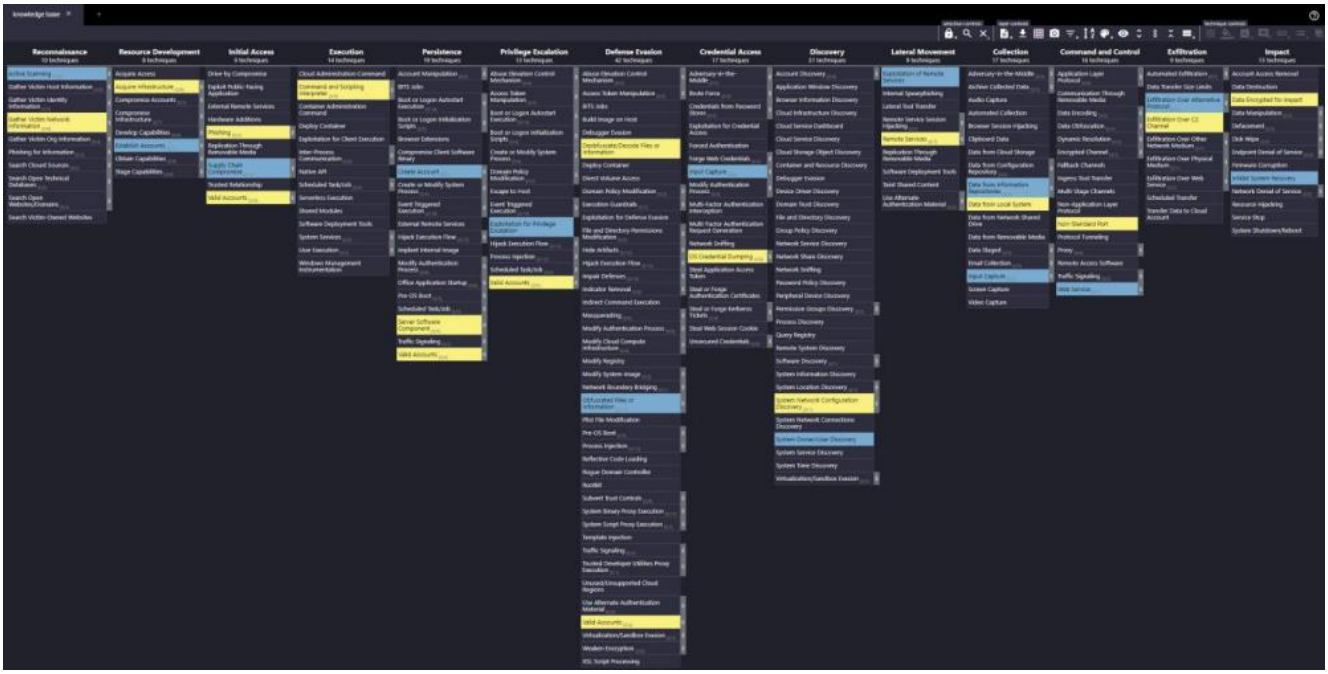


Рисунок 3.4 – Вектори атак на бази знань LMS

Перший вектор атаки охоплює комплекс послідовних дій зловмисника, спрямованих на компрометацію системи управління навчанням (LMS) через взаємодію як із користувачем, так і з інфраструктурою. Спочатку зловмисник проводить ретельне попереднє дослідження, збираючи інформацію про мережеву інфраструктуру цільової системи — це може відбуватися як за допомогою відкритих джерел, так і через активне сканування мережі. Далі створюється необхідна для атаки інфраструктура, що слугує базою для подальших дій.

Поштовхом для проникнення часто слугує фішингова атака — користувачу надсилається шкідливе повідомлення, яке заохочує до взаємодії з компрометованим вмістом. Після отримання первинного доступу зловмисник використовує команди і скрипти для проведення розвідки та підготовки подальших дій, реалізуючи це через механізми командного інтерпретатора системи.

Для збереження контролю над LMS уражається серверне програмне забезпечення: зловмисник додає шкідливий модуль до серверної частини системи, що дозволяє йому підтримувати стійку присутність у системі. Одночасно з цим відбувається отримання або підбір дійсних облікових даних користувачів, що

дозволяє зловмиснику обійти стандартні механізми автентифікації та підвищити рівень доступу.

Для уникнення виявлення засобами безпеки використовуються методи декодування або розшифрування раніше прихованої інформації. Паралельно здійснюється експорт облікових даних із системи, що дає змогу надалі поширювати атаку. Далі зловмисник проводить детальний аналіз конфігурації мережі, виявляючи доступні хости та сервіси, після чого через віддалені служби поширює шкідливу активність на інші вузли інфраструктури.

Зібрані дані безпосередньо отримуються з локальної системи, де був досягнутий доступ. Для обходу механізмів фільтрації та виявлення комунікації використовуються нестандартні порти, що ускладнює моніторинг активності. Отримана інформація передається через канал командного управління (C2) до інфраструктури зловмисника. Завершальним кроком атаки є шифрування критично важливих даних, що унеможливлює їх подальше використання та може супроводжуватися вимогою викупу

Другий вектор атаки фокусується на компрометації системи управління навчанням (LMS) через використання вразливостей самої системи та ланцюга постачання її компонентів. Спершу відбувається активне сканування елементів LMS з метою виявлення доступних служб та відкритих портів, що дозволяє зловмиснику отримати уявлення про мережеву архітектуру та цілі для подальших дій. Наступним кроком є створення фіктивного облікового запису, який слугує точкою початкового доступу до системи.

Зловмисник може компрометувати програмне забезпечення або залежності, що постачаються в LMS, на етапі доставки або оновлення, що забезпечує йому прихований доступ до системи. Для підтримання контролю він створює додаткові облікові записи з розширеними правами. Використовуючи наявні вразливості, атакуючий підвищує свої привілеї всередині системи, що дає змогу реалізовувати більш глибокий контроль над LMS.

Для уникнення виявлення застосовуються техніки обфускації шкідливих файлів чи інформації, що приховують їх присутність. Додатково зловмисник

встановлює програмне забезпечення для перехоплення натискань клавіш (keylogger), щоб викрасти облікові дані користувачів. Ідентифікація привілейованих користувачів і власників системи допомагає точково націлити атаки та посилити вплив.

Подальші кроки передбачають експлуатацію віддалених сервісів, що дозволяє зловмиснику горизонтально рухатися мережею та розширювати контроль над іншими компонентами інфраструктури. Для отримання цінної інформації атакуючий вилучає дані з внутрішніх репозиторіїв LMS, таких як база знань, навчальні матеріали або персональні дані користувачів.

Організація каналу командного управління здійснюється через вебслужби, які використовують HTTP / HTTPS-трафік, що ускладнює виявлення атаки, адже її активність маскується під звичайний мережевий трафік. Витік інформації реалізується через нетипові мережеві протоколи, наприклад DNS або FTP, що дозволяє уникати стандартних засобів моніторингу.

Заключним етапом є навмисне унеможливлення відновлення системи: зловмисник видаляє резервні копії, пошкоджує точки відновлення або змінює системні параметри, відповідальні за аварійне відновлення, що значно ускладнює повернення до нормального функціонування.

В контексті мережевого з’єднання атаки зазвичай спрямовані на перехоплення трафіку, порушення захисту мережі або дестабілізацію її роботи. Подальші вектори атак базуються на моделі MITRE ATT&CK для мереж, як показано на (рис. 3.5).

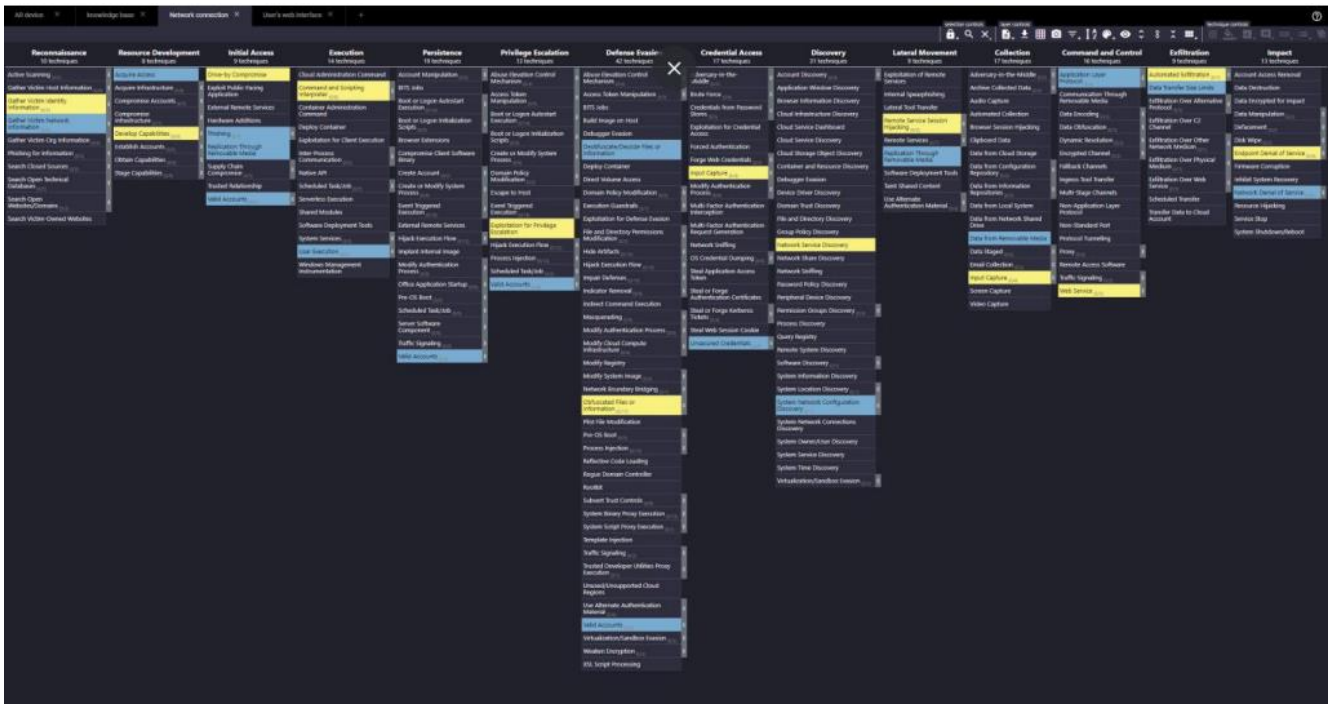


Рисунок 3.5 – Вектори атак на мережеві з’єднання

Перший вектор моделює комплексну, багатофазну атаку, що поєднує різноманітні техніки для досягнення повного контролю над системою LMS. Його основні характеристики:

1. початковий доступ. Здійснюється через збір інформації про користувачів і цілі (Gather Victim Identity Information) та зараження системи через відвідування скомпрометованих сайтів (Drive-by Compromise), що часто базується на соціальній інженерії;

2. розробка і застосування інструментів. Зловмисник готує власні шкідливі сценарії і інструменти (Develop Capabilities) для гнучкого й ефективного проникнення;

3. підвищення привілеїв. Використання локальних уразливостей (Exploitation for Privilege Escalation) дозволяє розширити можливості атаки всередині системи;

4. ухилення від виявлення. Застосування обфускації (Obfuscated Files or Information) та прихованих засобів перехоплення даних (Input Capture) мінімізує ризики виявлення;

5. розвідка і розширення контролю. Активне сканування мережевих сервісів (Network Service Scanning), перехоплення SSH-сесій (SSH Hijacking), доступ до спільних мережевих ресурсів (Data from Network Shared Drive) допомагають зловмиснику рухатися по мережі та збирати цінні дані;

6. управління і ексфільтрація. Вебсервіси як канали C2 (Command and Control) підтримують зв'язок із зараженими вузлами, а автоматизована ексфільтрація (Automated Exfiltration) забезпечує передачу викраденої інформації;

7. порушення роботи системи. При необхідності виконується DoS-атака (Endpoint Denial of Service) для виведення з ладу окремих елементів інфраструктури або відволікання уваги захисту.

Цей вектор відображає стратегічний підхід зловмисника — від первинного проникнення через вебінтерфейси та користувачів до глибинного контролю над мережею LMS, із використанням як технічних вразливостей, так і соціальних механізмів. Його послідовність і різноманітність технік робить його особливо небезпечним, вимагаючи комплексних і багаторівневих заходів безпеки

Вектор моделює комплексну атаку, яка включає послідовне використання низки технік, починаючи від початкового доступу через соціальну інженерію, до компрометації мережевої інфраструктури та вебінтерфейсу(рис.3.6):

1. Gather Victim Network Information — зловмисник здійснює розвідку з метою вивчення мережевої архітектури, маршрутизації, IP-діапазонів і використовуваного мережевого обладнання;

2. Acquire Infrastructure — для реалізації атаки зловмисник розгортає власну інфраструктуру, наприклад, сервери керування (C2), фішингові домени або проксі;

3. Phishing — надсилаються шкідливі електронні листи, що містять вкладення або посилання на заражені ресурси з метою ініціації доступу;

4. User Execution — користувача спонукають самостійно запустити шкідливий файл, який забезпечує початкове зараження системи;

5. Valid Accounts — для закріплення в системі зловмисник використовує легітимні облікові записи (викрадені або отримані шляхом підбору);

6. Deobfuscate/Decode Files or Information — проводиться розшифрування або деобфускація шкідливого коду, щоб активізувати приховані можливості програми;

7. Unsecured Credentials — здійснюється пошук облікових даних у відкритих конфігураційних файлах, реєстрах чи незахищених сховищах;

8. System Network Configuration Discovery — аналізуються параметри мережевої конфігурації системи (IP-адреси, підмережі, маршрути);

9. Replication Through Removable Media — використовуються знімні носії для копіювання або розповсюдження шкідливих компонентів по інфраструктурі;

10. Data from Removable Media — зловмисник здійснює збір даних із зовнішніх носіїв, підключених до заражених систем;

11. Application Layer Protocol — для передачі команд або ексфільтрації даних застосовуються протоколи прикладного рівня (HTTP, HTTPS, DNS тощо);

12. Data Transfer Size Limits — обсяг переданих даних навмисно обмежується для уникнення виявлення системами безпеки;

13. Network Denial of Service — виконується атака типу "відмова в обслуговуванні" (DoS) з метою порушення доступності критичних елементів мережі. Вебінтерфейси користувачів часто є основними мішенями для атак, оскільки вони слугують точками входу до системи. Використовуючи Enterprise ATT&CK фреймворк, ми можемо розробити наступні вектори атаки (рис. 3.11):

1. Active Scanning — проводиться активне сканування вебінтерфейсу на наявність вразливостей, помилок конфігурації або відкритих служб;

2. Compromise Infrastructure — інфраструктура, що обслуговує вебінтерфейс (наприклад, сервери), може бути скомпрометована через сторонні сервіси або вразливості у програмному забезпеченні;

3. Drive-by Compromise — під час взаємодії з вебінтерфейсом користувач перенаправляється на заражену сторінку, яка автоматично завантажує шкідливий код;

4. System Services — шкідливий код виконується у контексті служб вебсервера або операційної системи, отримуючи доступ до ресурсів серверного

рівня;

5. Server Software Component — впроваджуються шкідливі компоненти безпосередньо в серверне програмне забезпечення LMS;

6. Exploitation for Privilege Escalation — використовуються вразливості в вебінтерфейсі або бекенді для підвищення рівня доступу атакуючого;

7. Obfuscated Files or Information — усі шкідливі скрипти або файли обфускуються, щоб обійти сигнатурні системи захисту або автоматизовані;

8. Input Capture — виконується перехоплення введеної користувачем інформації (наприклад, логінів, паролів) за допомогою кейлогерів або скриптів;

9. File and Directory Discovery — здійснюється пошук у файловій системі з метою виявлення чутливих документів, конфігурацій чи збережених облікових даних;

10. Exploitation of Remote Services — зловмисник використовує вразливі віддалені служби або хостинг, щоб поширитися вглиб інфраструктури;

11. Data from Information Repositories — відбувається збір інформації з баз даних або внутрішніх репозиторіїв, доступ до яких можливий через вебінтерфейс;

12. Web Service (C2) — зловмисник управляє скомпрометованою системою через легітимні вебсервіси, замаскувавши керування у стандартному трафіку;

13. Defacement — для нанесення репутаційної шкоди або відволікання уваги зловмисник змінює вміст вебсторінки (наприклад, замінює логотип, додає повідомлення або обмежує функціональність).

У цьому сценарії моделюється активний пошук атакуваним вебсайтів жертви, з подальшою компрометацією користувачів та збереженням постійного доступу до інфраструктури:

1. Search Victim–Owned Websites — зловмисник ідентифікує вебресурси, що належать організації-жертві, для аналізу їх структури та можливих точок входу;

2. Establish Accounts — створюються фальшиві або тестові облікові записи, які можуть бути використані пізніше в атаці;

3. Drive-by Compromise — через вразливі скрипти або модулі на вебсайті зловмисник впроваджує код, що автоматично виконується у браузері користувача;

4. User Execution — соціальна інженерія або електронна пошта з вкладенням спонукає користувача самостійно активувати шкідливий код;

5. Valid Accounts — легітимні облікові записи (отримані шляхом фішингу або збору даних) використовуються для входу в систему без викриття;

6. Obfuscated Files or Information — всі шкідливі компоненти ретельно маскуються, щоб уникнути детектування сигнатурними методами;

7. Input Capture — триває перехоплення даних користувача, особливо під час введення автентифікаційної інформації на вебформі;

8. System Information Discovery — здійснюється аналіз конфігурації операційної системи, зібрання інформації про встановлене ПЗ, мережеві параметри тощо;

9. Remote Services — для горизонтального переміщення або розширення впливу використовуються віддалені протоколи, наприклад, RDP, SSH або SMB;

10. Data from Information Repositories — отримується доступ до конфіденційних даних з баз даних або систем керування знаннями;

11. Exfiltration Over C2 Channel — дані передаються зловмиснику через заздалегідь підготовлений канал керування (C2);

12. Service Stop — на завершальному етапі можуть бути примусово зупинені ключові сервіси (наприклад, служби вебсервера або бази даних), щоб викликати збої або втрату доступу до системи.

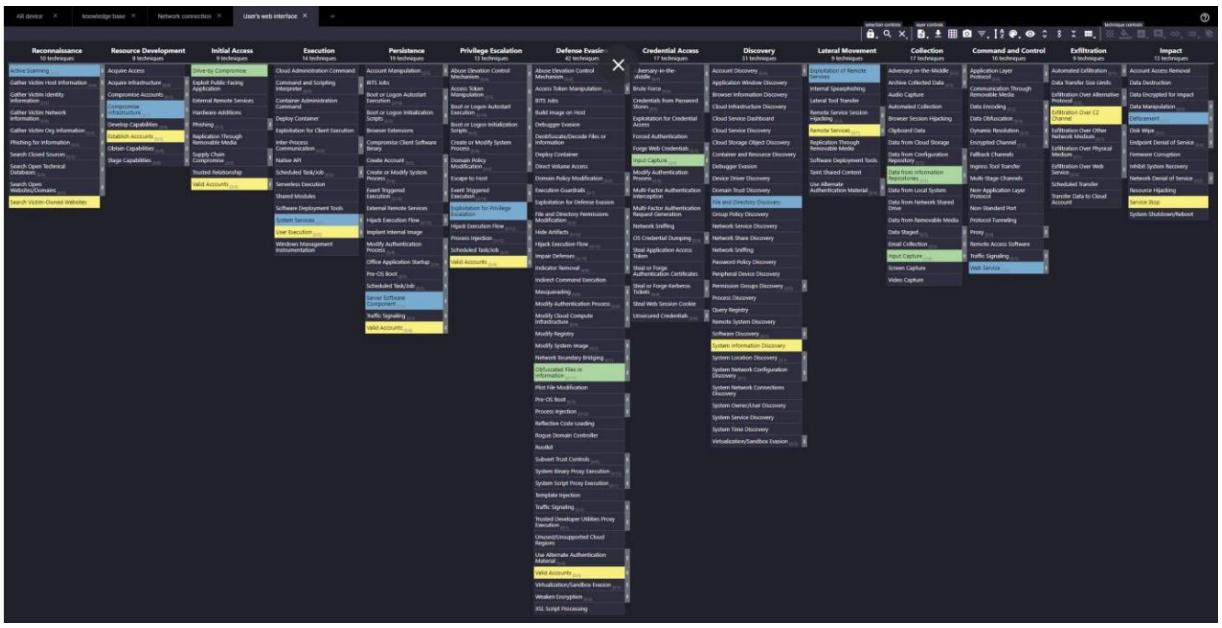


Рисунок 3.6– Вектори атак на веб інтерфейс користувача

Описані етапи охоплюють різноманітні тактики, які зловмисники можуть застосовувати для атаки на систему через вебінтерфейс. Важливо усвідомлювати, що кожен компонент системи — зокрема база даних LMS, мережеве з’єднання, вебінтерфейс користувача та пристрої доповненої реальності — має власні уразливості та може бути ціллю окремого вектору атаки.

Однак, з огляду на взаємозв’язок між цими компонентами, компрометація одного елемента потенційно може призвести до вторинного ураження інших частин системи. Тому для формування повної моделі загроз доцільно інтегрувати окремі вектори атак, що стосуються кожного компонента, у єдину схему. Це дозволяє моделювати цілісну картину атак на всю навчальну систему з елементами доповненої реальності (рис. 3.7).

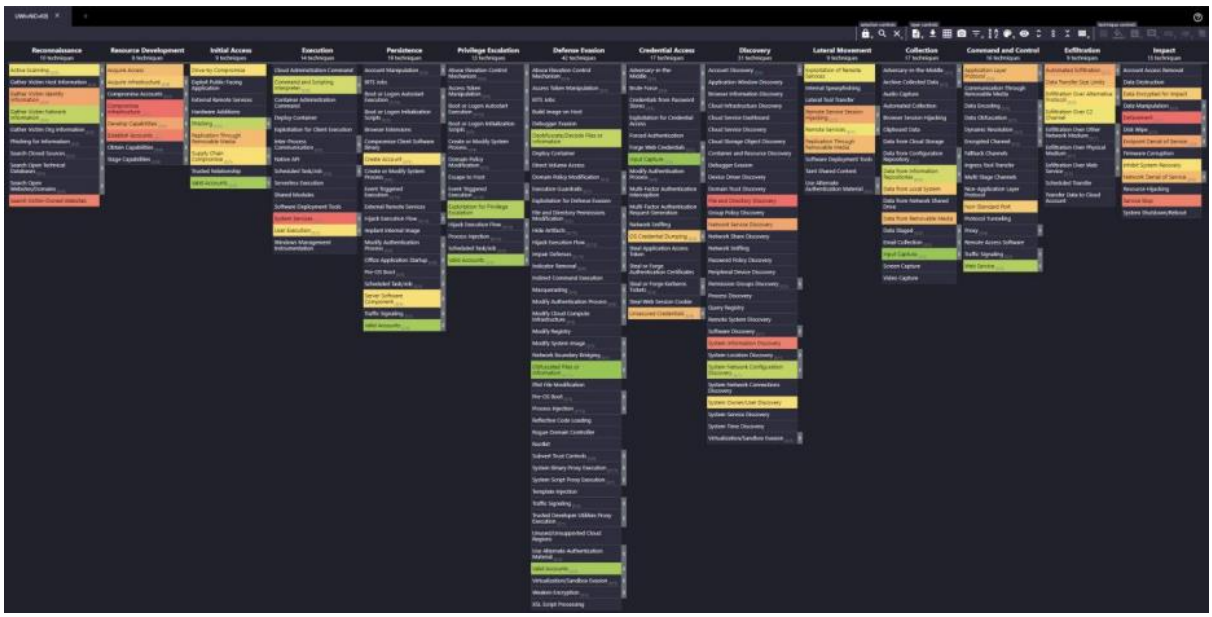


Рисунок 3.7 – Модель загроз безпеки навчальної системи з доповненою реальністю

MITRE ATT&CK Navigator є потужним інструментом для моделювання та візуалізації векторів атак у межах визначеного середовища. Однак, платформа має певні обмеження: зокрема, неможливість об’єднувати матриці з різних доменів. Це означає, що, наприклад, матриці з Enterprise ATT&CK не можуть бути безпосередньо інтегровані з матрицями з Mobile ATT&CK або ICS ATT&CK у межах одного шару. На рисунку 3.13 представлено результат такої багаторівневої візуалізації, де кожен шар показує окрему ATT&CK-матрицю із техніками, притаманними конкретному компоненту. Об’єднання цих шарів дозволяє сформувати узагальнений огляд загроз, які можуть впливати на систему загалом, з урахуванням взаємодії між її підсистемами.

Таким чином, MITRE ATT&CK Navigator стає не лише засобом візуалізації атак, а й інструментом стратегічного планування захисту. Завдяки можливості моделювати сценарії з урахуванням різних точок входу та взаємозв’язаних компонентів, платформа дозволяє виявити неочевидні шляхи атаки та розробити більш цілісну і ефективну архітектуру кібербезпеки.

ВИСНОВКИ

У результаті виконаної роботи було проведено комплексне дослідження автоматизованого моніторингу кіберзагроз в системах критичної інфраструктури. Розглянуто ключові поняття критичної інфраструктури, її роль у функціонуванні держави та особливості кіберзагроз, які становлять безпосередню небезпеку для таких об'єктів. Визначено, що порушення в роботі критичних систем може мати значні наслідки для національної безпеки, економіки та добробуту громадян, тому їхній захист потребує спеціалізованих, надійних і ефективних методів виявлення загроз.

У роботі проаналізовано сучасні стандарти та нормативно-правові документи, які регламентують вимоги до забезпечення кібербезпеки, зокрема міжнародні стандарти ISO/IEC 27000, IEC 62443, рекомендації NIST, а також українське законодавство. Особливу увагу приділено традиційним і сучасним технологіям моніторингу, серед яких сигнатурні методи, поведінковий аналіз, кореляція подій, машинне навчання та інтегровані системи класу SIEM, EDR, XDR.

Проведено огляд і порівняння сучасних інструментів автоматизованого виявлення загроз, таких як Wazuh, Splunk. Встановлено, що найефективнішими є рішення, які поєднують кілька підходів до детекції — наприклад, сигнатурний аналіз із поведінковою аналітикою або машинним навчанням. Вибір конкретного інструменту має враховувати потреби організації, тип інфраструктури, рівень загроз і наявні ресурси.

Окрему увагу приділено аналізу застосування фреймворку MITRE ATT&CK — як відкритої бази знань про поведінку зловмисників, яка дозволяє моделювати атаки, структурувати процеси моніторингу та створювати більш точні сценарії виявлення загроз. Використання MITRE ATT&CK Navigator на практиці підтвердило ефективність підходу до побудови візуальних профілів технік атак та покриття засобами безпеки.

Результати дослідження свідчать про необхідність і доцільність впровадження автоматизованих систем моніторингу кіберзагроз, заснованих на сучасних фреймворках, у критичну інфраструктуру. Такі рішення дозволяють своєчасно виявляти загрози, знижувати ризики, оптимізувати процес реагування на інциденти та забезпечити надійний захист життєво важливих інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Учасники проектів Вікімедіа. Об'єкти критичної інфраструктури – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Об'єкти_критичної_інфраструктури (дата звернення: 01.06.2025).

2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.06.2025).

3. Дія.Освіта – IT-студії. Дія.Освіта – IT-студії. URL: https://it-osvita.diia.gov.ua/task/item/4a074822-05ff-4a36-9c22-62d581b79717 (дата звернення: 01.06.2025).

4. Учасники проектів Вікімедіа. Кібератака на енергетичні компанії України – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_енергетичні_компанії_України (дата звернення: 01.06.2025).

5. Учасники проектів Вікімедіа. Кібератака на colonial pipeline – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_Colonial_Pipeline (дата звернення: 01.06.2025).

6. Розширене виявлення і реагування (Extended Detection and Response - XDR) | ESKA. ESKA. URL: https://eska.global/solutions/xdr (дата звернення: 01.06.2025).

7. Нова кібератака на банки була "найбільшою в історії України" й досі триває - BBC News Україна. BBC News Україна. URL: https://www.bbc.com/ukrainian/news-60401775 (дата звернення: 01.06.2025).

8. https://elit–web.ua/. URL: https://elit–web.ua/ua/blog/chto–takoe–ddos–ataki (дата звернення: 02.04.2025).

9. Шпаргалка MITM – HackYourMom. HackYourMom. URL: https://hackyourmom.com/kibervijna/shpargalka–mitm/ (дата звернення: 12.05.2025).

10. Шахрайські та фішингові сайти. Аналіз, тренди та рекомендації для клієнтів, 2022/2023 – Асоціація ЄМА. Асоціація ЄМА. URL: https://www.ema.com.ua/citizens/cyber-safety-school/shahrajski-ta-fishingovi-sajti-analiz-trendi-ta-rekomendacii-dlja-kliientiv-2022-2023/ (дата звернення: 01.06.2025).

11. Iso/iec 27001:2022. ISO. URL: https://www.iso.org/standard/27001 (дата звернення: 01.06.2025).

12. Системи виявлення загроз на кінцевих точках (EDR) і антивіруси. Amind. URL: https://www.amind.ua/ua-services/endpoint-detection-and-response-edr-and-antivirus (дата звернення: 01.06.2025).

13. IEC 62443 – промислова інформаційна безпека | Phoenix Contact. Access Denied. URL: https://www.phoenixcontact.com/uk-ua/standart-informatsiynoyi-bezpeky-iec-62443 (дата звернення: 01.06.2025).

14. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? | ESKA Блог. ESKA. URL: https://eska.global/blog/sho-take-upravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo (дата звернення: 01.06.2025).

15. Системи аналізу поведінки користувачів та сутностей | ESKA. ESKA. URL: https://eska.global/solutions/ueba (дата звернення: 01.06.2025).

16. Що таке IPS/IDS і де застосовується - Блог - HostZealot. HostZealot. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 01.06.2025).

17. What is SOAR? Security orchestration, automation, and response | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-soar (дата звернення: 01.06.2025).

18. MITRE ATT&CK Navigator. MITRE ATT&CK Navigator. URL: https://mitre.microfocus.com/layered-analytics (дата звернення: 01.06.2025).

19. IBM. What is the MITRE ATT&CK Framework? | IBM. IBM - United States. URL: https://www.ibm.com/think/topics/mitre-attack (дата звернення: 01.06.2025).

20. Matrix - Enterprise | MITRE ATT&CK®. MITRE ATT&CK®. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 01.06.2025).

21. Все, що ви хотіли знати про XDR. Trellix. Майбутнє XDR. Ми забезпечуємо безпеку. URL: https://trellix.bakotech.com/home/everything-you-ever-wanted-to-know--about-xdr (дата звернення: 01.06.2025).

22. Mitre att&ck®. MITRE ATT&CK®. URL: https://attack.mitre.org/ (дата звернення: 01.06.2025).

23. The zeek network security monitor. Zeek. URL: https://zeek.org/ (date of access: 01.06.2025).

24. Behavioral analytics in cybersecurity | splunk. Splunk. URL: https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html (дата звернення: 01.06.2025).

25. CrowdStrike Falcon - захист пристроїв в Києві та Україні | Netwave. Netwave. URL: https://netwave.ua/product/crowdstrike-falcon/ (дата звернення: 01.06.2025).

26. Mastering signature-based detection in cybersecurity: everything you need to know. Fidelis Security. URL: https://fidelissecurity.com/threatgeek/network-security/signature-based-detection/ (дата звернення: 01.06.2025).

27. Wazuh: SIEM and EDR for Cybersecurity. 4Geeks. URL: https://4geeks.com/lesson/wazuh-siem-and-edr-for-cybersecurity (дата звернення: 01.06.2025).

28. Splunk | the key to enterprise resilience. Splunk. URL: https://www.splunk.com/ (дата звернення: 01.06.2025).

29. Машинне навчання: що це, його методи, типи, які завдання вирішує та приклади застосування ML на практиці. De Novo. URL: https://denovo.ua/resources/what-is-machine-learning (дата звернення: 01.06.2025).

30. Кореляція подій у SIEM: бачити більше, діяти швидше. Головна | IT Specialist. URL: https://my-itspecialist.com/korelyatsiya-podiy-v-siem (дата звернення: 01.06.2025).

31. Зайцев М. І., Бученко І. А. Використання MITRE ATT&CK для виявлення та реагування на кіберзагрози в критичних системах. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. науково-практ. конф., м. Київ, 15 трав. 2025 р. Київ, 2025. Подано до друку.

32. Зайцев М. І., Бученко І. А. Інтеграція SIEM-систем для покращення кібербезпеки критичної інфраструктури. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. науково-практ. конф., м. Київ, 15 трав. 2025 р. Київ, 2025. Подано до друку.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯОСВІТНЬОГОСТУПЕНЯБАКАЛАВРА

на тему: «Автоматизовані методи моніторингу для виявлення кіберзагроз в системах критичної інфраструктури »

Виконав студент групи КІД-42
Зайцев Максим Ігорович

Керівник кваліфікаційної роботи:
Бученко Ігор Анатолійович, старший викладач кафедри КІ

Київ – 2025

Мета роботи – Підвищення ефективності виявлення кіберзагроз у системах критичної інфраструктури за рахунок впровадження автоматизованих методів моніторингу

Об`єкт дослідження – Процес моніторингу кіберзагроз у системах критичної інфраструктури

Предмет дослідження – Автоматизовані методи моніторингу для виявлення кіберзагроз в системах критичної інфраструктури.

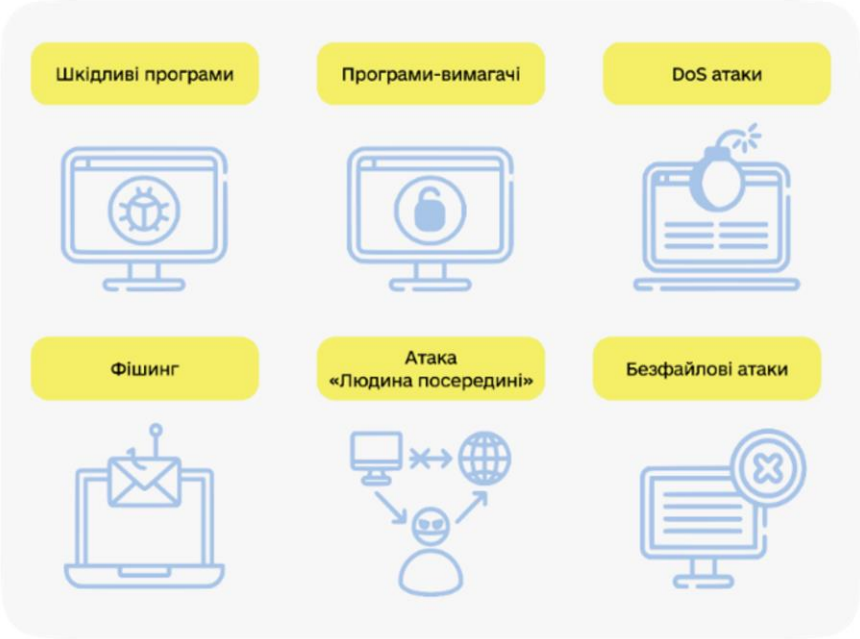
Актуальність обраної теми

У сучасному цифровому світі питання забезпечення кібербезпеки набуває особливої актуальності, особливу роль у цій архітектурі займають об’єкти критичної інфраструктури — системи, безперебійне функціонування яких є життєво важливим для національної безпеки, економічної стабільності та добробуту суспільства.

У зв’язку з цим забезпечення кібербезпеки критичної інфраструктури стає пріоритетним напрямом як для окремих держав, так і для міжнародних організацій. Одним із ключових викликів сучасності є те, що зростання цифровізації супроводжується зростанням кіберзагроз. Хакерські атаки, шкідливе програмне забезпечення, цілеспрямовані кампанії (APT–групи), соціальна інженерія та інші форми кіберзлочинності — усе це створює реальні ризики для стабільного функціонування критичних об’єктів.

3

Типові кіберзагрози



4

Стандарти і нормативна правова база в галузі кібербезпеки



Рисунок 1.8 – Логотип організації ISO зі стандартом 27001

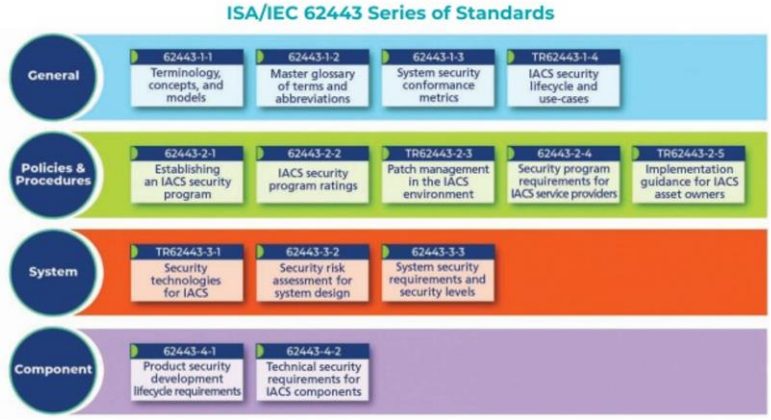


Рисунок 1.9 – Серія стандартів ISA/IEC 62443

5

Традиційні та сучасні методи моніторингу





6

Структура автоматизованого моніторингу



7

Типи автоматизовних систем моніторингу кіберзагроз

1. SIEM (рис.1.5);
2. EDR;
3. IDS/IPS (рис.1.11);
4. UEBA.

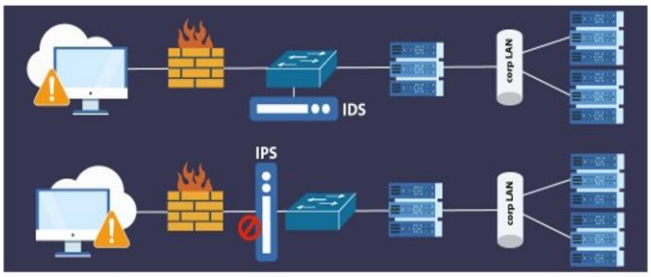


Рисунок 1.11 – Системи виявлення та запобігання вторгненням

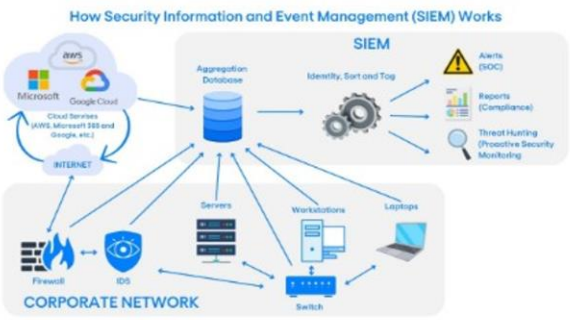


Рисунок 1.15– приклад схеми роботи SIEM рішення

8

Застосування фреймворку MITRE ATT&CK

Рисунок 2.4 - Процес моделювання векторів кібератак за допомогою ATT&CK Navigator



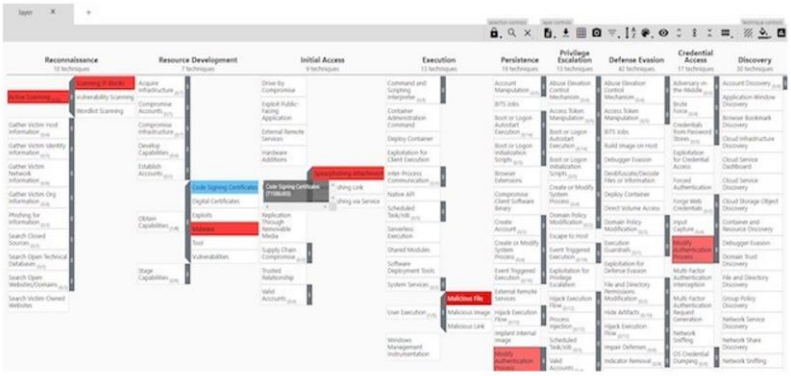
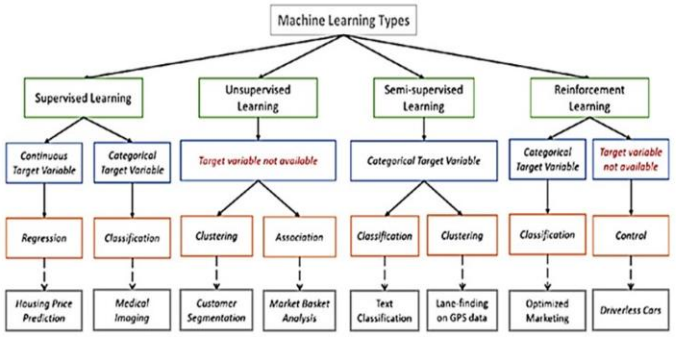


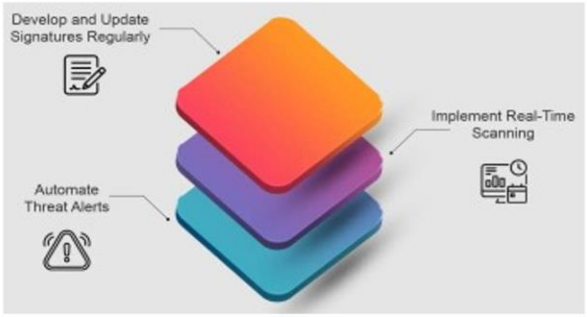
Рисунок 2.5 - Процес моделювання векторів кібератак за допомогою ATT&CK Navigator

9

Автоматизовані методи виявлення кіберзагроз

1. Сигнатурний аналіз
2. Поведінкова аналітика
3. Кореляція подій
4. Методи машинного навчання





10

Сучасні інтструменти автоматизованого виявлення

Таблиця 3.1 – порівняльна характеристика інструментів SIEM/EDR

Функція	Wazuh	Splunk
Збір та аналіз журналів	Комплексний	Екстенсивний
Оповіщення в режимі реального часу	Так	Так
Інтеграція розвідки загроз	Так	Так
Моніторинг цілісності файлів	Вбудований	Через доповнення
Звітність про відповідність	Екстенсивний	Комплексний
Масштабованість	Високий	Дуже високий
Інтеграція з хмарою	Сильний	Відмінно
Аналіз поведінки користувачів та сутностей (UEBA)	Обмежена	Розширений
Вартість	Відкритий код	Висока
Легкість розгортання	Помірний	Комплекс
Створення власного правила	Гнучкий	Висока гнучкість
Інтеграції зі сторонніми розробниками	Добре	Екстенсивний

11

Застосування MITRE ATT&CK Navigator для моделювання загроз



Рисунок 3.2 – Вектори атак на AR пристрої



Рисунок 3.4 – Вектори атак на бази знань LMS



Рисунок 3.6 – Вектори атак на веб-інтерфейс користувача



Рисунок 3.7 – Модель загроз безпеки навчальної системи з доповненою реальністю

12

ВИСНОВКИ

У результаті виконаної роботи було проведено комплексне дослідження автоматизованого моніторингу кіберзагроз в системах критичної інфраструктури. Розглянуто ключові поняття критичної інфраструктури, її роль у функціонуванні держави та особливості кіберзагроз, які становлять безпосередню небезпеку для таких об'єктів. Визначено, що порушення в роботі критичних систем може мати значні наслідки для національної безпеки, економіки та добробуту громадян, тому їхній захист потребує спеціалізованих, надійних і ефективних методів виявлення загроз.

У роботі проаналізовано сучасні стандарти та нормативно-правові документи, які регламентують вимоги до забезпечення кібербезпеки, зокрема міжнародні стандарти ISO/IEC 27000, IEC 62443, рекомендації NIST, а також українське законодавство. Особливу увагу приділено традиційним і сучасним технологіям моніторингу, серед яких сигнатурні методи, поведінковий аналіз, кореляція подій, машинне навчання та інтегровані системи класу SIEM, EDR, XDR.

13

ПРОДОВЖЕННЯ ВИСНОВКІВ

Проведено огляд і порівняння сучасних інструментів автоматизованого виявлення загроз, таких як Wazuh, Splunk. Встановлено, що найефективнішими є рішення, які поєднують кілька підходів до детекції — наприклад, сигнатурний аналіз із поведінковою аналітикою або машинним навчанням. Вибір конкретного інструменту має враховувати потреби організації, тип інфраструктури, рівень загроз і наявні ресурси.

Окрему увагу приділено аналізу застосування фреймворку MITRE ATT&CK — як відкритої бази знань про поведінку зловмисників, яка дозволяє моделювати атаки, структурувати процеси моніторингу та створювати більш точні сценарії виявлення загроз. Використання MITRE ATT&CK Navigator на практиці підтвердило ефективність підходу до побудови візуальних профілів технік атак та покриття засобами безпеки.

Загалом, результати дослідження свідчать про необхідність і доцільність впровадження автоматизованих систем моніторингу кіберзагроз, заснованих на сучасних фреймворках, у критичну інфраструктуру. Такі рішення дозволяють своєчасно виявляти загрози, знижувати ризики, оптимізувати процес реагування на інциденти та забезпечити надійний захист життєво важливих інформаційних систем.

14

РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ

1. Зайцев М. І., Бученко І. А. Інтеграція SIEM-систем для покращення кібербезпеки критичної інфраструктури. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. науково-практ. конф., м. Київ, 15 трав. 2025 р. Київ, 2025. Подано до друку

2. Зайцев М. І., Бученко І. А. Використання MITRE ATT&CK для виявлення та реагування на кіберзагрози в критичних системах. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. науково-практ. конф., м. Київ, 15 трав. 2025 р. Київ, 2025.Подано до друку