ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**Аналіз безпеки протоколів зв'язку для інтернету речей IoT**»

на здобуття освітнього ступеня магістра

зі спеціальності 172 «Електронні комунікації та радіотехніка»

освітньо-професійної програми «Телекомунікаційні системи та мережі»

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

_____ Данііл ДУЖИК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. ТСДМ-61
Данііл ДУЖИК
Ім'я, ПРІЗВИЩЕ

Керівник: Олексій ГЕТЬМАНЕЦЬ
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 телекомунікацій

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти магістр
Спеціальність 172 «Електронні комунікації та радіотехніка»
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою ТСМ
Віктор ЗАЇКА Ім'я, ПРІЗВИЩЕ
«____» _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дужик Даніїл Євгенович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Аналіз безпеки протоколів зв'язку для інтернету речей IoT»
керівник кваліфікаційної роботи Олексій Гетьманець, канд. техн. наук
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 30 жовтня 2025 р. № 467
2. Строк подання кваліфікаційної роботи «___» _____ 20__ р.
3. Вихідні дані до кваліфікаційної роботи: методи забезпечення інформаційної безпеки в мережі Інтернету речей, загрози інформаційної безпеки Інтернету речей (CVE-2017- 7253, CVE-2021-33044, CVE-2021-36260), методи оцінювання ризику (матриці ймовірності та наслідків, Return of Security Investment)
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд об'єкту захисту.
2. Огляд основних загроз та методів забезпечення інформаційної безпеки Інтернету речей в мережах.
3. Дослідження пристроїв Інтернету речей на наявність відомих вразливостей.
4. Аналіз ефективності методів захисту та оцінка ризиків інформаційної безпеки Інтернету речей
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «___» _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Отримання завдання*	*20.09.2025*	
2	*Збір матеріалів для дослідження*	*7.10.2025*	
3	*Розробка 1 розділу*	*21.10.2025*	
4	*Розробка 2 розділу*	*10.11.2025*	
5	*Розробка 3 розділу*	*01.12.2025*	
6	*Розробка 4 розділу*	*13.12.2025*	
7	*Оформлення кваліфікаційної роботи*	*30.12.2025*	

Здобувач(ка) вищої освіти _____ Даніїл ДУЖИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Олексій ГЕТЬМАНЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Пояснювальна записка: 80 с., 32 рис., 2 табл., 13 джерел.

КЛЮЧОВІ СЛОВА: CVE, IOT, IP-КАМЕРИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, МЕРЕЖІ, МЕТОДИ ЗАХИСТУ, ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ, ДОСЛІДЖЕННЯ.

Об’єктом дослідження є сукупність процесів, пов’язаних із забезпеченням інформаційної безпеки в інфраструктурі Інтернету речей.

Предмет дослідження — методи, моделі та практичні підходи до підвищення рівня інформаційної безпеки в мережах Інтернету речей.

Метою кваліфікаційної роботи є зменшення рівня ризиків інформаційної безпеки в IoT-системах шляхом обґрунтованого вибору та впровадження ефективних методів захисту інформації.

Методи дослідження – порівняння, емпіричний аналіз, розрахунки.

У ході виконання роботи застосовано такі методи дослідження: аналітичне узагальнення та порівняння, емпіричний аналіз, а також розрахункові методи оцінювання ризиків.

Інтенсивний розвиток інформаційно-комунікаційних технологій сприяв широкому впровадженню інтелектуальних систем управління та сервісів. За цих умов проблема забезпечення інформаційної безпеки набуває особливої актуальності.

Активне використання рішень Інтернету речей супроводжується зростанням кількості потенційних загроз, що зумовлює фундаментальний характер завдань із захисту інформації.

У межах дослідження проведено аналіз сучасних методів забезпечення інформаційної безпеки в мережах Інтернету речей.

Визначено основні загрози та проблемні аспекти функціонування IoT-систем, а також сформульовано рекомендації щодо застосування відповідних засобів захисту.

Виконано дослідження ефективності методів забезпечення інформаційної безпеки з використанням загальновідомих уразливостей.

На основі отриманих результатів здійснено якісне та кількісне оцінювання ризиків.

У результаті якісного аналізу сформовано перелік пріоритетних ризиків, які надалі були піддані кількісній оцінці.

ABSTRACT

An explanatory note: 80 p., 32 fig., 2 tables, 13 sources.

KEYWORDS: CVE, IOT, IP CAMERAS, INFORMATION SECURITY, CYBER THREATS, NETWORKS, PROTECTION METHODS, EFFICIENCY ASSESSMENT, RESEARCH.

The object of the research is the set of processes related to ensuring information security within the Internet of Things infrastructure.

The subject of the research comprises methods, models, and practical approaches aimed at improving the level of information security in Internet of Things networks.

The purpose of this qualification work is to reduce information security risks in IoT systems through the justified selection and implementation of effective information protection methods.

The research methods applied in this work include analytical generalization and comparison, empirical analysis, as well as calculation-based risk assessment methods.

The intensive development of information and communication technologies has contributed to the widespread implementation of intelligent control systems and services. Under these conditions, the problem of ensuring information security becomes particularly relevant.

The active use of Internet of Things solutions is accompanied by an increase in the number of potential threats, which determines the fundamental nature of information protection tasks.

Within the scope of the study, an analysis of modern methods for ensuring information security in Internet of Things networks was conducted.

The main threats and problematic aspects of IoT system operation were identified, and recommendations for the application of appropriate protection measures were formulated.

The effectiveness of information security methods was studied using well-known vulnerabilities.

Based on the obtained results, qualitative and quantitative risk assessments were carried out.

As a result of qualitative analysis, a list of priority risks was formed, which was subsequently subjected to quantitative evaluation.

ЗМІСТ

Перелік скорочень, умовних позначень, символів, одиниць і термінів… 7
Вступ 9
1 Огляд об’єкту захисту 13
1.1 Перспективи розвитку Інтернету речей 13
1.2 Типи мереж Інтернету речей 14
1.3 Комунікаційні протоколи та стандарти Інтернету речей 16
1.4 Архітектура Інтернету речей…… 20
2 Огляд основних загроз та методів забезпечення інформаційної безпеки інтернету речей в мережах 22
2.1 Огляд загроз інформаційної безпеки Інтернету речей 22
2.2 Огляд основних вимог щодо безпеки мережі Інтернету речей 34
3 Дослідження пристроїв Інтернету речей на наявність відомих вразливостей 38
3.1 Загальні положення 38
3.2 Опис методів сканування елементів мережі 39
3.3 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2017-7253 46
3.4 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2021-33044 50
3.5 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2021-36260 58
4 Аналіз ефективності методів захисту та оцінка ризиків інформаційної безпеки Інтернету речей 75
4.1 Загальні положення 75
4.2 Аналіз ефективності методів захисту методом матриці ймовірності та наслідків 76
4.3 Аналіз ефективності методів захисту методом Return of Security Investment 81
Висновки 84
Перелік джерел посилання 86

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ПЗ – програмне забезпечення
ALE – annualized loss expectancy
AMQP – advanced message queuing protocol
API – application programming interface
ARO – annualized rate of occurrence
BAN – body area network
BLE – bluetooth low-energy
CAN – corporate area network
CoAP – constrained application protocol
CVE – common vulnerabilities and exposures
DDoS – distributed denial of service
DDS – data distribution service
FTP – file transfer protocol
HTTP – hypertext transfer protocol
HTTPS – hypertext transfer protocol secure
IoT – internet of things
IP – internet protocol
JtR – john the ripper
JWT – json web token
LAN – local area network
LoRaWAN – long range wide area network
MAC – media access control
MAN – metropolitan area network
MD – message-digest algorithm
MQQT – message queue telemetry transport
NFC – near-field communication
Nmap – network mapper
P2P – peer-to-peer
PAN – personal area network
PoC – proof of concept

ROSI – return of security investment
RTSP – real time streaming protocol
SD – secure digital
SHA – secure hash algorithm
SLE – single loss expectancy
SSH – secure shell
SSL – secure sockets layer
SYN – synchronize
TCP – transmission control protocol
TLS – transport layer security
UDP – user datagram protocol
UPnP – universal plug and play
URI – uniform resource identifier
VLAN – virtual local area network
WAN – wide area network
Wi-Fi – wireless fidelity
XML – extensible markup language

ВСТУП

Забезпечення інформаційної безпеки на сучасному етапі розвитку інформаційних технологій є однією з ключових науково-практичних проблем. Стрімка цифровізація та активне впровадження інтелектуальних інформаційних систем зумовили широке поширення концепції Інтернету речей (Internet of Things, IoT), для якої питання захисту інформації набувають особливої актуальності та системного характеру.

Під Інтернетом речей у науковій літературі зазвичай розуміють глобальну динамічну мережеву інфраструктуру, що функціонує на основі стандартизованих і сумісних протоколів зв'язку та забезпечує взаємодію фізичних і віртуальних об'єктів, наділених унікальними ідентифікаторами, фізичними характеристиками й інтелектуальними інтерфейсами. Практична реалізація промислових IoT-рішень уже знайшла застосування у таких галузях, як сільське господарство, харчова промисловість, системи відеоспостереження, екологічний моніторинг та інші сфери. Водночас ефективне впровадження IoT-пристроїв у промислових умовах потребує попереднього врахування галузевої специфіки, а також вимог до рівня безпеки, вартості, конфіденційності та можливих ризиків.

Однією з основних проблем функціонування мереж Інтернету речей є недостатній рівень захисту від несанкціонованого доступу та зовнішнього впливу. У разі успішної кібератаки наслідки можуть варіюватися від матеріальних збитків до створення загроз життю та здоров'ю людини. IoT-пристрої, підключені до глобальної мережі, у разі компрометації можуть бути використані зловмисниками для віддаленого керування обладнанням, зокрема критично важливими системами життєзабезпечення та промислової безпеки.

З метою досягнення поставленої мети в першому розділі роботи розглянуто перспективи розвитку концепції Інтернету речей, а також проаналізовано основні технології й стандарти, що забезпечують комутацію та конвергенцію IoT-інфраструктури. Досліджено можливі варіанти інтеграції IoT-пристроїв з наявними мережами та наведено загальну архітектуру Інтернету речей.

У другому розділі виконано аналіз основних проблем і загроз інформаційної безпеки Інтернету речей у мережевому середовищі, а також розглянуто сучасні методи та засоби захисту інформації.

Третій розділ присвячено дослідженню IoT-пристроїв із використанням відомих уразливостей інформаційної безпеки та аналізу вимог нормативного забезпечення. Запропоновано підходи до сканування IoT-пристроїв із застосуванням

інструментів Network Mapper (Nmap) та пошукової системи Shodan. Проведено аналіз результатів сканування мережевих портів і активних сервісів із формуванням відповідних висновків.

У четвертому розділі здійснено якісну та кількісну оцінку ризиків інформаційної безпеки. На основі якісного аналізу визначено перелік пріоритетних ризиків, які в подальшому були піддані кількісному оцінюванню. У ході кількісної оцінки встановлено ступінь впливу імовірних загроз на цільові показники проєкту з урахуванням ймовірності їх реалізації. Обґрунтовано ефективність запропонованих методів захисту, впровадження яких дозволило суттєво знизити кінцевий рівень ризику та підвищити загальний рівень безпеки споживчих IoT-систем.

Окремі результати дослідження були представлені та апробовані на міжнародних наукових конференціях [1–3].

1 ОГЛЯД ОБ’ЄКТУ ЗАХИСТУ

1.1 Перспективи розвитку Інтернету речей

Стрімкий розвиток інформаційних технологій сприяв активному формуванню інтелектуальних систем управління та сервісів. За цих умов Інтернет речей (IoT) сформувався як окремий напрям, що динамічно розвивається. Його впровадження сприяє трансформації традиційних виробничих процесів і повсякденного способу життя у більш автоматизований та «розумний» формат, що дозволяє підвищити ефективність соціально-економічних процесів і якість життя населення. Концепцію IoT часто розглядають як черговий етап еволюції світової інформаційної індустрії після появи персональних комп’ютерів та глобальної мережі Інтернет.

Інтернет речей характеризується наявністю великої кількості об’єктних пристроїв, автономною взаємодією кінцевих вузлів та повсюдним інтелектуальним сервісним середовищем. IoT являє собою складну інтегровану мережеву систему, здатну об’єднувати комунікаційну та галузеву інфраструктуру, забезпечуючи ефективне використання інформаційних і телекомунікаційних ресурсів у різних сферах діяльності. Це, у свою чергу, сприяє підвищенню рівня цифровізації галузей та вдосконаленню існуючої інфраструктури.

Незважаючи на значний потенціал застосування, розвиток Інтернету речей у різних секторах відбувається нерівномірно. Загалом IoT все ще перебуває на стадії становлення, оскільки багато технологій, стандартів, продуктів і ринкових механізмів залишаються недостатньо зрілими. Водночас у таких напрямах, як інформаційна безпека, розумні будинки, енергетика, транспорт, охорона здоров’я та логістика, концепція IoT поступово знаходить практичне застосування. Відмінності у державній політиці, технологічному розвитку та ринкових умовах зумовлюють суттєві диспропорції у розвитку окремих сегментів ринку Інтернету речей.

Подальший розвиток IoT супроводжується низкою викликів, серед яких ключовими є питання безпеки та конфіденційності, захисту даних, управління ресурсами, обміну інформацією, стандартизації та відкритості сервісів. Очікується, що протягом найближчих років технології Інтернету речей продовжать активно розвиватися та набудуть широкого поширення.

1.2 Типи мереж Інтернету речей

Мережі поділяються на категорії залежно від діапазону відстаней, які вони забезпечують. На рис. 1.1 наведено типи мереж IoT, що мають такі властивості та сфери застосування:

- Nano-мережі являють собою сукупність надмалих пристроїв, розміри яких зазвичай не перевищують кількох мікрометрів, та які призначені для виконання елементарних функцій, зокрема виявлення параметрів, оброблення, збереження інформації й керування виконавчими механізмами. Такі мережі знаходять застосування у біометричних системах, оборонній сфері та різних напрямах нанотехнологій. У галузі охорони здоров'я nano-мережі можуть використовуватися для збору критично важливих медичних даних пацієнтів і передавання їх до інформаційних систем, що дозволяє підвищити точність та ефективність медичного моніторингу. Окрім виявлення патологічних утворень, зокрема пухлин, концепція Internet of Nano-Things у медичних системах відкриває можливості для проведення детальної діагностики та підтримки процесу лікування шляхом застосування високоточних і локалізованих лікарських засобів;
- Near-Field Communication (NFC) — це технологія короткодіапазонного бездротового зв'язку з невисокою швидкістю передавання даних, яка забезпечує взаємодію електронних пристроїв на відстані кількох сантиметрів. Завдяки обмеженому радіусу дії NFC широко використовується у системах безконтактної оплати, електронних ідентифікаційних документах, а також у рішеннях контролю доступу, зокрема у вигляді карт-ключів;
- Body Area Network (BAN) — це тип мережі, призначений для об'єднання носимих обчислювальних пристроїв, які можуть розміщуватися безпосередньо на тілі людини, поблизу нього або імплантуватися всередину організму. Такі мережі забезпечують обмін даними між сенсорами та іншими пристроями, що функціонують у режимі реального часу. BAN широко застосовується у медичних системах для моніторингу стану здоров'я, у рішеннях для підвищення рівня особистої безпеки та благополуччя, а також у сфері спорту й рекреації;
- Personal Area Network (PAN) — це різновид мережі, що забезпечує взаємодію електронних пристроїв у межах невеликого простору, зазвичай однієї або кількох кімнат. Прикладом використання PAN є ситуація, коли користувач одночасно застосовує портативний комп'ютер, персональний цифровий помічник та бездротовий принтер, об'єднуючи їх у єдину мережу без необхідності фізичного

підключення. Такі мережі можуть функціонувати автономно або бути інтегрованими з Інтернетом чи іншими мережевими інфраструктурами за допомогою бездротових технологій;

- Local Area Network (LAN) – це локальна мережа, що охоплює обмежену територію, зокрема одну будівлю або окремий офісний простір. У межах LAN комп'ютери та мобільні пристрої мають можливість спільного використання ресурсів, таких як периферійне обладнання або мережеві сховища даних, завдяки локальному підключенню. Основними технологіями побудови LAN є Ethernet і Wireless Fidelity (Wi-Fi). Ethernet являє собою стандартизовану технологію дротового з'єднання, яка забезпечує взаємодію між пристроями, тоді як Wi-Fi використовує радіохвилі для бездротового обміну даними між комп'ютерами, принтерами, мобільними телефонами та іншими пристроями;
- Corporate Area Network (CAN) — це тип мережі, призначений для об'єднання кількох локальних мереж у межах обмеженої території, такої як підприємство, навчальний заклад або організаційний комплекс. CAN забезпечує централізоване керування мережевими ресурсами та підтримує ефективний обмін даними між підрозділами в рамках єдиної інфраструктури;
- Metropolitan Area Network (MAN) — це масштабна мережа, призначена для охоплення території міста або великого населеного пункту, у якій для передавання даних часто застосовуються мікрохвильові та інші бездротові технології. Використання MAN створює технічні передумови для впровадження концепції «розумного міста», що передбачає інтеграцію міської інфраструктури з цифровими сервісами. Інтернет речей відіграє ключову роль у розробленні таких систем, спрямованих на забезпечення сталого розвитку, підвищення рівня комфорту та ефективності життєдіяльності міського населення;
- Wide Area Network (WAN) — це мережа, що функціонує на значних географічних відстанях та поєднує різні типи локальних і регіональних мереж, зокрема LAN і MAN. У межах Інтернету речей WAN широко використовується для підключення розподілених сенсорних систем, призначених для фіксації змін фізичного або логічного стану об'єктів та навколишнього середовища. До фізичних параметрів, що підлягають моніторингу, належать температура, освітленість, тиск, рівень шуму та рух, тоді як логічні зміни можуть відображати наявність чи відсутність об'єкта, його місцезнаходження або характер активності. У контексті IoT як фізичні, так і логічні дані мають однакове значення для прийняття рішень. Подібні мережеві рішення широко застосовуються у промислових системах та різних галузевих вертикалях для забезпечення комплексного моніторингу й управління процесами.

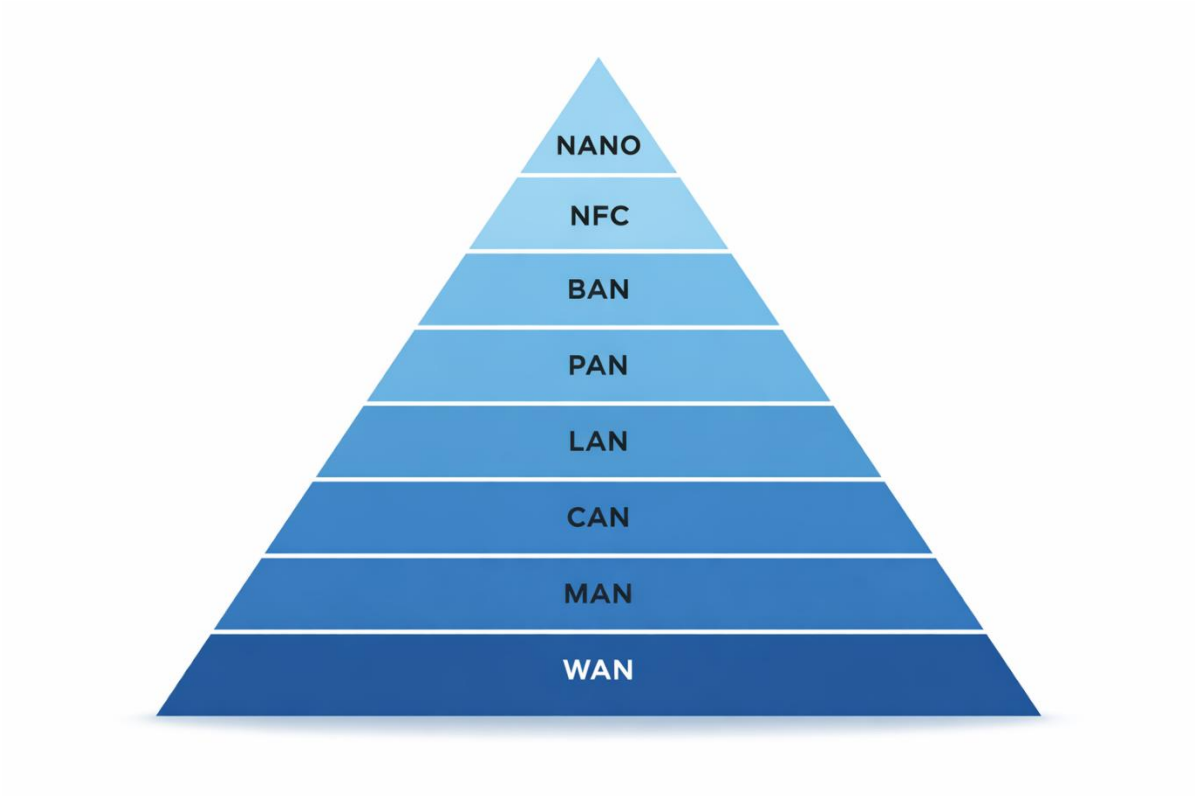


Рисунок 1.1 – Типи мереж IoT

1.3 Комунікаційні протоколи та стандарти Інтернету речей

Протоколи Інтернету становлять невід'ємний компонент технологічного стеку Інтернету речей. За відсутності відповідних протоколів і стандартів апаратні засоби IoT не здатні повноцінно функціонувати, оскільки саме вони забезпечують обмін даними між пристроями. Отримані в результаті передавання дані обробляються та перетворюються на корисну інформацію, доступну кінцевому користувачу.

Під час розгляду концепції Інтернету речей протоколам і стандартам часто приділяється недостатньо уваги, оскільки основний акцент зазвичай робиться на сам процес взаємодії між компонентами системи. Хоча зв'язок між IoT-пристроями, сенсорами, шлюзами, серверною інфраструктурою та користувацькими застосунками є важливою складовою IoT, без коректно підібраних протоколів передавання даних така взаємодія не може бути реалізована належним чином.

Протоколи та стандарти IoT можна розділити на дві окремі групи:

- протоколи обміну даними IoT, що відповідають рівням представлення та прикладному рівню;мережеві протоколи для IoT (канал передачі даних/фізичний рівень)
- мережеві протоколи IoT, які функціонують на фізичному рівні та рівні каналу передавання даних

Обмін даними в межах протоколів і стандартів Інтернету речей може здійснюватися як через дротові, так і через бездротові або стільникові мережі зв'язку. Залежно від вимог до швидкості передавання, надійності та енергоспоживання застосовуються різні протоколи обміну даними IoT, серед яких найбільш поширеними є такі:

- Message Queue Telemetry Transport (MQTT) — це полегшений протокол обміну повідомленнями, призначений для передавання невеликих обсягів даних від сенсорів до прикладних програм або проміжного програмного забезпечення. MQTT працює поверх стеку TCP/IP та реалізує модель взаємодії «видавець–передплатник», яка включає три основні компоненти: видавця, передплатника та брокера. Видавець формує та надсилає повідомлення, передплатники їх отримують, а брокер виконує функції маршрутизації, автентифікації та забезпечення безпеки. Завдяки низьким вимогам до ресурсів MQTT добре підходить для недорогих IoT-пристроїв із обмеженою пам'яттю та низьким енергоспоживанням;
- Data Distribution Service (DDS) є масштабованим протоколом обміну даними, орієнтованим на забезпечення високоякісного та надійного зв'язку в IoT-системах. Подібно до MQTT, DDS використовує модель «видавець–передплатник», однак може бути розгорнутий у широкому діапазоні середовищ — від хмарних платформ до вбудованих пристроїв. Це робить його придатним для систем реального часу. Важливою перевагою DDS є незалежність обміну даними від апаратної та програмної платформи, що дозволяє вважати його одним із перших відкритих міжнародних стандартів проміжного програмного забезпечення для IoT;
- Advanced Message Queuing Protocol (AMQP) — це відкритий прикладний протокол, який використовується для організації надійного обміну транзакційними повідомленнями між серверними компонентами. Основними функціями AMQP є приймання повідомлень, їх розміщення у чергах та зберігання до моменту безпечної обробки клієнтською програмою, а також встановлення логічних зв'язків між компонентами системи. Завдяки високому рівню безпеки та надійності AMQP найчастіше застосовується в серверних аналітичних середовищах, зокрема у фінансовій сфері. Водночас через значні накладні витрати

цей протокол малопридатний для сенсорних IoT-пристроїв з обмеженими ресурсами, що обмежує його використання в IoT;

- HyperText Transfer Protocol (HTTP) є базовим протоколом передавання даних у Всесвітній павутині. Незважаючи на широке поширення, HTTP не вважається оптимальним вибором для IoT-рішень через високі накладні витрати, значне енергоспоживання та негативний вплив на автономність пристроїв. Проте в окремих галузях цей протокол все ще використовується для реалізації IoT-сервісів;
- Constrained Application Protocol (CoAP) — це протокол прикладного рівня, розроблений спеціально для пристроїв з обмеженими обчислювальними ресурсами. Він базується на концепціях HTTP, але адаптований для використання в енергообмежених IoT-системах. CoAP характеризується низькими накладними витратами, простотою реалізації та підтримкою багатоадресної передачі, що робить його ефективною альтернативою HTTP для Інтернету речей;
- WebSocket – це протокол зв'язку, який працює поверх TCP-з'єднання та забезпечує двосторонній обмін повідомленнями між клієнтом і сервером у режимі реального часу. Завдяки використанню одного постійного з'єднання WebSocket зменшує затримки та спрощує обмін даними. Подібно до CoAP, цей протокол дозволяє оптимізувати керування з'єднаннями та зменшити накладні витрати під час взаємодії між компонентами IoT-систем.

Мережеві протоколи Інтернету речей призначені для організації підключення та взаємодії пристроїв у межах мережевої інфраструктури. Як правило, ці протоколи базуються на технологіях, що широко застосовуються в глобальних і локальних мережах. Нижче наведено найбільш поширені мережеві протоколи, які використовуються в IoT-системах:

- Wi-Fi – це одна з найвідоміших технологій бездротового зв'язку, що забезпечує високу швидкість передавання даних і здатна обробляти значні обсяги інформації. У контексті Інтернету речей Wi-Fi використовується для підключення пристроїв, які не мають жорстких обмежень щодо енергоспоживання. Технологія працює на радіочастотах 2,4 ГГц та 5 ГГц, кожна з яких поділяється на окремі канали, що дозволяє зменшити рівень перевантаження бездротових мереж і підвищити стабільність з'єднання;
- Bluetooth – є технологією короткодіапазонного зв'язку, інтегрованою в більшість сучасних смартфонів та мобільних пристроїв, що робить її зручною для персональних IoT-рішень. Значним кроком у розвитку цієї технології стало впровадження стандарту Bluetooth Low Energy (BLE), також відомого як Bluetooth Smart. BLE орієнтований на мінімізацію енергоспоживання та підтримує масштабованість, що робить його придатним для широкого спектра IoT-додатків і

гнучким до ринкових інновацій;

- ZigBee – це легкий протокол пакетного передавання даних, який зазвичай застосовується у системах з невисокими вимогами до пропускної здатності, таких як мікроконтролери та сенсорні пристрої. Однією з його переваг є можливість масштабування мережі до великої кількості вузлів. Водночас порівняно з Bluetooth ZigBee має меншу дальність передавання даних, але характеризується низьким енергоспоживанням і високим рівнем безпеки;
- Z-Wave – є популярною технологією бездротового зв’язку, яка переважно використовується в системах домашньої автоматизації. Протокол функціонує в діапазоні радіочастот 800–900 МГц, що дозволяє зменшити рівень завад, характерних для діапазону 2,4 ГГц, у якому працюють Wi-Fi та ZigBee. Особливістю Z-Wave є залежність робочої частоти від регіону використання, що потребує врахування під час вибору обладнання. Найбільш ефективно цей протокол застосовується у побутових IoT-рішеннях, тоді як у корпоративних середовищах його використання є обмеженим;
- Long Range Wide Area Network (LoRaWAN) – це мережевий протокол, призначений для побудови масштабних глобальних IoT-мереж. Він орієнтований на підтримку великої кількості малопотужних пристроїв, зокрема в проєктах «розумних міст». LoRaWAN забезпечує економічно ефективний, безпечний та двосторонній обмін даними на значних відстанях, що зумовлює його широке застосування в різних галузях.

1.4 Архітектура Інтернету речей

Архітектура IoT – це система з безлічі елементів, таких як датчики, приводи, протоколи, хмарні сервіси та рівні, що складають мережеву систему IoT.

Єдиного консенсусу з архітектури IoT немає, оскільки різні дослідники пропонували різні архітектури. Переважають три-, чотири- та п’яти рівневі архітектури.

Розглянемо класичну архітектуру Інтернету речей, що включає чотири рівні.

1) Сенсорний рівень. IoT-пристрої збирають показання з датчиків та виконують фізичні дії. Ці датчики або приводи приймають дані (фізичні параметри/параметри навколишнього середовища), обробляють дані та передають дані мережею.

2) Мережевий рівень. Даний рівень забезпечує передавання даних між сенсорними пристроями та іншими компонентами системи. Його основу складають шлюзи, які отримують інформацію від IoT-пристроїв і передають команди керування у зворотному напрямку. Такі шлюзи можуть бути реалізовані як апаратні маршрутизатори або програмні рішення та використовують різноманітні мережеві протоколи. Окрім функцій передавання даних, розширені шлюзи можуть виконувати завдання фільтрації трафіку, захисту від шкідливого програмного забезпечення, а також приймати елементарні рішення на основі отриманих даних.

3) Рівень обробки даних. На цьому рівні відбувається зберігання, оброблення та аналітичний аналіз даних, отриманих від сенсорів. Зазвичай він реалізується у вигляді серверної інфраструктури, яка може базуватися на фізичних серверах, віртуальних машинах або хмарних технологіях. Оброблені дані надалі передаються до центрів обробки даних або безпосередньо використовуються прикладними сервісами.

4) Рівень додатків. Цей рівень відповідає за взаємодію з кінцевим користувачем і реалізується у вигляді мобільних або веб-застосунків. Він забезпечує доступ до даних IoT-пристроїв, керування системою та наочне відображення результатів аналізу у зручному для користувача форматі.

На рис. 1.2 зображено класичну еталонну модель IoT.

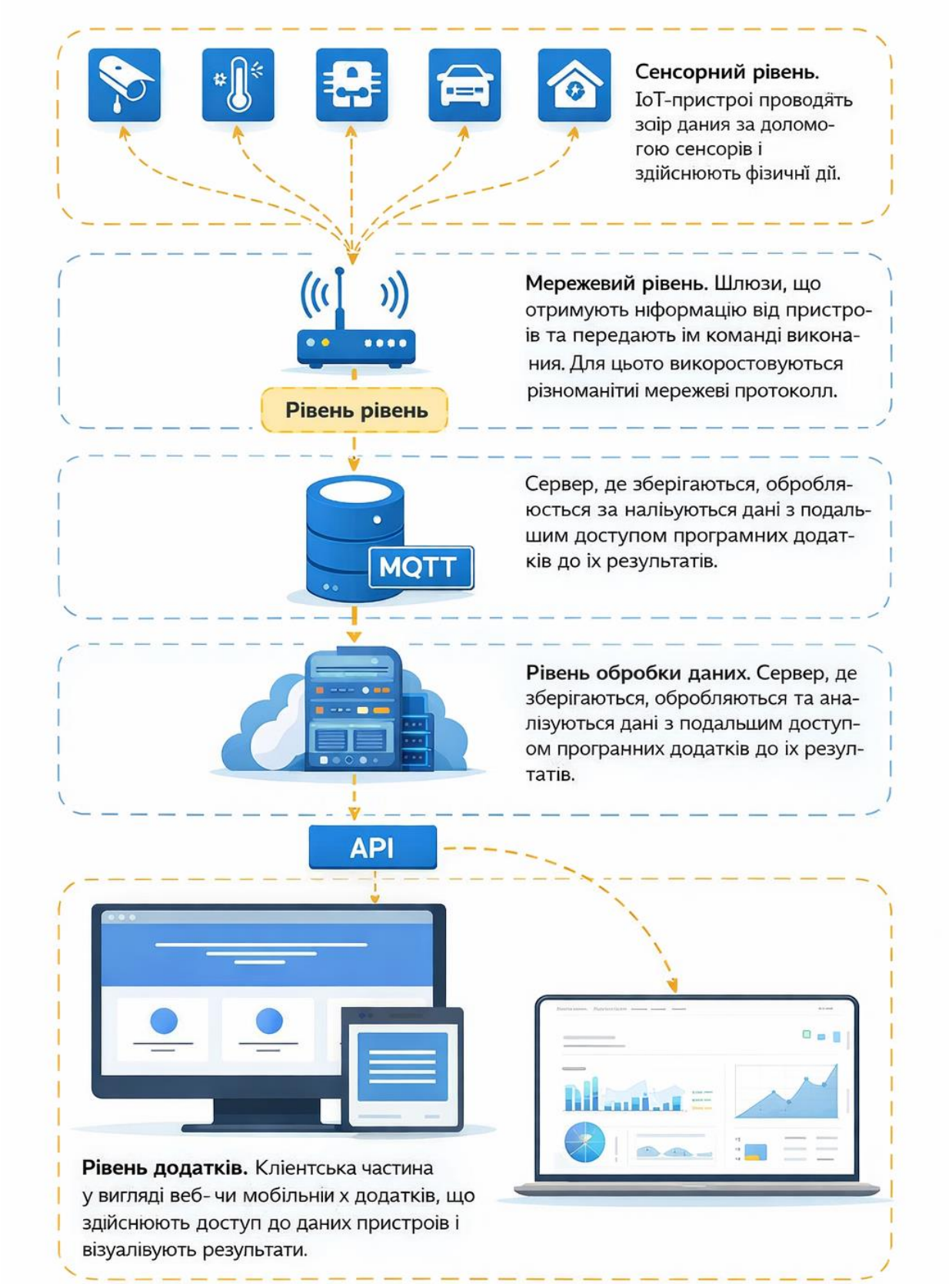


Рисунок 1.2 — Класична еталонна модель IoT

2 ОГЛЯД ОСНОВНИХ ЗАГРОЗ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ В МЕРЕЖАХ

2.1 Огляд загроз інформаційної безпеки Інтернету речей

Елементи мереж Інтернету речей здатні здійснювати обмін даними в автоматичному режимі, без прямої участі людини. Перетворення таких пристроїв на автономні мережеві вузли суттєво ускладнило забезпечення їхньої безпеки. Усі «розумні» пристрої підключені до мережі та передають дані відповідно до свого функціонального призначення, що робить цю інформацію привабливою ціллю для кіберзловмисників.

Поняття безпеки Інтернету речей охоплює сукупність підходів і механізмів, спрямованих на захист мережевих та інтернет-підключених пристроїв. Концепція IoT є надзвичайно широкою і продовжує розширюватися разом із розвитком технологій. Сьогодні практично будь-який сучасний технічний пристрій — від носимих гаджетів і побутових термостатів до ігрових консолей — може взаємодіяти з Інтернетом або іншими пристроями в мережі.

Безпека IoT являє собою комплекс методів, стратегій та програмно-апаратних засобів, призначених для запобігання компрометації таких пристроїв. Водночас саме здатність до постійного мережевого підключення, яка є ключовою перевагою Інтернету речей, значною мірою підвищує рівень уразливості IoT-систем до кібератак.

Зі збільшенням кількості способів взаємодії між пристроями зростає й кількість потенційних каналів атак. Протоколи та інтерфейси, зокрема HTTP і Application Programming Interface (API), широко використовуються в IoT-рішеннях, однак за наявності помилок у реалізації або налаштуванні можуть бути використані зловмисниками для перехоплення даних.

IoT-пристрої зазнають різноманітних загроз інформаційній безпеці, серед яких поширеними є уразливості механізмів керування сесіями, файлів cookie, а також недоліки в реалізації протоколів автентифікації, зокрема OAuth. Кількість атак, що експлуатують подібні вразливості, постійно зростає. У зв’язку з цим перспективним підходом є застосування механізмів автентифікації на основі JSON Web Token (JWT) у поєднанні з технологіями browser fingerprinting, що дозволяє підвищити рівень захисту облікових записів користувачів і зменшити ризик викрадення токенів автентифікації [1].

Однією з ключових причин компрометації пристроїв Інтернету речей є прагнення зловмисників до отримання фінансової вигоди. У контексті монетизації особливу зацікавленість для кіберзлочинців становлять IP-камери відеоспостереження, що пояснюється низкою чинників.

1) Постійний зв'язок. IP-камери передбачають постійне підключення до мережі Інтернет для забезпечення коректної роботи. Така доступність спрощує їх виявлення зловмисниками та створює умови для несанкціонованого використання після успішного злому пристрою.

2) Низькі витрати на зламування. Після виявлення вразливості в пристрої певної моделі аналогічні методи атаки можуть бути застосовані до інших пристроїв того ж типу, що значно знижує собівартість злому в розрахунку на один пристрій.

3) Відсутність нагляду. На відміну від персональних комп’ютерів, зазвичай експлуатуються без постійного контролю з боку користувачів і мають обмежені можливості керування безпекою. У більшості випадків на таких пристроях неможливо встановити додаткові засоби захисту, зокрема антивірусне програмне забезпечення.

4) Висока продуктивність. Обчислювальних ресурсів сучасних IP-камер часто достатньо для виконання шкідливих операцій, зокрема майнінгу криптовалюти, при цьому власники пристроїв можуть тривалий час не помічати сторонньої активності.

5) Висока пропускна здатність для виходу до Інтернету. Висока пропускна здатність каналів зв’язку, необхідна для передавання відеопотоку, робить IP-камери зручним інструментом для організації розподілених атак типу відмова в обслуговуванні (DDoS).

1) Дистанційний вплив. Окрім наведених аспектів, існує низка загальних проблем безпеки Інтернету речей, які продовжують становити загрозу фінансовим інтересам як окремих користувачів, так і організацій. Однією з таких проблем є можливість дистанційного впливу на IoT-пристрої. Через постійне підключення до мережі вони мають значну поверхню атаки, що дозволяє зловмисникам здійснювати віддалений доступ і маніпуляції. Тому системи безпеки IoT, подібно до хмарних середовищ, повинні враховувати наявність великої кількості потенційних точок входу та забезпечувати належний рівень захисту активів.

2) Відсутність галузевого передбачення. У процесі цифрової трансформації бізнесу аналогічні зміни відбуваються й у низці галузей та їхніх продуктів. Зокрема, такі сфери, як автомобілебудування та охорона здоров’я, останніми роками суттєво розширили використання IoT-пристроїв з метою

підвищення ефективності та зниження витрат. Водночас така цифровізація призвела до значного зростання технологічної залежності, що у разі інцидентів безпеки може посилювати негативні наслідки витоків даних. Особливу стурбованість викликає той факт, що зазначені галузі дедалі більше покладаються на IoT-пристрої, які за своєю природою є більш уразливими. Крім того, значна кількість компаній виявилася не готовою інвестувати достатні фінансові та організаційні ресурси в захист таких систем, що призводить до зростання рівня кіберзагроз для виробників і користувачів.

3) Ресурсні обмеження. Відсутність стратегічного підходу до безпеки не є єдиною проблемою, з якою стикаються сучасні IoT-системи. Важливим фактором ризику також є обмежені апаратні та програмні ресурси багатьох IoT-пристроїв. Значна частина з них не має достатньої обчислювальної потужності для впровадження повноцінних засобів захисту, таких як складні брандмауери або антивірусні рішення, а інколи обмежується лише базовими можливостями мережевого підключення.

Забезпечення безпеки IoT-пристроїв базується передусім на підтримці цілісності програмного коду, перевірці автентичності користувачів і пристроїв, коректному розмежуванні прав доступу, у тому числі до згенерованих даних, а також на можливості виявлення як віртуальних, так і фізичних атак.

Проблеми інформаційної безпеки Інтернету речей підтверджуються результатами незалежних досліджень. Зокрема, компанія Hewlett Packard Enterprise провела аналіз безпеки IoT-пристроїв у споживчому сегменті, який виявив значну кількість уразливостей — від використання стандартних паролів до експлуатації незахищених веб-інтерфейсів, що застосовуються більшістю пристроїв для взаємодії з елементами IoT-екосистеми [5].

Оскільки Інтернет речей охоплює різноманітні сфери застосування та технологічні підходи, це зумовлює широкий спектр загроз інформаційній безпеці. Найбільш критичні проблеми пов’язані безпосередньо з мережевими IoT-пристроями. Однією з ключових груп загроз є використання слабких, легко вгадуваних або жорстко закодованих облікових даних, що створює передумови для несанкціонованого доступу до розгорнутих систем.

Група 1. Слабкі паролі, паролі, які можна вгадувати або жорстко закодовані.

Використання загальнодоступних або незмінних облікових даних, які можна легко підбирати методом грубою сили, що надає несанкціонований доступ до розгорнутих систем. Розглянемо вразливості, що призводять до проблем безпеки.

1) Криптографічна стійкість характеризує здатність алгоритмів або механізмів автентифікації протидіяти спробам криптоаналізу. Надійним вважається такий механізм захисту, для компрометації якого зловмиснику необхідні надмірні обчислювальні ресурси, значні обсяги перехоплених даних або неприйнятно тривалий час, після завершення якого захищена інформація втрачає актуальність. У випадку використання простих або коротких паролів зловмисники можуть успішно застосовувати методи перебору, що дозволяє відносно швидко отримати доступ до пристрою або системи.

2) Поширеною проблемою безпеки є використання стандартних облікових даних, з якими IoT-пристрої постачаються виробником. Типовими прикладами таких паролів є комбінації на кшталт «admin:admin» або «admin:admin12345». Оскільки прошивки та базові налаштування зазвичай є однаковими для всіх пристроїв певної моделі, а користувачі часто не змінюють початкові облікові дані, ці паролі стають загальновідомими. У результаті зловмисники можуть використовувати словникові атаки для отримання доступу до великої кількості однотипних пристроїв.

3) Жорстко закодовані або вбудовані облікові дані являють собою паролі, які зберігаються у програмному коді або прошивці пристрою у відкритому вигляді. Такі паролі часто використовуються для спрощення масового розгортання та налаштування IoT-рішень, проте водночас створюють серйозну загрозу кібербезпеці. У багатьох системах передбачено стандартний обліковий запис адміністратора з фіксованим паролем, який є однаковим для всіх пристроїв певного типу та не змінюється кінцевими користувачами. У разі виявлення такого пристрою зловмиснику достатньо знайти відповідні облікові дані, що часто знаходяться у відкритому доступі, після чого він отримує повний контроль над системою.

Група 2. Небезпечні мережеві служби.

Суттєву загрозу інформаційній безпеці IoT-систем становлять зайві або неналежно захищені мережеві служби, що функціонують безпосередньо на пристроях, особливо ті, які мають прямий доступ з мережі Інтернет. Такі служби можуть порушувати конфіденційність, цілісність, автентичність або доступність інформації, а також створювати умови для несанкціонованого дистанційного керування пристроями. Мінімізація кількості непотрібних або небезпечних мережевих сервісів є одним із базових етапів забезпечення безпеки IoT-інфраструктури. Розглянемо основні вразливості, пов’язані з цією групою загроз.

1) Вразливі сервіси. Мережеві служби, що працюють на IoT-пристроях, часто використовують відкриті порти для обміну даними. Кожен такий порт і відповідний сервіс потенційно може містити вразливості, причинами яких є застарілі версії програмного забезпечення, помилки конфігурації або недостатня криптографічна стійкість механізмів автентифікації. Такі сервіси, як Telnet або Secure Shell (SSH), можуть бути корисними на етапах розробки та налагодження, проте в промисловій експлуатації зазвичай не є необхідними й повинні бути обмежені або вимкнені.

2) Атаки типу «відмова в обслуговуванні» є одним із найпоширеніших способів порушення працездатності мережевих сервісів. Існує багато методів реалізації таких атак, зокрема шляхом масового надсилання мережевих запитів, маніпуляції пакетами, експлуатації програмних або логічних уразливостей. У результаті сервіс може стати недоступним для легітимних користувачів через перевантаження, помилки виконання або виснаження ресурсів.

3) Використання служби Universal Plug and Play (UPnP). UPnP являє собою набір мережевих протоколів, призначених для автоматизації підключення пристроїв до мережі Інтернет. У разі активації цієї функції як на IoT-пристрої, так і на маршрутизаторі, переадресація необхідних портів відбувається автоматично без участі користувача. Небезпека такого підходу полягає в тому, що UPnP не передбачає використання шифрування, а передавання даних здійснюється у відкритому вигляді. Це створює умови для перехоплення інформації та дозволяє будь-якому пристрою автоматично отримати доступ до мережі. У результаті користувач часто не усвідомлює, які саме порти відкриті та доступні з Інтернету, що значно підвищує ризик компрометації системи.

4) Переповнення буфера. Переповнення буфера виникає у випадках, коли програма намагається записати в буфер обсяг даних, що перевищує виділений для нього розмір, або звертається до областей пам’яті за його межами. Буфер у такому разі являє собою послідовну ділянку пам’яті, призначену для зберігання різних типів даних — від текстових рядків до числових масивів. Запис поза межами виділеної пам’яті може призвести до пошкодження даних, збоїв у роботі системи, відмови в обслуговуванні або виконання шкідливого програмного коду.

Група 3. Небезпечні інтерфейси.

Небезпечні веб-інтерфейси, серверний API, хмарні або мобільні інтерфейси за межами пристрою, що дозволяє скомпрометувати пристрій або пов’язані з ним компоненти. Поширені проблеми включають відсутність автентифікації, відсутність або слабке шифрування, а також відсутність фільтрації введення та виведення. Розглянемо вразливості, що призводять до проблем безпеки.

1) Відсутність двохфакторної автентифікації. Двофакторна автентифікація є механізмом захисту, який передбачає використання двох незалежних факторів для підтвердження особи користувача. Першим фактором зазвичай виступає пароль, тоді як другим може бути одноразовий код, надісланий на мобільний пристрій, або біометричні дані. Відсутність такого механізму значно підвищує ризик несанкціонованого доступу у разі компрометації облікових даних..

2) Перерахування облікових записів. За наявності недоліків у реалізації механізмів автентифікації зловмисник може здійснювати анонімне перерахування імен користувачів або доступних ресурсів. Отриману інформацію надалі використовують для спроб підбору паролів. Наприклад, форма входу може повідомляти про помилку введення логіна, що дозволяє зловмиснику підтвердити існування конкретного облікового запису.

3) Незахищене відновлення пароля. Механізми відновлення доступу до облікового запису можуть бути скомпрометовані через використання методів підбору, експлуатацію вразливостей або застосування типових відповідей на секретні запитання. Надійна відповідь повинна бути відомою лише користувачеві, не публікуватися у відкритих джерелах та суттєво відрізнятися від поширених варіантів. Водночас слід враховувати можливість отримання такої інформації зловмисниками за допомогою соціальної інженерії, спуфінгу, фішингу або міжсайтового скриптингу.

4) Відсутність блокування облікового запису. Для запобігання багаторазовим спробам несанкціонованого входу система автентифікації повинна передбачати блокування облікового запису після досягнення визначеної кількості невдалих спроб. Водночас блокування може відбуватися і без злочинного наміру, наприклад у разі багаторазового введення неправильного пароля користувачем або використання застарілих облікових даних сервісами. Проте відсутність такого механізму значно спрощує реалізацію атак перебору паролів.

5) Перехоплення облікових даних в мережевому трафіку. У разі передавання даних між пристроєм і серверною частиною у відкритому вигляді вся інформація може бути перехоплена під час атаки типу «людина посередині». За таких умов зловмисник отримує доступ до облікових даних та іншої конфіденційної інформації, якою обмінюються клієнт і сервер. Поширеною проблемою є використання незахищених протоколів передавання даних, зокрема HTTP, замість їх зашифрованих аналогів, таких як HTTPS.

6) Управління сесією. Механізм сесій дозволяє зберігати стан автентифікації користувача до моменту завершення сеансу роботи. У разі викрадення ідентифікатора сесії та за відсутності додаткових перевірок, наприклад контролю

IP-адреси або обмеження кількості одночасних з'єднань, зловмисник може отримати повний доступ до системи з правами скомпрометованого облікового запису.

7) Наявність відомих уразливостей. Веб-інтерфейси IoT-систем можуть містити типові вразливості, зокрема міжсайтовий скриптинг, підробку міжсайтових запитів та SQL-ін'єкції. Експлуатація таких недоліків дозволяє зловмисникам порушувати роботу системи, отримувати несанкціонований доступ до даних або виконувати шкідливі дії від імені легітимних користувачів.

Група 4. Відсутність механізму безпечного оновлення.

Механізм безпечного оновлення передбачає гарантування цілісності та автентичності програмного забезпечення, що завантажується на пристрій, а також відсутність шкідливих наслідків під час перевірки або встановлення оновлень. За його відсутності IoT-пристрої стають особливо вразливими до атак. Розглянемо ключові проблеми, пов'язані з цією групою загроз.

1) Відсутність перевірки оновлення ПЗ перед завантаженням. За відсутності механізмів перевірки цифрових підписів і сертифікатів зловмисники можуть підмінити файли оновлень і розповсюджувати шкідливе програмне забезпечення під виглядом легітимних оновлень.

2) Відсутність шифрування ПЗ під час доставки. Незахищений канал зв'язку створює можливість перехоплення або модифікації файлів оновлень під час доставки. Тому передавання програмного забезпечення має здійснюватися з використанням захищених каналів зв'язку.

3) Відсутність механізмів захисту від повернення оновлень. Зловмисник може спробувати оновити пристрій старішою версією. Зловмисник може навмисно встановити застарілу версію програмного забезпечення, що містить відомі вразливості, або скинути налаштування пристрою до заводських. Це відкриває можливість повторної експлуатації раніше усунутих недоліків і отримання доступу до конфіденційної інформації.

4) ПЗ містить конфіденційну інформацію. У разі передавання оновлень, які містять закодовані облікові дані або іншу чутливу інформацію, зловмисник може перехопити ці дані та використати їх для компрометації системи.

5) Файл оновленого ПЗ не зашифровано. Нешифровані файли програмного забезпечення можуть бути змінені під час передавання або зберігання, що дозволяє зловмисникам порушити цілісність коду та інтегрувати в нього шкідливі компоненти.

Група 5. Використання небезпечних компонентів.

Значну загрозу інформаційній безпеці IoT-систем становить використання

небезпечних або застарілих програмних компонентів і бібліотек, експлуатація яких може призвести до компрометації пристрою. Подібні вразливості часто виникають через відсутність належного контролю за виконуваним програмним забезпеченням та механізмами його ізоляції. Розглянемо ключову вразливість, характерну для цієї групи загроз.

1) Відсутність довіреного середовища виконання. Більшість IoT-пристроїв за своєю архітектурою фактично є комп'ютерами загального призначення, що дозволяє запускати на них різноманітне програмне забезпечення. За відсутності довіреного середовища виконання зловмисники можуть встановлювати сторонні програми, які маскуються під легітимні компоненти системи та виконують шкідливі функції. Наприклад, на пристрій може бути інстальоване програмне забезпечення, призначене для участі в атаках типу відмова в обслуговуванні. Обмеження набору дозволених програм і функціональних можливостей пристрою, а також контроль за виконуваним кодом суттєво знижують ризик несанкціонованого використання IoT-пристроїв у зловмисних цілях.

Група 6. Недостатній захист конфіденційності.

Серйозною проблемою безпеки IoT-систем є неналежне поводження з персональними даними користувачів, які зберігаються безпосередньо на пристроях або в межах відповідної екосистеми. Такі дані можуть використовуватися небезпечно, без дотримання вимог захисту або без явної згоди власника інформації. Розглянемо ключову вразливість, що призводить до порушень конфіденційності.

1) Відсутність захисту персональних даних. ористувачі IoT-пристроїв часто зберігають на них конфіденційну інформацію. Зокрема, пристрої, підключені до бездротових мереж, можуть містити паролі доступу до мережі або облікові дані сервісів, з якими вони взаємодіють. Крім того, такі пристрої, як IP-камери, здатні здійснювати відео- та аудіозапис приміщень, у яких вони встановлені. Водночас у багатьох випадках ці дані не захищені шляхом шифрування або інших механізмів безпеки. У разі отримання доступу до такої інформації зловмисниками це призводить до серйозного порушення конфіденційності користувачів. Тому IoT-пристрої та пов'язані з ними сервіси повинні забезпечувати коректну та безпечну обробку персональних даних, а також їх зберігання й передавання виключно за згодою кінцевого користувача.

Група 7. Небезпечна передача та зберігання даних.

Однією з критичних проблем інформаційної безпеки IoT-систем є відсутність належного шифрування та ефективного контролю доступу до конфіденційних даних на будь-якому етапі їх життєвого циклу — під час зберігання, передавання

або оброблення. Такі недоліки створюють сприятливі умови для витоку інформації та її несанкціонованого використання. Розглянемо основні вразливості, що призводять до порушень безпеки.

1) Відсутність контролю доступу з урахуванням ролей. Контроль доступу з урахуванням ролей є розвитком вибіркової політики доступу, за якої повноваження користувачів групуються відповідно до виконуваних функцій. Кожному користувачеві може бути призначено одну або декілька ролей, а кожна роль визначає перелік допустимих привілеїв. Ієрархія ролей і механізми взаємного виключення керуються програмними засобами, що зменшує вплив людського фактора, спрощує адміністрування та підвищує загальний рівень інформаційної безпеки. За відсутності такого підходу ризик несанкціонованого доступу значно зростає.

2) Розширені привілеї. Принцип мінімальних привілеїв передбачає надання користувачам лише тих прав доступу, які є необхідними для виконання їхніх завдань. Проте в багатьох IoT-пристроях використовується єдиний обліковий запис або однаковий рівень привілеїв як для користувачів, так і для внутрішніх системних процесів. У разі компрометації такого облікового запису подальше обмеження доступу стає неможливим, а шкідливі дії привілейованих користувачів можуть залишатися непомітними.

3) Відсутність сегментування локальної мережі. Проникнення зловмисника до мережі через один уразливий IoT-пристрій може призвести до доступу до інших компонентів системи та конфіденційних даних. Одним із найефективніших методів зниження такого ризику є поділ корпоративної мережі на декілька ізольованих підмереж. Сегментація дозволяє обмежити поширення атак і ізолювати критично важливі ресурси від менш захищених пристроїв.

4) Передавання даних локальними мережами або через Інтернет без використання транспортного шифрування створює умови для перехоплення трафіку у відкритому вигляді. Типовим прикладом є застосування протоколу File Transfer Protocol (FTP) без підтримки механізмів захисту, таких як Secure Sockets Layer (SSL) або Transport Layer Security (TLS), що значно підвищує ризик компрометації інформації.

5) Погано впроваджені SSL та TLS. Застосування застарілих версій криптографічних протоколів, випущених раніше за TLS 1.1, не забезпечує належного рівня захисту даних. У протоколах SSL версій 2.0 і 3.0, а також TLS 1.0, наявні критичні вразливості, які можуть бути використані для перехоплення інформації під час атаки.

6) Некоректно налаштовані протоколи шифрування TLS та SSL. Для забезпечення повної безпеки зашифрованого з'єднання клієнтське програмне забезпечення повинно перевіряти коректність сертифіката, зокрема його чинність, термін дії та відповідність доменного імені. У разі недотримання цих вимог зловмисник може підробити сертифікат і непомітно отримати доступ до передаваних даних.

Група 8. Відсутність керування пристроями.

Належне керування IoT-пристроями є необхідною умовою забезпечення їх стабільної та безпечної роботи після впровадження в експлуатацію. Окрім цього, важливо організувати захищений доступ до пристроїв, здійснювати постійний контроль їхнього стану, своєчасно виявляти та усувати проблеми, а також централізовано керувати оновленнями програмного забезпечення. За відсутності таких механізмів значно зростає ризик виникнення інцидентів інформаційної безпеки. Розглянемо основні вразливості, пов'язані з недостатнім керуванням IoT-пристроями.

1) У процесі експлуатації програмного забезпечення регулярно виявляються нові вразливості, усунення яких потребує оперативного розповсюдження оновлень. Якщо пристрій не підтримує механізми оновлення або оновлення не застосовуються, він залишається вразливим до відомих загроз протягом тривалого часу, що створює сприятливі умови для атак.

2) Моніторинг безпеки передбачає безперервний збір і аналіз інформації про стан системи з метою виявлення підозрілої активності або несанкціонованих змін у мережі. За відсутності таких механізмів атаки можуть залишатися непоміченими, що унеможливлює своєчасне реагування та мінімізацію наслідків.

3) Журнали подій є важливим джерелом інформації про дії користувачів і системні процеси, зокрема входи та виходи з облікових записів, доступ до ресурсів і зміни конфігурацій. Наявність міток часу дозволяє проводити аналіз подій і виявляти неправомірні дії, наприклад спроби підбору паролів. Відсутність журналювання суттєво ускладнює розслідування інцидентів безпеки.

4) IoT-пристрої часто зберігають конфіденційну інформацію, тому неправильне або неконтрольоване виведення їх з експлуатації може призвести до витоку даних. Зловмисники можуть отримати доступ до накопичувачів, що містять облікові дані або персональну інформацію користувачів.

Для підвищення рівня захисту IoT-пристроїв необхідно впроваджувати сучасні механізми безпеки, зокрема шифрування даних та контроль цілісності програмного забезпечення. Виробники можуть сприяти безпечному використанню своїх рішень, надаючи детальну документацію та рекомендації для користувачів і

фахівців з інформаційної безпеки. Додатково пристрої мають бути захищені фізично, а у випадку компрометації — здатні блокувати виконання шкідливого програмного забезпечення та повідомляти користувача про інцидент. Зосередження уваги на зазначених аспектах дозволяє суттєво підвищити загальний рівень безпеки IoT-систем.

Інтернет речей характеризується наявністю значної кількості загроз, здатних негативно впливати на рівень інформаційної безпеки та конфіденційність як окремих користувачів, так і організацій. Серед усього різноманіття ризиків виокремлюють сім загроз, які на сьогодні є найбільш актуальними. Зі збільшенням кількості підключених до мережі IoT-пристроїв масштаб і складність потенційних атак зростатимуть, а наслідки неналежно захищених IoT-систем можуть мати серйозні негативні наслідки для бізнесу, користувачів і суспільства загалом. У зв'язку з цим виникає необхідність у постійних заходах, спрямованих на виявлення, усунення та запобігання вразливостям як апаратних компонентів, так і програмного забезпечення Інтернету речей.

Розглянемо найбільш поширені та небезпечні загрози, що виникають унаслідок проблем інформаційної безпеки IoT-систем.

1) Ботнети. Кіберзлочинці можуть інфікувати IoT-пристрої шкідливим програмним забезпеченням, яке надає можливість дистанційно керувати об'єднаними в бот-мережу пристроями через сервери управління та контролю. Такі ботнети використовуються для викрадення конфіденційної інформації, отримання доступу до онлайн-банкінгу, а також для здійснення кібератак, зокрема DDoS-атак і фішингових кампаній. Сукупна обчислювальна потужність сотень тисяч або навіть мільйонів заражених IoT-пристроїв дозволяє реалізовувати масштабні атаки з серйозними наслідками.

2) DDoS-атака. Дослідження демонструють сценарії, за яких трафік, згенерований IP-камерами спостереження, може бути використаний для організації DDoS-атак з метою уповільнення або повного виведення з ладу сервісів. Такі атаки можуть слугувати підготовчим етапом до подальших злочинів, зокрема крадіжок зі зломом. Використовуючи доступ до IP-камери, зловмисники отримують інформацію про планування приміщення, наявні цінності та інші пристрої в мережі, після чого поширюють атаку шляхом підбору паролів і аналізу відкритого мережевого трафіку. Подібні інциденти демонструють, як кіберзагрози можуть призводити до реальних подій із суспільно небезпечними наслідками.

3) Атаки «людина посередині». Атаки цього типу становлять суттєву загрозу конфіденційності та цілісності даних. Вони відносно прості в реалізації та водночас достатньо ефективні, що робить їх привабливими для зловмисників.

Атаки «людина посередині» можуть застосовуватися для компрометації IoT-пристроїв, зокрема розумних побутових приладів або автономних транспортних засобів. Оскільки IoT-пристрої часто обмінюються даними в режимі реального часу, зловмисник може перехоплювати або змінювати інформацію між кількома пристроями одночасно, що призводить до серйозних збоїв у роботі систем.

4) Крадіжка даних. Унаслідок порушень безпеки з IoT-систем можуть викрадатися персональні дані користувачів, облікові дані, платіжна інформація та адреси електронної пошти. Отримавши такі відомості, зловмисники здатні здійснювати більш складні та цілеспрямовані атаки, включаючи крадіжку особистих даних. Крім того, уразливості IoT-пристроїв, інтегрованих у корпоративні мережі, можуть використовуватися як точка входу для проникнення до внутрішніх бізнес-систем організацій, наприклад через компрометацію окремого датчика або контролера.

5) Соціальна інженерія. Соціальна інженерія є одним із поширених методів атак, за якого зловмисники маніпулюють користувачами з метою отримання конфіденційної інформації, зокрема паролів або облікових даних. Найчастіше такі атаки реалізуються через фішингові електронні повідомлення, зміст яких спеціально сформований для введення жертви в оману. У випадку IoT-систем подібні атаки можуть бути ще ефективнішими, оскільки IoT-пристрої часто зберігають значні обсяги персональних даних користувачів, наприклад відеозаписи з IP-камер спостереження. Використання такої інформації дозволяє зловмисникам здійснювати складні, цілеспрямовані атаки соціальної інженерії, орієнтовані не лише на конкретного користувача, а й на членів його родини чи інших осіб, які взаємодіють із уразливими IoT-мережами. У результаті соціальна інженерія стає ефективним інструментом несанкціонованого доступу до даних користувачів.

6) Розширені постійні загрози. Розширені постійні загрози є серйозною проблемою інформаційної безпеки для сучасних організацій. Вони являють собою цілеспрямовані кібератаки, у межах яких зловмисник отримує несанкціонований доступ до мережі та залишається непоміченим протягом тривалого періоду часу. Метою таких атак є постійне спостереження за мережевою активністю та викрадення критично важливих даних. Запобігання, виявлення та нейтралізація розширених постійних загроз є складним завданням через їхню багаторівневу та приховану природу. З поширенням Інтернету речей значні обсяги інформації передаються між великою кількістю пристроїв, що створює додаткові точки входу для зловмисників. Компрометація IoT-пристроїв може використовуватися для проникнення як у персональні, так і в корпоративні мережі з подальшим

викраденням конфіденційних даних.

7) Програми-вимагачі. Програми-вимагачі належать до категорії шкідливого програмного забезпечення, призначеного для блокування доступу до файлів або пристроїв із подальшою вимогою викупу. Таке ПЗ застосовує потужні алгоритми шифрування, що унеможливлює доступ до комп'ютерів, даних і ресурсів мережі без спеціального ключа. Сучасні програми-вимагачі відзначаються високим рівнем складності та здатністю знаходити й знищувати резервні копії, що значно ускладнює процес відновлення інформації. Наявність IoT-пристроїв у поєднанні з відсутністю належних механізмів безпеки створює зручні умови для проникнення зловмисників у мережі та реалізації атак із використанням програм-вимагачів.

2.2 Огляд основних вимог щодо безпеки мережі Інтернету речей

На основі проаналізованих загроз та проблем інформаційної безпеки IoT-систем доцільно сформулювати низку рекомендацій, спрямованих на зниження ризиків реалізації потенційних атак. Запропоновані заходи дозволяють підвищити рівень захищеності мережі Інтернету речей та мінімізувати можливі наслідки порушення безпеки.

Група 1. Для зменшення ризиків, пов'язаних із використанням ненадійних облікових даних, рекомендується впровадження таких заходів безпеки:

1) Визначити вимоги до мінімальної довжини, складності та періодичності зміни паролів відповідно до галузевих рекомендацій стандарту NIST SP 800-63B.

2) Забезпечити унікальність паролів для кожного окремого IoT-пристрою з метою унеможливлення масової компрометації системи.

3) Повністю виключити використання жорстко закодованих паролів у програмному забезпеченні та конфігураціях пристроїв.

Група 2. Небезпечні мережеві служби. Розглянемо рекомендовані методи безпеки.

1) Надати доступ лише до необхідних мережевих портів із використанням механізмів фільтрації портів відповідно до штатного режиму роботи пристрою.

2) Змінити стандартні номери портів на нестандартні, обравши значення з діапазону 1025–65535, що ускладнює автоматизоване сканування.

3) Використовувати сервіси, стійкі до атак, пов'язаних із переповненням буфера.

4) Забезпечити захист мережевих служб від атак типу відмова в обслуговуванні шляхом застосування відповідних механізмів обмеження та контролю трафіку.

5) Виконувати налаштування переадресації портів вручну та повністю вимкнути підтримку протоколу UPnP, що зменшує ризик несанкціонованого доступу.

Група 3. Небезпечні інтерфейси. Для підвищення рівня захисту користувацьких, серверних та хмарних інтерфейсів рекомендується впровадити такі заходи:

1) За можливості використовувати механізми двофакторної автентифікації для підвищення рівня захисту облікових записів.

2) Обов’язково змінювати стандартні логіни та паролі, встановлені за замовчуванням.

3) Забезпечити надійність процедур відновлення пароля та не допускати розкриття інформації, яка може вказувати на існування чинного облікового запису.

4) Налаштувати порогові значення для блокування облікових записів у разі багаторазових невдалих спроб входу.

5) Захистити облікові дані від перехоплення як у внутрішньому, так і в зовнішньому мережевому трафіку шляхом використання захищених протоколів.

6) Провести тестування інтерфейсів за допомогою автоматизованих інструментів з метою виявлення вразливостей типу міжсайтового скриптингу, підробки міжсайтових запитів та SQL-ін’єкцій, а також реалізувати захисні механізми проти зазначених загроз.

Група 4. Для зменшення ризиків, пов’язаних із компрометацією процесу оновлення ПЗ IoT-пристроїв, доцільно впровадити такі заходи безпеки:

1) Застосовувати загальноприйняті криптографічні алгоритми для шифрування файлів оновлення програмного забезпечення.

2) Використовувати захищене з’єднання під час передавання файлів оновлення з метою запобігання їх перехопленню або підміні.

3) Забезпечити перевірку цифрового підпису оновлення перед його завантаженням і встановленням для підтвердження цілісності та автентичності.

4) Проводити перевірку сервера оновлень з метою впевненості у коректному налаштуванні механізмів транспортного шифрування та відсутності відомих вразливостей.

5) Регулярно створювати резервні копії системи для можливості відновлення працездатності у разі некоректного або скомпрометованого оновлення.

Група 5. З метою зменшення ризиків, пов’язаних із використанням уразливих бібліотек або програмних модулів, рекомендується реалізувати такі заходи:

1) Перевіряти наявність та коректність цифрових підписів постачальника для програмних компонентів і бібліотек, що використовуються в IoT-пристроях.

2) За можливості впроваджувати системи запобігання вторгненням для виявлення та блокування підозрілої активності на рівні пристрою або мережі.

Група 6. Для забезпечення належного захисту персональних та чутливих даних рекомендується дотримуватися таких принципів:

1) Обмежувати обсяг зібраної інформації, надаючи перевагу збору лише тих даних, які є необхідними для функціонування IoT-системи.

2) Застосовувати криптографічні методи для захисту зібраних даних як під час зберігання, так і під час передавання.

3) Надати доступ до конфіденційної інформації виключно уповноваженим користувачам або службам із відповідними правами доступу.

Група 7. Для підвищення рівня захисту даних у процесі зберігання та передавання в IoT-мережах доцільно застосувати такі рекомендації:

1) Вимикати обліковий запис адміністратора у випадках, коли його використання не є необхідним для роботи системи.

2) За можливості впроваджувати механізми контролю доступу з урахуванням ролей користувачів.

3) Забезпечити сегментацію мережі з ізоляцією критично важливої інформації шляхом використання технології Virtual Local Area Network (VLAN).

4) Налаштовувати списки контролю доступу на мережевих інтерфейсах для фільтрації трафіку за IP-адресами, MAC-адресами та портами.

5) Забезпечити шифрування даних із використанням протоколів SSL та TLS;

6) У разі неможливості використання SSL або TLS застосовувати інші стандартизовані галузеві методи шифрування для захисту даних під час передавання.

7) Уникати використання власних або нестандартних криптографічних протоколів через ризик наявності прихованих вразливостей.

Група 8. Для забезпечення стабільної та безпечної експлуатації IoT-пристроїв необхідно впроваджувати комплексні механізми керування протягом усього життєвого циклу пристрою. До рекомендованих заходів безпеки належать такі:

1) Забезпечити регулярне оновлення програмного забезпечення шляхом увімкнення функції автоматичного оновлення або підписки на офіційні повідомлення виробника щодо виходу нових версій ПЗ.

2) Не вимикати системні журнали подій та здійснювати їх періодичний аналіз з метою виявлення підозрілої активності або ознак компрометації.

3) За можливості впровадити систему виявлення вторгнень для своєчасного реагування на несанкціоновані дії в мережі або на пристрої.

4) Перед виведенням пристрою з експлуатації необхідно переконатися у відсутності на ньому конфіденційної або персональної інформації.

5) У разі списання пристрою виконати повне очищення пам’яті або здійснити фізичне знищення носіїв даних для унеможливлення відновлення інформації.

Атаки на IoT-пристрої в більшості випадків не потребують складних технічних засобів. Часто зловмиснику достатньо скористатися обліковими даними, встановленими за замовчуванням, або отримати доступ до відкритого мережевого порту для повного захоплення пристрою. Значна кількість IoT-рішень не має навіть базових механізмів захисту, що суттєво спрощує їх компрометацію. У зв’язку з цим навіть відносно невеликий перелік базових вимог безпеки здатен істотно підвищити загальний рівень захищеності IoT-систем. Запропоновані вимоги можуть розглядатися як реалістичний початковий етап на шляху до значного підвищення рівня безпеки споживчих IoT-пристроїв.

3 ДОСЛІДЖЕННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА НАЯВНІСТЬ ВІДОМИХ ВРАЗЛИВОСТЕЙ

3.1 Загальні положення

Захист інформації являє собою комплексну діяльність, спрямовану на запобігання витоку інформації через різноманітні канали мережевої взаємодії, а також на виявлення та блокування таких каналів. Процес захисту включає ідентифікацію потенційних шляхів витоку інформації, оцінку її значущості та розроблення ефективних заходів, спрямованих на недопущення несанкціонованого доступу, витоку або розкрадання даних.

Визначення цінності інформаційних ресурсів дозволяє зосередити зусилля насамперед на захисті найбільш критично важливих відомостей, компрометація яких може призвести до суттєвих негативних наслідків. Об’єктом технічного захисту в такому випадку є інформація, що підпадає під дію Закону України «Про інформацію», а також конфіденційні відомості, передані державі у користування або володіння. Виходячи з цього, основною метою захисту інформації є недопущення її витоку, спотворення або порушення цілісності. Досягнення зазначеної мети забезпечується шляхом застосування методів тестування та моніторингу, які становлять організовану сукупність технічних і програмних засобів, спрямованих на ефективне забезпечення інформаційної безпеки [6].

Інформаційна безпека реалізується завдяки використанню захищених програмних і апаратних засобів інформаційної діяльності, спеціалізованих засобів захисту та контролю, які мають сертифікати відповідності вимогам нормативних документів у сфері технічного захисту інформації. Крім того, можуть застосовуватися спеціальні інженерні споруди, системи та засоби, що забезпечують додатковий рівень захисту.

У даній кваліфікаційній роботі основна увага зосереджена на дослідженні методів забезпечення інформаційної безпеки в IoT-мережах.. Підрозділ розпочинається з аналізу загальновідомих уразливостей інформаційної безпеки, описаних у базі Common Vulnerabilities and Exposures (CVE), характерних для IP-камер, виготовлених компаніями Hikvision та Dahua.

Підключення IP-камер до мережі Інтернет є стійкою та загальноприйнятою тенденцією розвитку сучасних систем відеоспостереження. З огляду на значну кількість таких пристроїв, розгорнутих у різних країнах світу, навіть відносно

невелика частка IP-камер, доступних з мережі Інтернет, становить привабливу ціль для зловмисників. Компрометація подібних пристроїв може використовуватися як для збору конфіденційної інформації, так і для реалізації подальших кібератак.

З метою підвищення рівня інформаційної безпеки IoT-мереж та протидії можливим атакам у роботі пропонуються методи дослідження IoT-пристроїв у мережі з використанням відомих уразливостей інформаційної безпеки. Застосування таких методів дозволяє своєчасно виявляти слабкі місця в системах та розробляти ефективні заходи щодо їх усунення.

3.2 Опис методів сканування елементів мережі

Для дослідження мережевих елементів та оцінювання рівня їх захищеності за сценарієм збору інформації застосовується сканер Nmap. Nmap є безкоштовним програмним засобом з відкритим вихідним кодом, призначеним для виявлення хостів у мережі та ідентифікації сервісів, що функціонують на цих хостах. Інструмент широко використовується для аналізу безпеки та проведення мережевого аудиту, оскільки дозволяє отримати детальне уявлення про реальні служби та протоколи.

Більшість IoT-пристроїв не оснащені повноцінними вбудованими механізмами захисту, а в окремих випадках не підтримують регулярні оновлення програмного забезпечення або виправлення безпеки. Така ситуація створює сприятливі умови для кіберзлочинців, які можуть використовувати вразливості мережевих сервісів для несанкціонованого доступу. Водночас можливості Nmap щодо виявлення та аудиту дозволяють оперативно знаходити активні хости в мережі, визначати запущене на них програмне забезпечення. На рис. 3.1 наведено головне меню сканеру Zenmap.

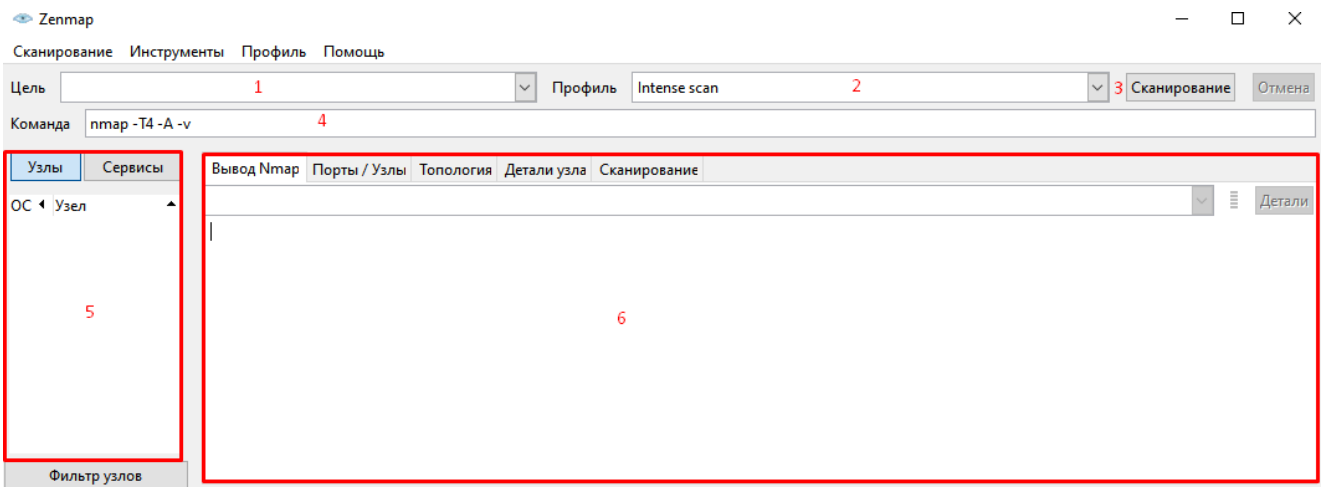


Рисунок 3.1 – Огляд головного меню програми Zenmap

З рис. 3.1 видно інтерфейс головного вікна програми Zenmap та її основні функціональні елементи. Нижче наведено опис ключових компонентів програми, позначених на рисунку відповідними цифрами.

1) Ціль: поле для задання IP-адреси або діапазону IP-адрес, які підлягають скануванню. Наприклад, може бути вказано одну адресу типу 192.168.130.129 або діапазон адрес, наприклад 192.168.130.120–192.168.130.140.

2) Профіль: випадаючий список із заздалегідь налаштованими режимами сканування Nmap. Користувач може обрати відповідний тип перевірки, зокрема швидке, стандартне або інтенсивне сканування, залежно від поставлених задач.

3) Сканування: кнопка запуску процесу аналізу мережі. Тривалість сканування залежить від кількості заданих цілей та обраного профілю, проте у більшості випадків процедура виконується достатньо швидко.

4) Команда: поле, в якому відображається сформована команда Nmap відповідно до вибраних параметрів. За необхідності користувач може вручну доповнити команду додатковими ключами або опціями для отримання розширеної інформації про досліджуваний вузол.

5) Хости/сервіси: панель, у якій відображається перелік виявлених хостів і мережевих сервісів, отриманих у результаті виконання сканування.

6) Основна інформаційна частина інтерфейсу, що містить п’ять вкладок: «Вивід Nmap», «Порти/Хости», «Топологія», «Деталі хоста», «Сканування». Вкладка «Вивід Nmap» відображає повний текстовий результат виконаних операцій сканування та містить узагальнену інформацію про виявлені вузли. У вкладці «Порти/Хости» подається структурований перелік відкритих портів і відповідних мережевих сервісів, визначених під час аналізу. Вкладка «Топологія» забезпечує графічне представлення мережі, демонструючи взаємозв’язки між виявленими вузлами та їхнє розташування відносно один одного. Вкладка «Деталі хоста» надає детальні відомості про окремий вузол у зручному для аналізу візуальному форматі, що спрощує інтерпретацію результатів сканування.

У вкладці «Сканування» зберігається журнал усіх виконаних сканувань разом із використаними командами Nmap протягом поточної сесії роботи з програмою Zenmap..

Як зазначалося раніше, програма Zenmap надає можливість використання заздалегідь налаштованих профілів сканування, які охоплюють десять основних типів перевірок мережі. Такі профілі значно спрощують процес аналізу та дозволяють швидко обрати оптимальний режим сканування залежно від

поставлених завдань. Розглянемо їхні основні характеристики.

1) Інтенсивне сканування – забезпечує оперативну перевірку найбільш уживаних TCP-портів, а також виконує ідентифікацію операційної системи, активних сервісів і їх версій.

2) Інтенсивне сканування плюс User Datagram Protocol (UDP) – розширений варіант інтенсивного сканування, який, окрім TCP-портів, додатково аналізує UDP-порти

3) Інтенсивне сканування, всі порти TCP. На відміну від стандартного режиму, у якому перевіряється лише обмежена кількість найпопулярніших портів, цей профіль здійснює повне сканування всього діапазону TCP-портів, що потребує значно більше часу.

4) Інтенсивне сканування, без пінгу. Працює аналогічно іншим інтенсивним режимам, проте не виконує попередню перевірку доступності вузла. Такий підхід є доцільним у випадках, коли ICMP-запити блокуються, але відомо, що хост активний.

5) Пінг-сканування. Призначене виключно для перевірки доступності хостів у мережі без аналізу портів і сервісів.

6) Швидке сканування. Оптимізований режим, що зменшує час перевірки шляхом обмеження кількості аналізованих TCP-портів до ста найбільш поширених.

7) Швидке сканування плюс. Аналог швидкого сканування, який додатково визначає тип операційної системи та її версію.

8) Швидке трасування. Дозволяє виконати трасування маршрутів і ping-перевірку всіх вузлів, заданих у параметрах цілі.

9) Звичайне сканування – передбачає використання TCP SYN-сканування для тисячі найпоширеніших TCP-портів із попереднім виявленням хоста за допомогою ICMP-exo-запитів.

10) Найбільш детальний режим аналізу, орієнтований на максимальне виявлення інформації про вузол. Навіть у разі відсутності відповіді на початкові ping-запити сканування продовжується з використанням кількох протоколів для визначення доступності хоста. Після його виявлення здійснюється глибокий аналіз операційної системи, активних сервісів і їх версій на основі TCP та UDP. Додатково використовується маскування вихідного порту під стандартний порт DNS (53), що дозволяє обійти окремі обмеження фільтрації трафіку.

Альтернативним інструментом скануванням елементів мереж є Router Scan. Router Scan – це програма для виконання аудиту безпеки, вона сканує мережі, знаходить різні пристрої. Для виявлених об’єктів програма здійснює спроби

підбору облікових даних, а також перевіряє наявність відомих уразливостей, характерних для мережевого обладнання. У разі успішної експлуатації вразливостей або коректного підбору логінів і паролів можливе отримання конфіденційної інформації з пристрою, наприклад параметрів доступу до бездротової мережі Wi-F. На рис. 3.2 зображено огляд головного меню програми Router Scan.

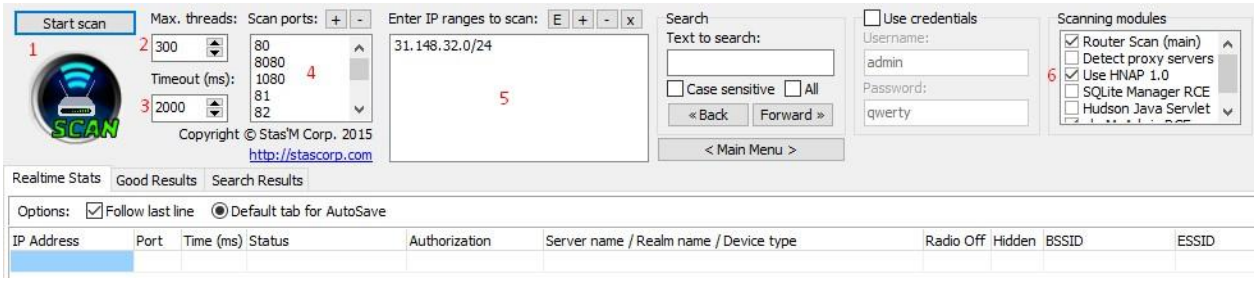


Рисунок 3.2 – Огляд головного меню програми Router Scan

З рисунка 3.2 можна побачити головне вікно програми Router Scan, у якому зосереджені основні елементи керування та налаштування процесу сканування. Розглянемо ключові функціональні компоненти інтерфейсу, позначені на рисунку.

1) Головна кнопка. Призначена для запуску процедури аналізу мережі. Після початку роботи трансформується у дві окремі кнопки, що дозволяють тимчасово призупинити або повністю зупинити процес сканування.

2) Максимальна кількість потоків. Визначає число пристроїв, які можуть оброблятися паралельно в межах одного сеансу сканування. Значення цього параметра безпосередньо залежить від обчислювальних ресурсів робочої або віртуальної машини: чим вища продуктивність системи, тим більшу кількість потоків можна задіяти без втрати стабільності.

3) Тайм-аут з’єднання. Задає граничний час очікування відповіді від пристрою у мілісекундах. Значення цього параметра потребує індивідуального підбору залежно від характеристик мережі, зокрема швидкості з’єднання, якості каналу та особливостей провайдера, з метою уникнення помилкових втрат зв’язку.

4) Список портів для сканування. Містить список TCP-портів, які підлягають перевірці під час аналізу заданих IP-діапазонів. За замовчуванням більшість портів опитуються з використанням протоколу HTTP/1.0, тоді як порти 443, 4343 та 8443 перевіряються через HTTPS із застосуванням бібліотеки OpenSSL. Для розширення області виявлення мережевих сервісів доцільно додатково включати альтернативні порти, зокрема 81, 88, 8000, 8081, 8082, 8088, 8888 тощо. Зміна переліку портів можлива також шляхом редагування

конфігураційного файлу *ports.txt*.

5) Список IP діапазонів для сканування. Визначає адресні діапазони, у межах яких здійснюється сканування мережі. Налаштування цих параметрів може бути змінене вручну через файл *ranges.txt*, що дозволяє гнучко адаптувати процес дослідження до конкретної мережевої інфраструктури.

6) Модулі сканування. Router Scan підтримує кілька спеціалізованих модулів аналізу, серед яких основний модуль реалізує два базові методи перевірки доступності та безпеки пристроїв, а додаткові модулі розширюють функціональні можливості програми. Основний модуль забезпечує швидке виявлення цільових пристроїв, виконуючи автоматизований перебір облікових даних та застосування відомих уразливостей, характерних для відповідних моделей обладнання. Усі результати сканування зберігаються для подальшого аналізу. Усі отримані під час сканування результати відображаються у зрозумілому та зручному для користувача графічному інтерфейсі з можливістю гнучкого налаштування параметрів відображення. Крім того, результати роботи програми можуть бути експортовані та збережені у файли різних форматів для подальшого аналізу або документування.

Для пошуку цілей (діапазонів IP-адрес в конкретному місті) можливо використати сервіс «4it.me» або інший, який видає IP діапазони міста. На рис. 3.3 зображено використання сервісу «4it.me» для міста Кельн.

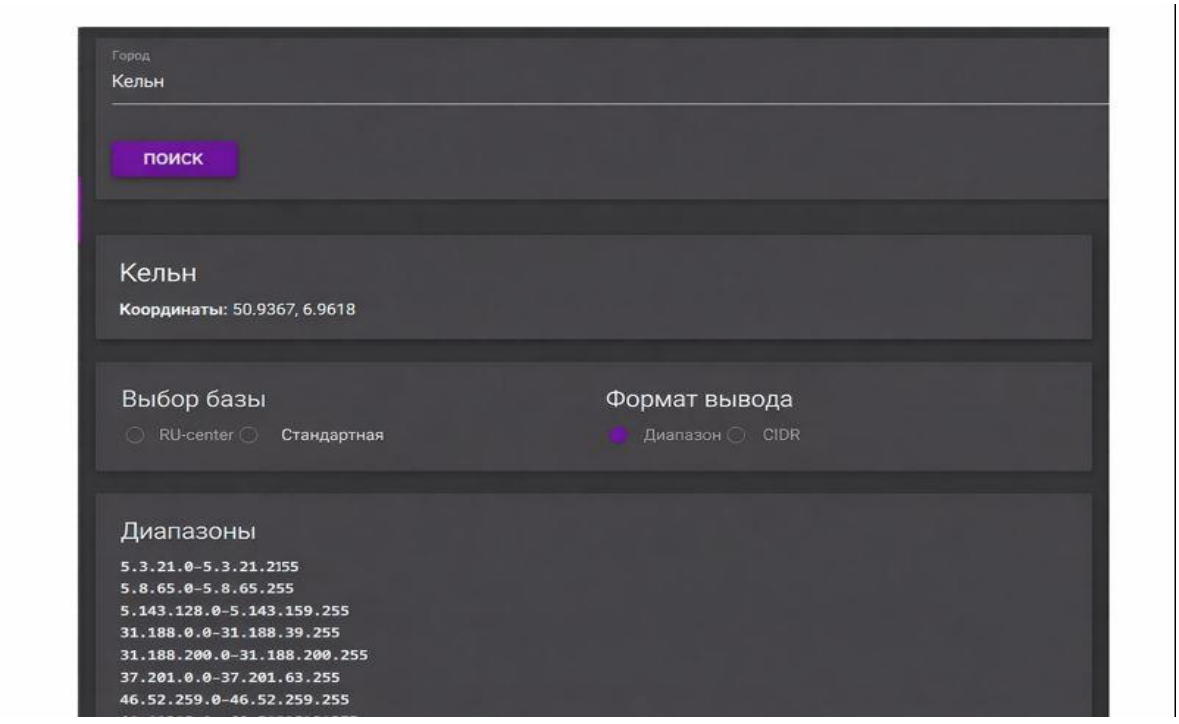


Рисунок 3.3 – Використання сервісу «4it.me» для пошуку діапазону IP-адрес міста

На рис. 3.3 наведено результати запиту до онлайн-сервісу 4it.me, який використовується для отримання географічних координат населеного пункту та відповідних йому діапазонів IP-адрес. Отримані IP-діапазони було збережено у файл *ranges.txt*, після чого активовано режим сканування в програмі Router Scan. Підсумкові результати виконаного сканування представлені на рис. 3.4.

Realtime Stats | Good Results | Search Results | Wireless Networks

Options: Follow last line | Default tab for AutoSave

Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type	Radio Off	Hidden	BSSID	ESSID	Security	Key	WPS PIN
80	78	Done		ASUS RT-N12VP							
80	78	Done		ASUS RT-N12VP							
8080	78	Done		ASUS RT-N12VP							
80	94	Done	admin:@Dpw1N1$Tr80R	Hikvision App-webs DS-2CD2512F-IS	-	-	<no wireless>	-	-	-	-
80	93	Done		ASUS RT-N12 Rev.C1							
8080	94	Cancelled		DD-WRT (name: DD-WRT, model: Dlink-DIR300 rev b)			F0:7D:68:81:7A:AC	dd-wrt			
80	78	Done		ASUS RT-N12VP							
8080	94	Done		ASUS RT-N14U			AC:9E:17:77:A9:AC	Wireless			
1080	78	Cancelled		D-Link FR1000-1, firmware: 1.0.9							
80	78	Cancelled		D-Link DIR-300, firmware: 3.0.1							
1080	78	Cancelled		D-Link FR1000-1, firmware: 1.0.9							
80	94	Cancelled		D-Link DIR-822, firmware: 2.0.17							
8088	78	Cancelled		D-Link DIR-300, firmware: 3.0.1							
80	94	Done		ASUS RT-N11P							
8080	94	Done		Netis WF2780 Router			00:72:63:3E:BA:C4	SD_WIFI_2.4G	WPA/WPA2	9105660100	05643776
80	109	Done	admin:putin[illegible]vlo1	ZyNOS ADSL (P-660RU-T1)	-	-	<no wireless>	-	-	-	-
8080	93	Done		ASUS RT-N65U			08:60:6E:65:BB:CC	BTE CBX			
80	78	Done	admin:admin123	Hikvision App-webs DS-2CD2522FWD-IS	-	-	<no wireless>	-	-	-	-
81	94	Done	admin:admin	PSI Alliance App-webs IS-3NA66	-	-	<no wireless>	-	-	-	-
8888	219	Done	<empty>:Putin[illegible]ilo	Tenda Realtek Router, firmware: V02.03.01.32_cn			50:0F:F5:11:05:10	sergei	WPA/WPA2	77280620	43558810
80	94	Done		ASUS RT-N10PV2							
80	94	Done	admin:V030707v	Hikvision App-webs NC22VPR	-	-	<no wireless>	-	-	-	-
80	78	Done		ASUS RT-N66U			60:A4:4C:D2:7C:68	ASUS-2.4G			

Рисунок 3.4 – Результати сканування програми Router Scan

З рисунка 3.4 видно результати виконаного сканування, у межах якого відображаються доступні мережеві інтерфейси та активні адреси пристроїв. В окремій інформаційній панелі наведені дані автентифікації, зокрема логіни та паролі, а також зазначено тип сервісу, що використовується на відповідному пристрої.

Слід відзначити, що окрім стандартної перевірки мережі на наявність відкритих портів, програмний інструмент Router Scan також використовує відому уразливість phpMyAdmin Remote Code Execution (RCE). Дана вразливість надає можливість віддаленому зловмиснику виконувати довільні SQL-запити до бази даних. У разі успішної експлуатації це може призвести до несанкціонованого читання, модифікації або видалення даних, а також до повного контролю над уразливим програмним забезпеченням.

У результаті проведеного дослідження за допомогою Router Scan було отримано автентифікаційні дані IoT-пристрою виробництва компанії Hikvision, що дозволило на практичному прикладі продемонструвати одну з актуальних проблем інформаційної безпеки в екосистемі Інтернету речей.

Ще одним ефективним інструментом для виявлення IoT-пристроїв у глобальній мережі є пошукова система Shodan. Shodan являє собою спеціалізований пошуковий сервіс, який надає можливість здійснювати пошук різних типів мережевих вузлів, зокрема веб-камер, маршрутизаторів, серверів та

іншого обладнання, що має пряме підключення до Інтернету, із використанням гнучкої системи фільтрів.

Даний сервіс часто характеризують як пошукову систему банерів служб, тобто метаданих, які сервер надсилає клієнту у відповідь на запит. До таких даних можуть належати відомості про серверне програмне забезпечення, підтримувані протоколи та опції, інформаційні повідомлення або інші параметри, доступні ще до безпосередньої взаємодії з сервісом [7].

Основною аудиторією Shodan є фахівці з кібербезпеки, дослідники у сфері інформаційних технологій та представники правоохоронних органів. Водночас доступ до цього інструменту можуть отримувати й зловмисники, хоча багато з них використовують альтернативні методи збору інформації, зокрема ботнети, які здатні виконувати подібні завдання без прямого виявлення [8].

Застосування пошукової системи Shodan дозволяє визначити загальну кількість IP-камер компаній Hikvision та Dahua, що перебувають у відкритому доступі, а також отримати інформацію про задіяні сервіси. Відповідні результати пошуку наведені на рисунку 3.5.

.

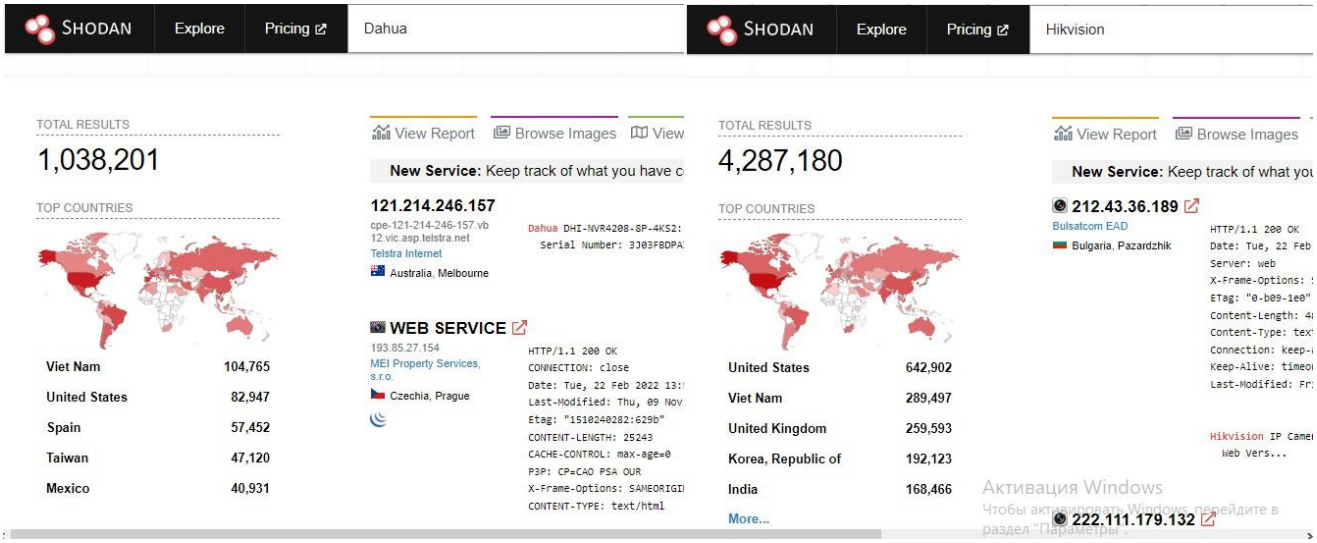


Рисунок 3.5 – Пошук IP-камер за допомогою пошукової системи Shodan

З рисунка 3.5 видно загальну кількість IoT-пристроїв, які потенційно можуть містити вразливості та належать виробникам систем відеоспостереження Dahua та Hikvision. Загальна кількість таких пристроїв становить 5 325 381 IP-камеру, що свідчить про значні масштаби проблеми безпеки. Наявність великої кількості вразливих пристроїв створює передумови для формування ботнет-мереж, у межах яких може використовуватися сукупна обчислювальна потужність сотень тисяч або навіть мільйонів IoT-пристроїв з метою здійснення масштабних DDoS-атак.

Для ефективного використання можливостей пошукової системи Shodan необхідно розуміти принципи формування пошукових запитів. IoT-пристрої функціонують за рахунок мережевих сервісів, а Shodan накопичує та зберігає інформацію про них у вигляді так званих банерів. Банер містить ключові метадані сервісу і є основним джерелом інформації в межах цього пошукового сервісу.

Подібно до класичних пошукових систем, Shodan підтримує прості запити за одним ключовим словом, однак його основна перевага полягає у можливості створення складних, параметризованих запитів, що значно розширюють аналітичні можливості.

Основні пошукові фільтри, які надає Shodan:

- City – пошук пристроїв у межах конкретного міста;
- Country – фільтрація результатів за країною розташування;
- Geo – пошук пристроїв за заданими географічними координатами;
- Hostname – відбір результатів за іменем хоста;
- Net – пошук за діапазоном IP-адрес;
- OS – фільтрація пристроїв за операційною системою;
- Port – виявлення пристроїв із відкритими портами;
- Vuln – пошук вузлів із відомими вразливостями;
- Before / After – обмеження результатів за часовим проміжком.

Shodan акумулює значні обсяги технічної інформації, яка зазвичай не є загальнодоступною, та подає її у зручному для аналізу форматі. Окрім цього, сервіс дозволяє здійснювати пасивний аналіз загроз, що є корисним інструментом для попередньої оцінки рівня уразливості та формування подальших напрямів дослідження інформаційної безпеки.

3.3 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2017-7253

У мережевих IP-камерах компанії Dahua з версією програмного забезпечення 3.200.0001.6 було виявлено критичну вразливість інформаційної безпеки, що отримала ідентифікатор CVE-2017-7253. Дана вразливість пов’язана з некоректною обробкою вхідних даних у невідомому фрагменті програмного коду, що дозволяє зловмиснику здійснити підвищення рівня привілеїв.

Інформація про вразливість була оприлюднена 30 березня 2017 року, а офіційна реєстрація в базі CVE відбулася 24 березня 2017 року. Експлуатація вразливості можлива віддалено та не потребує складної автентифікації, що значно підвищує рівень загрози. Для реалізації атаки достатньо наявності облікового запису з мінімальними привілеями.

Процес компрометації IP-камер Dahua з уразливим програмним забезпеченням може бути реалізований за таким сценарієм:

1) Використання стандартних облікових даних користувача з низьким рівнем доступу для формування спеціального запиту до визначеного URI, що дозволяє отримати перелік усіх користувачів системи.

2) подальший вхід до пристрою з використанням облікових даних адміністратора, що надає повний контроль над IP-камерою [9].

Експлуатація вразливості CVE-2017-7253 реалізується поетапно та включає такі кроки:

- виконання дампа бази даних віддалених користувачів
- визначення першого доступного облікового запису адміністратора з подальшим вилученням логіну та хешу пароля;
- ініціація ідентифікатора сесії, за необхідністю обчислює новий хеш (покоління три);
- виконання процедури автенфікації та завершення сеансу роботи з віддаленим пристроєм.

З метою виявлення потенційно вразливих IoT-пристроїв у мережі було використано сканер Zenmap, який є графічною оболонкою інструмента Nmap та забезпечує зручний доступ до його функціональних можливостей. Використання Zenmap дозволяє швидко ідентифікувати веб-сервери з відкритими портами та службами, що можуть бути пов’язані з уразливими IP-камерами. На рис. 3.6 наведено приклад результатів сканування мережі з метою виявлення потенційно вразливого веб-сервера.

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Dahua webcam httpd
|_http-favicon: Unknown favicon MD5: BD9E17C46BBBC18AF2A2BD718DDDAD0E
|_http-title: WEB SERVICE
| http-methods:
|_  Supported Methods: GET POST
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|WAP|router|VoIP phone
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X|2.4.X (96%), Excito embedded (91%), MikroTik RouterOS 6.X (89%), Drobo
embedded (89%), Grandstream embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/h:excito:b3 cpe:/o:linux:linux_kernel:4 cpe:/
o:linux:linux_kernel:2.4.20 cpe:/o:mikrotik:routeros:6.15 cpe:/h:drobo:5n cpe:/h:grandstream:gxv3275
Aggressive OS guesses: Linux 3.2 - 3.8 (96%), Linux 3.2 - 3.16 (93%), Linux 2.6.32 - 3.10 (93%), Linux 2.6.32 - 3.13 (91%
), Excito B3 file server (Linux 2.6.39) (91%), Linux 3.11 - 4.1 (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 2.6.33 (90%),
Tomato 1.27 - 1.28 (Linux 2.4.20) (89%), MikroTik RouterOS 6.15 (Linux 3.3.5) (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.219 days (since Sat Mar 19 06:09:03 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=241 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: webcam
```

Рисунок 3.6 – Пошук потенційно вразливого веб-серверу за допомогою сканера Zenmap

На рис. 3.6 відображено результати аналізу мережі, з яких видно, що на цільовому пристрої відкрито порт 80, через який функціонує HTTP-сервіс. На даному порту розгорнуто веб-сервер, що працює під керуванням операційної системи Linux та використовується в системі відеоспостереження виробника Dahua. З метою перевірки рівня захищеності було застосовано Proof of Concept (PoC) для вразливості CVE-2017-7253, у результаті чого проведено детальне дослідження веб-серверу. Отримані результати представлені на рис. 3.7.

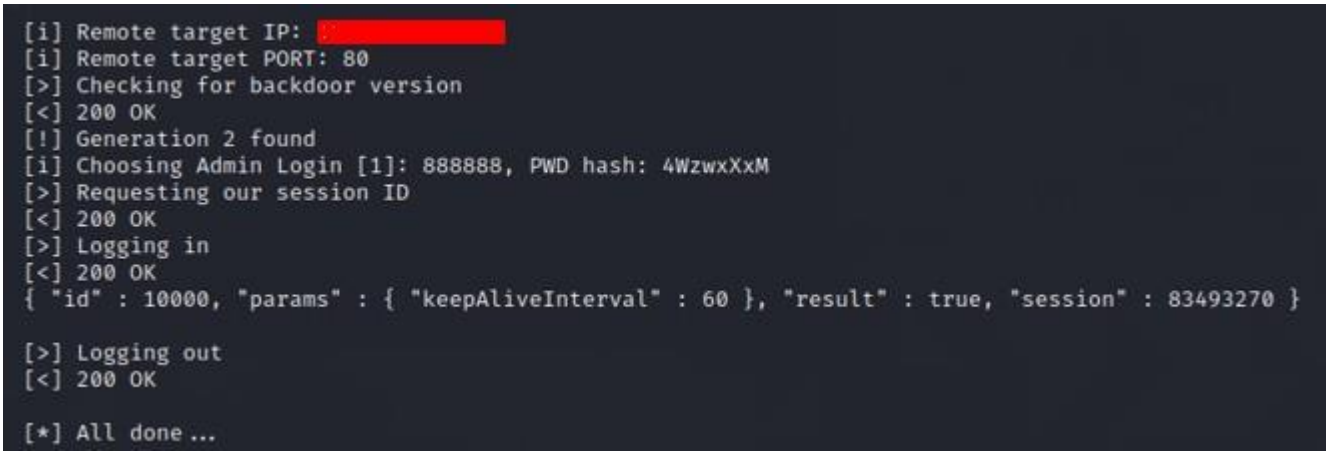


Рисунок 3.7 – Дослідження веб-серверу на вразливість CVE-2017-7253

Як показано на рис. 3.7, у ході аналізу веб-серверу було виконано запит програмного забезпечення до сервера з метою визначення його версії.

У даному випадку сервер ідентифікувався як такий, що належить до другого покоління. Після цього без проходження процедури автентифікації було здійснено отримання дампу бази даних віддалених користувачів.

У результаті було виявлено першого доступного облікового запису з адміністративними привілеями, для якого визначено логін **«888888»** та хеш пароля **«4WzwxXxM»**. Після отримання цих даних програмне забезпечення виконало процедуру входу на віддалений пристрій, отримало ідентифікатор активної сесії, а після успішної автентифікації завершило сеанс шляхом виходу з системи.

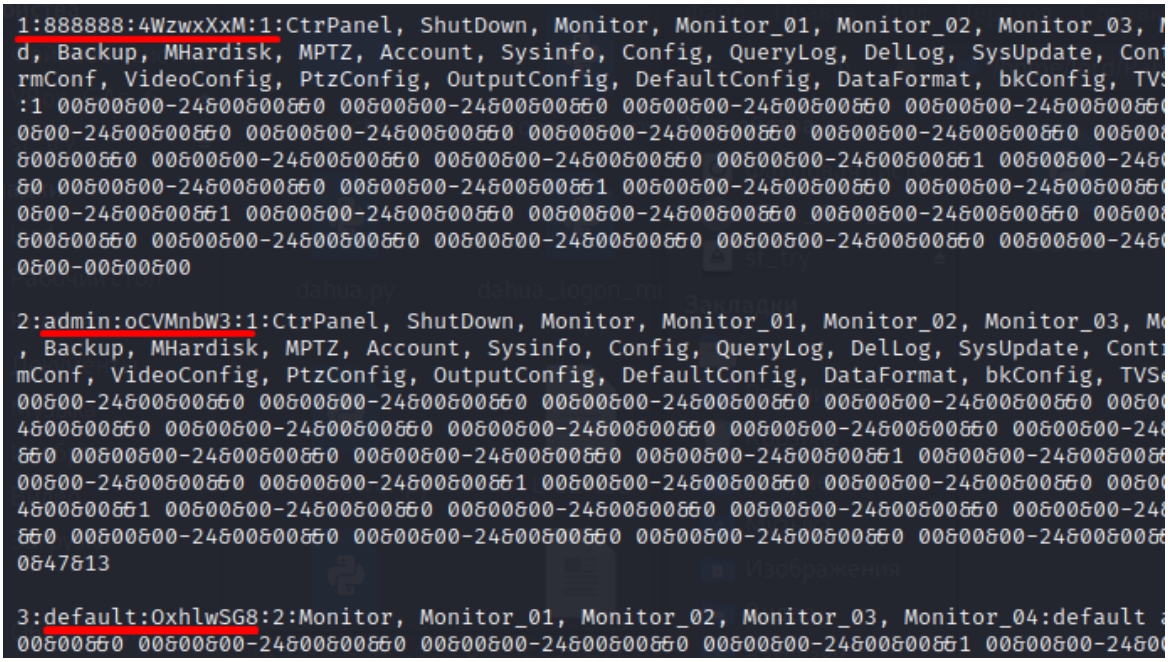


Рисунок 3.8 – Дамп бази даних віддалених користувачів з усіма обліковими даними

На рис. 3.8 представлено базу даних віддалених користувачів, яка містить три облікові записи. Основною причиною компрометації IoT-пристроїв у даному випадку є використання слабких або стандартних паролів. З цієї причини рекомендовано обов’язково змінювати паролі, встановлені за замовчуванням, на складні комбінації, що відповідають сучасним вимогам інформаційної безпеки.

Перший та третій облікові записи є прикладами жорстко закодованих облікових даних, тобто таких, у яких логін і пароль вбудовані безпосередньо у програмне забезпечення пристрою та не можуть бути видалені або змінені користувачем. Для другої версії програмного забезпечення продуктів Dahua перетворення відкритого пароля у хеш здійснюється з використанням власного 48-бітного алгоритму, тоді як у третій версії застосовується алгоритм хешування Message Digest 5 (MD5). В результаті цього хеш-значення «4WzwxXxM» відповідає відкритому паролю «888888», а хеш «OxhlwSG8» — паролю «default».

Відновлення відкритих паролів з отриманих хешів можливе за допомогою програмного забезпечення John the Ripper (JtR). John the Ripper є спеціалізованим інструментом для відновлення паролів за їх хеш-значеннями та широко використовується для аудиту слабких паролів у UNIX-подібних системах шляхом перебору можливих варіантів. Дане програмне забезпечення підтримує створення словників різної складності, автоматичне визначення типу хешу, а також витяг хешів із файлів, що є однією з його ключових переваг у порівнянні з аналогічними

інструментами. Програма також може виконувати аудит хешей Windows, Kerberos та інші. Існують реалізації під різні операційні системи. Дуже популярна через підтримку великої кількості хешей, авторозпізнавання хешу і налаштованого зламувача. Також підтримує безліч модулів, включаючи сторонні, що надають підтримку MD4 хешей, паролів баз даних тощо [10]. Приклад використання JtR для підбору пароля хешу «4WzwxXxM» за 48-бітним алгоритмом Dahua наведено на рис. 3.9.

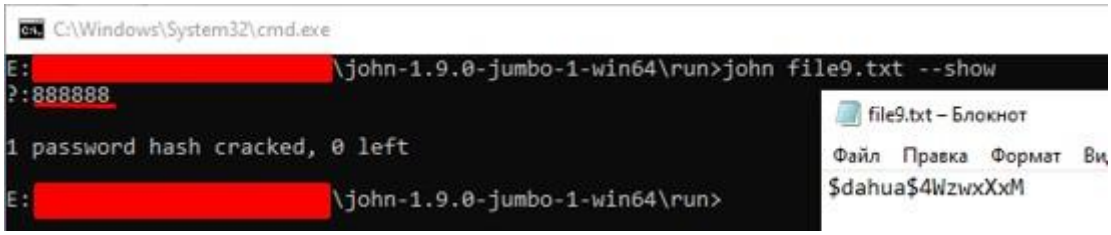


Рисунок 3.9 – Використання John The Ripper для підбору пароля

Можливо зробити проміжний висновок, що в такому випадку не виконуються основні методи безпеки. Вразливість CVE-2017-7253 є застарілою тому мало коли зустрічається, але становить критичний рівень небезпеки. Використання застарілого ПЗ та не своєчасне його оновлення призводить до компрометації системи. Порушено контроль доступу, оскільки при налаштуванні паролі за замовчуванням не були змінені та не змінено стандартні порти.

3.4 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2021-33044

Ще одна група уразливостей пов’язана з механізмом обходу автентифікації в пристроях Dahua, зокрема з вразливостями CVE-2021-33044 та CVE-2021-33045, які виникають під час процесу входу до системи. Зловмисник може обійти процедуру автентифікації шляхом формування та надсилання спеціально підготовлених шкідливих пакетів даних [11]. Дані вразливості пов’язані з некоректною обробкою вхідних даних у компоненті Data Packet Handler. Маніпуляції з неконтрольованими або невалідованими вхідними параметрами призводять до порушення механізмів перевірки автентичності, що створює умови для несанкціонованого доступу до пристрою. У результаті цього порушуються ключові властивості інформаційної безпеки, а саме конфіденційність, цілісність та доступність даних.

Обидві зазначені вразливості можуть бути експлуатовані дистанційно під час процедури автентифікації шляхом надсилання на цільовий пристрій спеціально сформованих пакетів даних. Приклади таких шкідливих пакетів наведено на рис. 3.10.

```
# Authentication bypass start
if logon == "netkeyboard":
    """ 'CVE-2021-33044, Authentication bypass,
    when setting param: 'clientType": "NetKeyboard' """
    params.update({
        "clientType": "NetKeyboard"
    })
    return params

elif logon == "loopback":
    """ loginType=5, @127.0.0.1 """
    """
    'CVE-2021-33045, Authentication bypass,
    when setting params: 'ipAddr':'127.0.0.1', 'loginType': 'Loopback' and 'clientType': 'Loca
    Note: Bypass fixed with newer firmware from beginning/mid 2020

    Legit usage: SNMP daemon traffic on 127.0.0.1 using port 5000 with l/p admin/admin
    """

    dh_hash = dahua_gen2_md5_hash(
        username=username, password=password, dh_realm=dh_realm, dh_random=dh_random,
        saved_host=saved_host)

    params.update({
        "loginType": "Loopback",
        "clientType": "Local",
        "passwordType": "Default",      # Plain working too
        "password": dh_hash     # Clear text password working too with 'passwordType': 'Plain'
    })

    return params
# Authentication bypass end
```

Рисунок 3.10 – Огляд спеціальних пакетів даних для уникнення автентифікації

Вразливість CVE-2021-33044 актуальна для тих IoT-пристроїв, програмне забезпечення яких не підтримує функціональність NetKeyboard та було випущене до червня 2021 року. У свою чергу, вразливість CVE-2021-33045 характерна для версій програмного забезпечення, датованих початком або серединою 2020 року. Додатково слід зазначити, що за наявності цих вразливостей програмне забезпечення надає можливість користувачам із мінімальними привілеями отримати повний доступ до консолі керування, зокрема шляхом анонімної автентифікації, що створює серйозну загрозу безпеці системи.

Для дослідження вразливості IoT-пристроїв Dahua обрано пошукову систему Shodan, яку наведено на рис. 3.11.

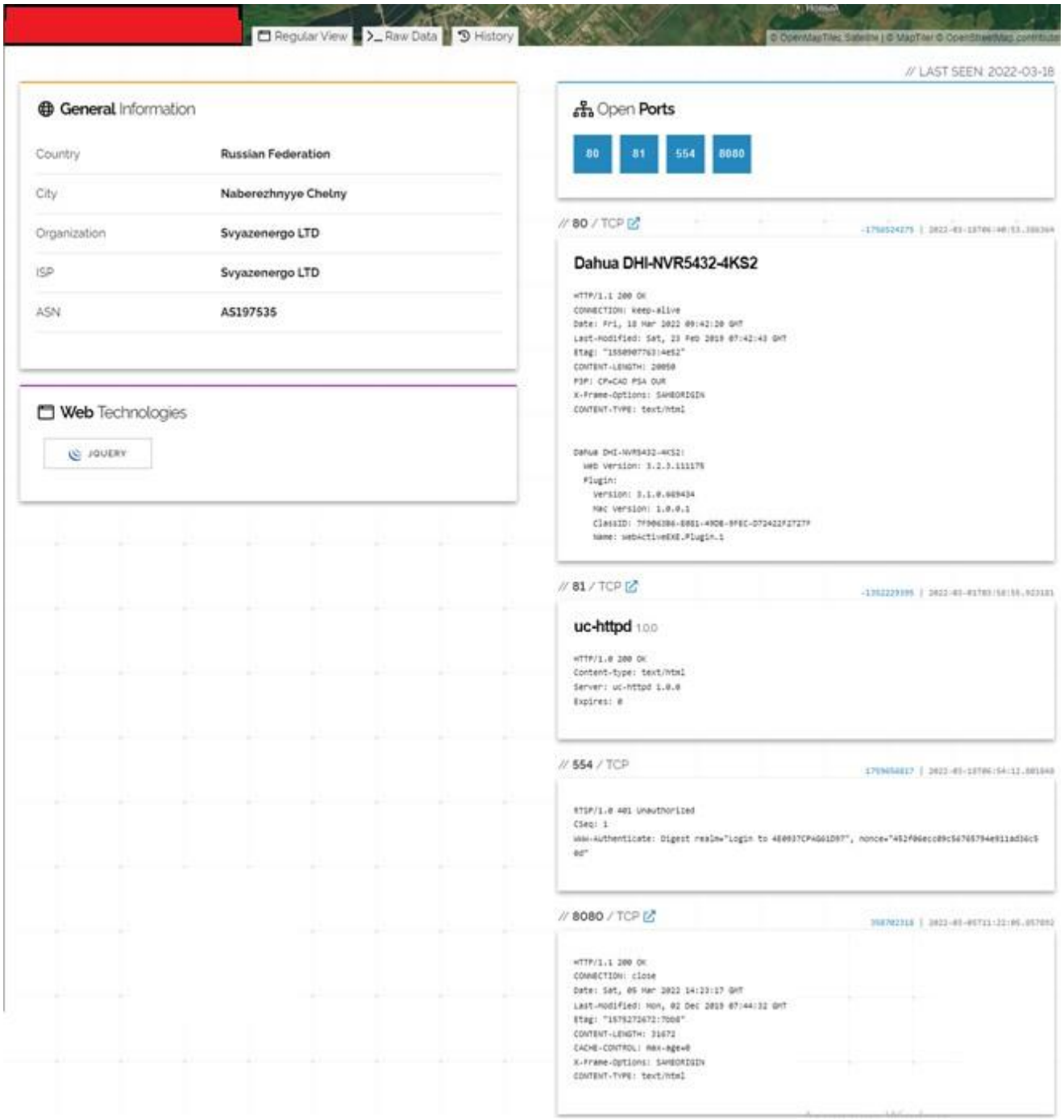


Рисунок 3.11 – Використання пошукової системи Shodan для IoT-пристроїв Dahua

На рис. 3.11 показано, що досліджуваний хост має декілька відкритих мережевих портів, на яких функціонують різні сервіси, при цьому основний веб-сервер працює через порт 80. Використовуючи отримані на попередніх етапах облікові дані, було здійснено експлуатацію вразливості CVE-2021-33044 із застосуванням протоколу HTTP через порт 8080. Результати проведеного дослідження наведені на рис. 3.12.

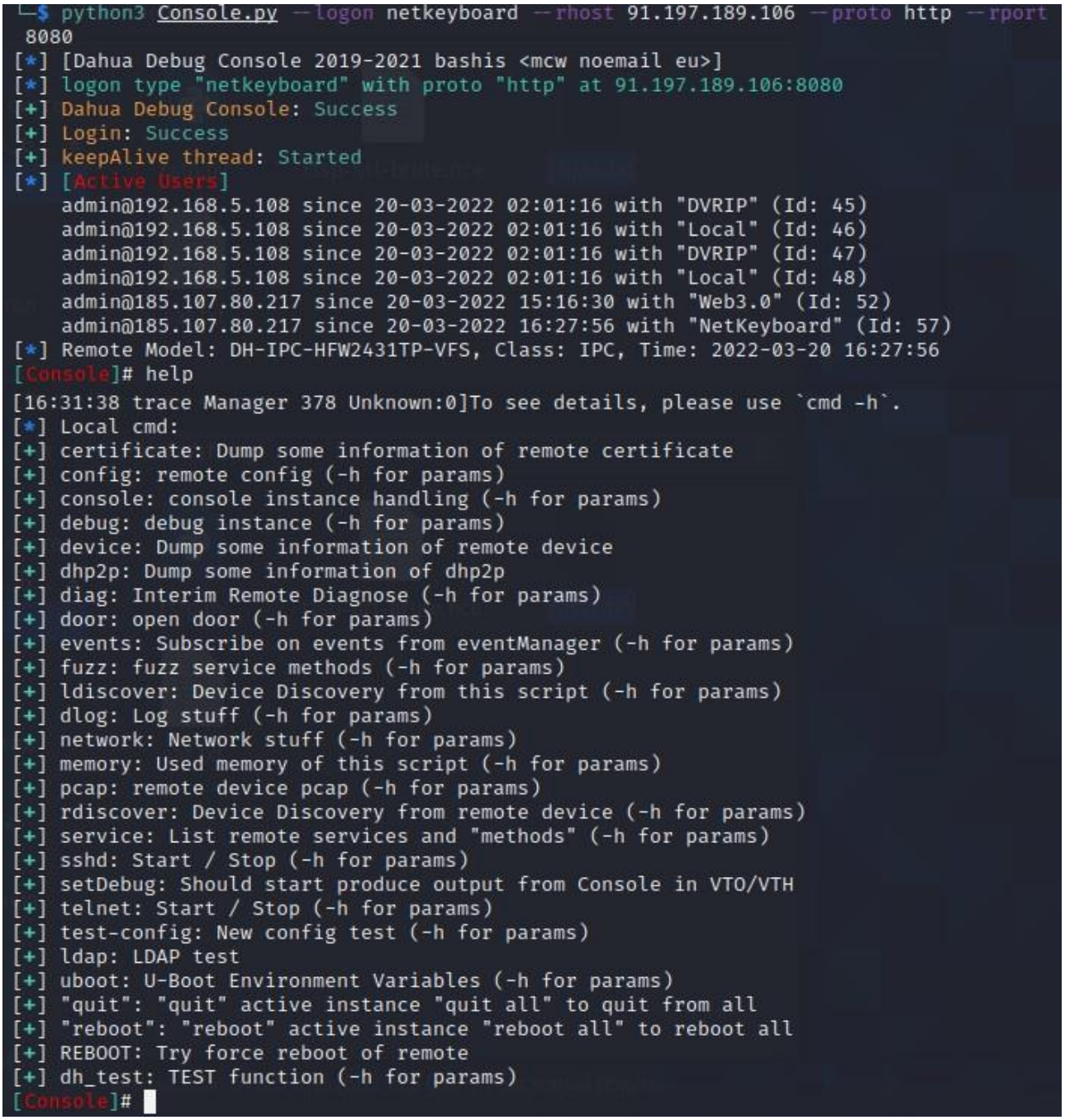


Рисунок 3.12 – Дослідження веб-серверу на вразливість CVE-2021-33044

На рис. 3.12 продемонстровано успішний обхід механізму автентифікації шляхом надсилання спеціально сформованих пакетів даних. У результаті експлуатації вразливості програмне забезпечення надає розширені функціональні можливості, зокрема дозволяє здійснювати дамп конфігураційних файлів системи та сертифікатів, активувати сервіси Telnet і SSH, а також виконувати інші адміністративні операції. На рис. 3.13 наведено результати отримання хеш-значень паролів та відповідних відкритих паролів.

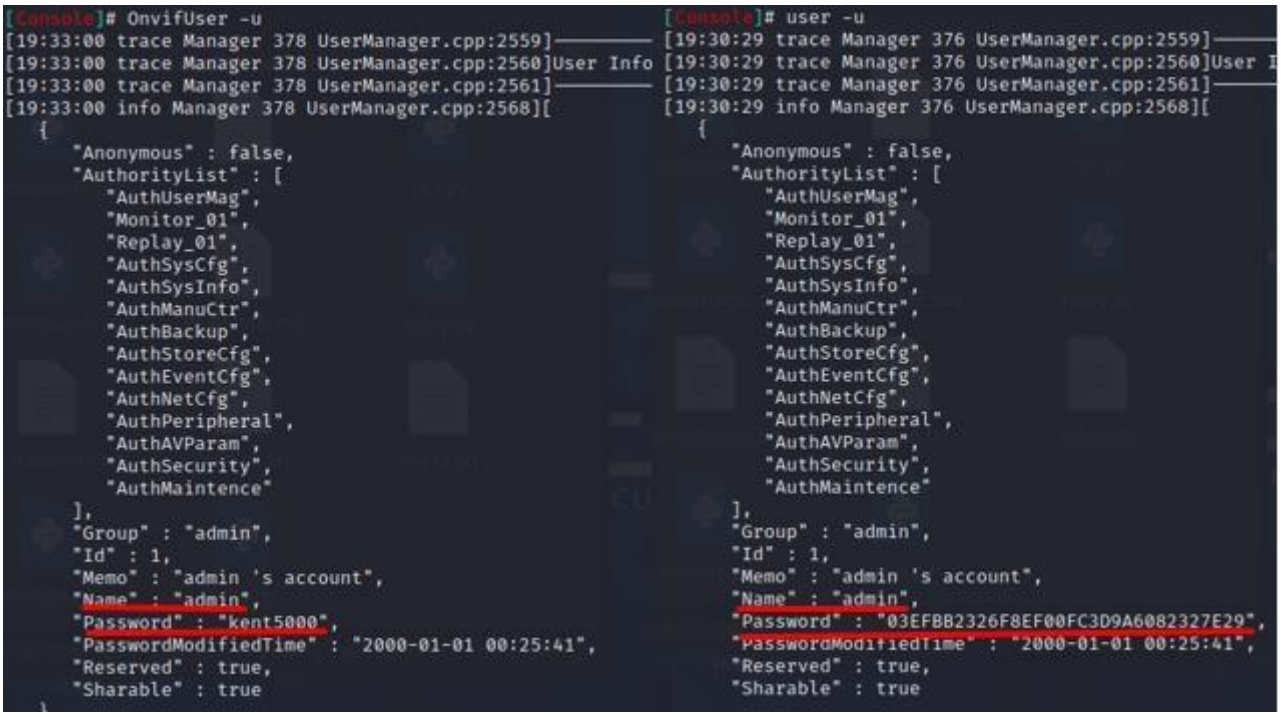


Рисунок 3.13 – Дамп хеш-паролю та відкритого паролю

Як показано на рис. 3.13, програмне забезпечення продуктів Dahua зберігає облікові дані не лише у хешованому вигляді, але й у відкритій формі, що становить суттєву загрозу для забезпечення конфіденційності інформації. Такий підхід до зберігання чутливих даних свідчить про недостатній рівень реалізації механізмів захисту. Додатковим підтвердженням цього є збереження паролів до бездротових мереж, сервісів Peer-to-Peer (P2P), FTP, Telnet та інших служб, що значно розширює потенційні вектори кібератак на систему. Як приклад порушення вимог конфіденційності на рис. 3.14 наведено збереження адреси електронної пошти у відкритому вигляді.

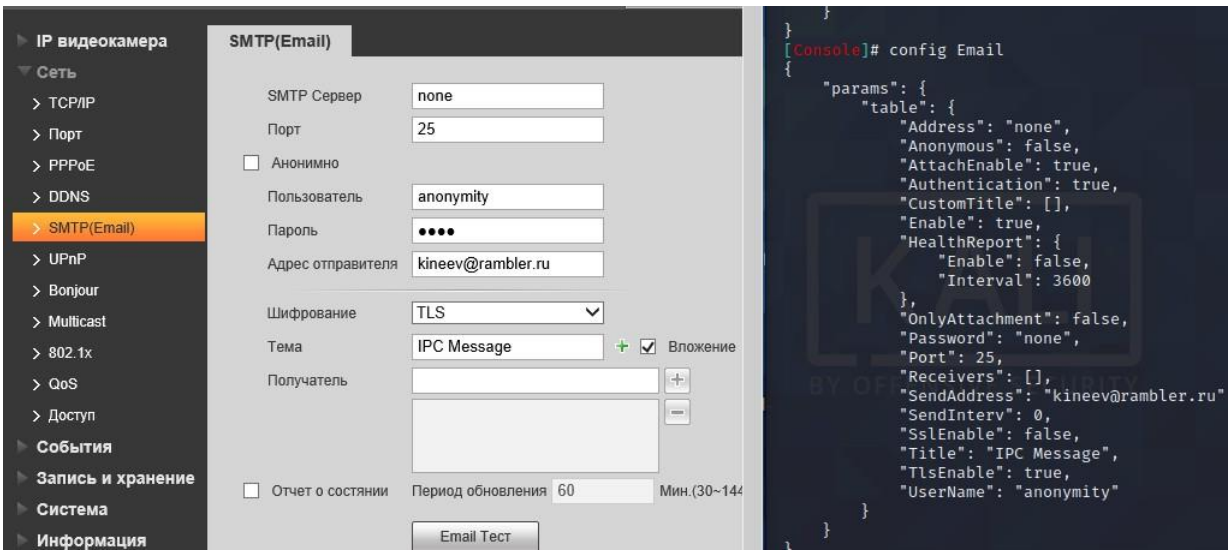


Рисунок 3.14 – Збереження адресу електронної пошти

Зберігання записів відеоспостереження на карті пам’яті Secure Digital (SD) підвищує рівень захисту конфіденційних даних, оскільки формує фізичний периметр безпеки, який простіше захистити, ніж мережеві канали. Використання хмарних сервісів або FTP-серверів для зберігання відеоданих є менш безпечним з точки зору інформаційної безпеки та може стати джерелом витоку інформації. Налаштування параметрів збереження відеозаписів наведено на рис. 3.15.



Рисунок 3.15 – Налаштування збереження записів відеоспостереження

Використовуючи отримані облікові дані з порту 8080, було здійснено вхід до основного веб-сервера через порт 80, оскільки параметри автентифікації є однаковими. Застосування ідентичних паролів для різних пристроїв становить критичну загрозу механізмам контролю доступу. На рис. 3.16 наведено перелік каналів передачі відеоданих головного веб-сервера.

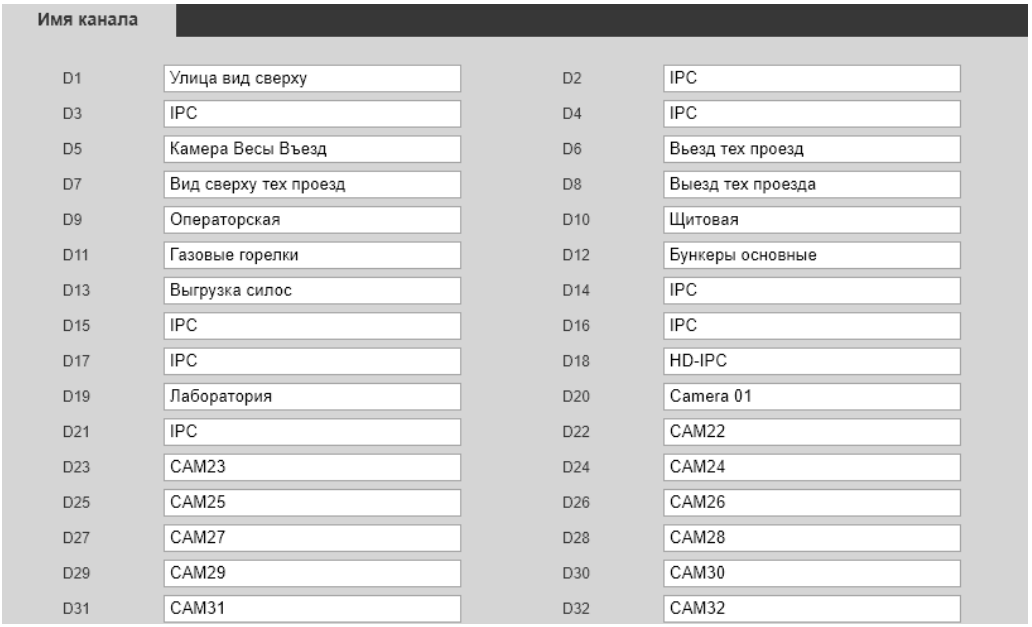


Рисунок 3.16 – Найменування каналів передачі даних відеоспостереження

Одним зі способів виявлення кібератак є використання журналу подій безпеки, який слугує централізованим сховищем системних логів для управління та аудиту безпеки. Постійний аналіз журналів у режимі реального часу дозволяє відстежувати стан системи, використання ресурсів і дії користувачів. У ході дослідження встановлено, що веб-сервер не використовує системний журнал, що унеможливлює аудит безпеки та своєчасне реагування на потенційні кібератаки. Перегляд налаштувань системного журналу наведено на рис. 3.17.

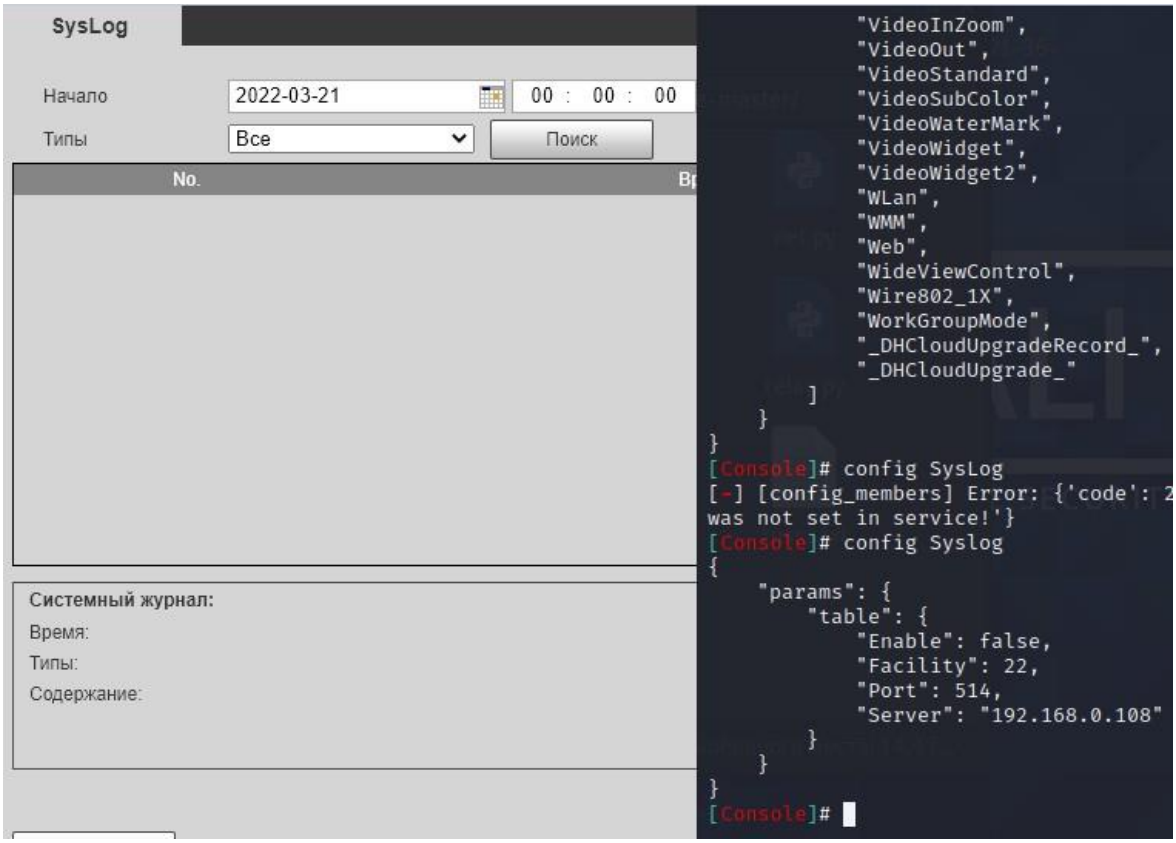


Рисунок 3.17 – Перегляд налаштування системного журналу

Стосовно безпеки, було переглянуте налаштування параметрів безпеки веб-серверу, яке зображене на рис. 3.18.

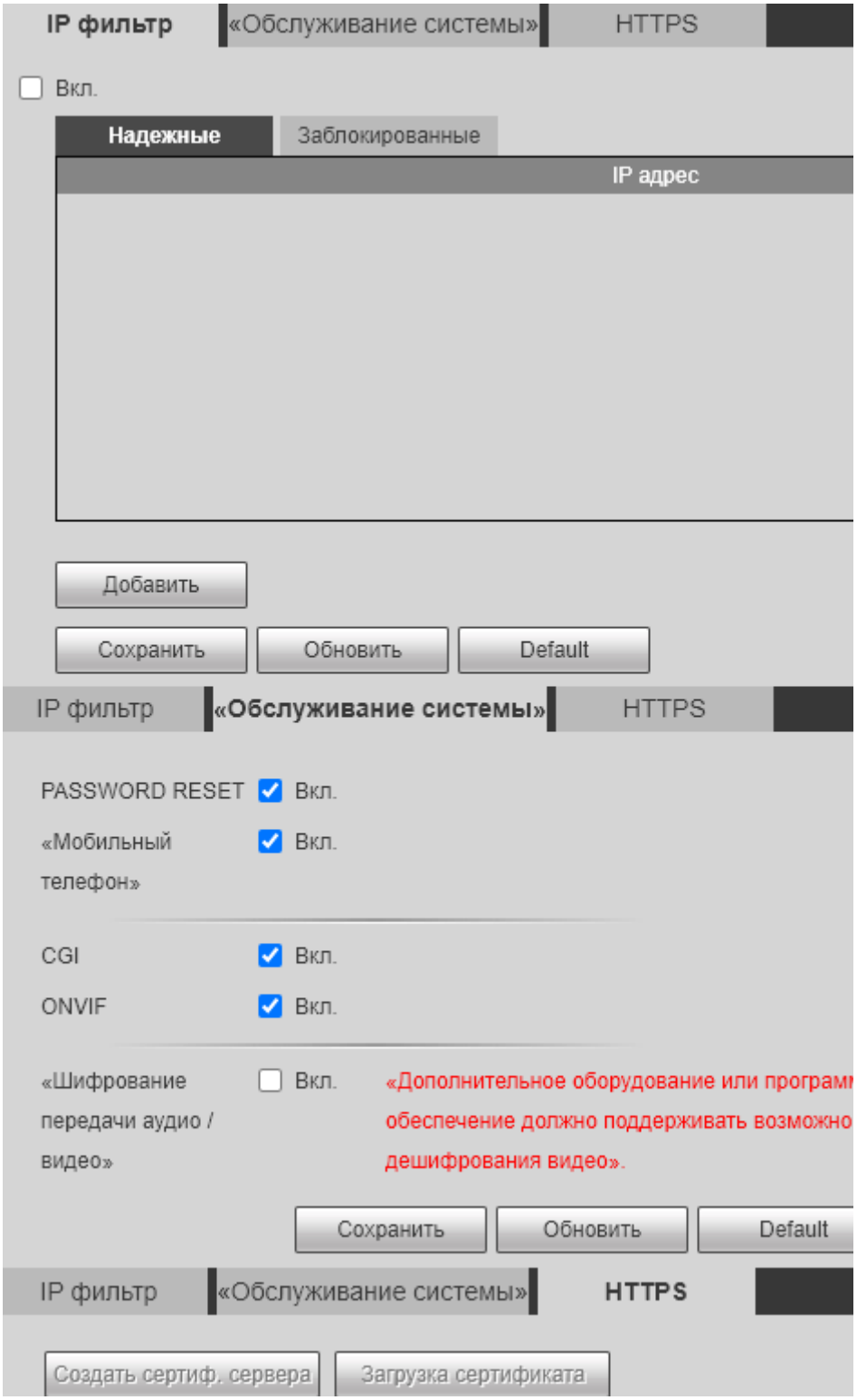


Рисунок 3.18 – Перегляд налаштування параметрів безпеки веб-серверу

На рис. 3.18 представлено основні параметри безпеки системи, зокрема IP-фільтрацію, обслуговування системи та налаштування протоколу HTTPS. Використання IP-фільтрації дозволяє обмежити доступ до пристрою з визначених адрес, що могло б запобігти компрометації системи навіть у разі отримання зловмисником облікових даних автентифікації.

У розділі обслуговування системи передбачено можливість відновлення пароля, керування пристроєм за допомогою мобільного телефону, а також підтримку протоколів CGI та ONVIF (профіль C), що спрощує інтеграцію зі стороннім програмним забезпеченням і забезпечує сумісність пристроїв різних виробників. Це сприяє відкритості та доступності ринку систем відеоспостереження. Крім того, на сервері можливо створити та завантажити самопідписаний або авторизований сертифікат X.509, що дозволяє використовувати протокол HTTPS і забезпечує захищений обмін даними між користувачем і сервером за допомогою криптографічних протоколів SSL/TLS.

Отже, досліджена версія програмного забезпечення пристроїв Dahua має обмежений набір механізмів забезпечення інформаційної безпеки, які до того ж не були належним чином задіяні. Не дотримано базових вимог безпеки, зокрема щодо контролю доступу, мінімізації поверхні атак, своєчасного оновлення програмного забезпечення, використання шифрування та захисту конфіденційних даних. Сукупність цих недоліків перетворює систему на легку ціль для потенційних зловмисників.

На підставі аналізу методів забезпечення інформаційної безпеки в IoT-мережах із використанням відомих уразливостей CVE-2021-33044 та CVE-2021-33045 було зроблено проміжний висновок, що зазначені уразливості мають критичний рівень небезпеки. Їх експлуатація призводить до порушення конфіденційності шляхом повного розкриття системної інформації та доступу до всіх файлів, втрати цілісності внаслідок повної компрометації системи, а також порушення доступності, оскільки зловмисник може повністю вивести ресурс з ладу та зробити його недоступним.

3.5 Дослідження пристроїв Інтернету речей на наявність вразливості CVE-2021-36260

Вразливість CVE-2021-36260 належить до класу ін’єкцій команд у веб-сервері окремих продуктів компанії Hikvision. Через відсутність належної перевірки вхідних даних зловмисник може сформувати спеціально підготовлений запит зі шкідливими командами та ініціювати атаку віддаленого виконання коду [12].

Дану вразливість було виявлено 20 червня 2021 року системним адміністратором та фахівцем з мережевої безпеки, відомим під псевдонімом Watchful_IP. Аналіз показав, що більшість сучасних моделей IP-камер Hikvision є

вразливими до критичної атаки віддаленого виконання коду без проходження автентифікації, навіть у версіях прошивок, актуальних станом на 21 червня 2021 року. Окрім цього, окремі застарілі моделі камер залишалися уразливими ще з 2016 року. Також було зафіксовано ураження деяких мережевих відеореєстраторів, хоча такі випадки трапляються рідше.

Під час дослідження було використано Proof of Concept (PoC), який реалізує механізм ін’єкції команд без автентифікації в IP-камери Hikvision. Встановлено, що модуль вбудовує шкідливу команду в корисне навантаження у форматі Extensible Markup Language (XML), яке передається у HTTP PUT-запиті на кінцеву точку /SDK/webLanguage. У результаті такої ін’єкції відбувається виконання команди від імені користувача з підвищеними привілеями (root). Реалізація PoC орієнтована на так звану «сліпу» атаку, за якої результат виконання команди безпосередньо не повертається зловмиснику. Перегляд програмного коду PoC з демонстрацією механізму ін’єкції команд у веб-сервер наведено на рис. 3.19.

```
def put(self, url, query_args, timeout):
    query_args = '<?xml version="1.0" encoding="UTF-8"?>' \
                 f'<language>$({query_args})</language>'
    return self.remote.put(self.uri + url, data=query_args, verify=False, allow_redirects=False, timeout=timeout)
```

Рисунок 3.19 – Перегляд програмного коду PoC з відображенням ін’єкції команд у веб-сервер

Це надає зловмиснику можливість повного захоплення пристрою з отриманням необмеженого доступу на рівні root. Такий рівень доступу перевищує повноваження легітимного власника пристрою, який зазвичай обмежений використанням так званої «захищеної оболонки» Perl Shell (psh). Дана оболонка фільтрує вхідні команди відповідно до заздалегідь визначеного набору дозволених, переважно інформаційних, інструкцій. У результаті успішної експлуатації вразливості відбувається повна компрометація IP-камери, що також створює можливість подальшого проникнення у внутрішні мережі та реалізації атак на пов’язані інформаційні ресурси.

Дана вразливість належить до категорії максимально критичних, оскільки дозволяє виконувати віддалений код без проходження процедури автентифікації. Для її експлуатації від власника пристрою не потрібні жодні дії, що робить атаку особливо небезпечною та масовою для великої кількості IP-камер компанії Hikvision. У результаті під загрозу потрапляють не лише самі пристрої, а й внутрішні мережі, до яких вони підключені, що значно розширює можливі вектори кібератак. З огляду на те, що такі камери часто використовуються на об’єктах

підвищеної важливості, існує реальний ризик компрометації навіть елементів критично важливої інфраструктури.

Дана вразливість належить до критичного класу та має комплексний вплив на всі основні властивості інформаційної безпеки. Порушується конфіденційність, оскільки зловмисник отримує повний доступ до системних файлів і службової інформації. Цілісність системи також зазнає повного руйнування через можливість зміни або видалення даних та механізмів захисту. Крім того, під загрозою перебуває доступність ресурсу, адже атакуючий може повністю вивести пристрій з експлуатації або зробити його недоступним для легітимних користувачів.

Для перевірки наявності вразливості достатньо мати мережевий доступ до HTTP/HTTPS-сервера пристрою (зазвичай порти 80 або 443). Автентифікаційні дані не потрібні, а власник IP-камери не повинен виконувати жодних дій. Атака відбувається непомітно для системи журналювання самого пристрою. З цією метою за допомогою пошукової системи Shodan було виявлено тридцять п’ять потенційно вразливих IoT-пристроїв, приклад одного з яких наведено на рис. 3.20.

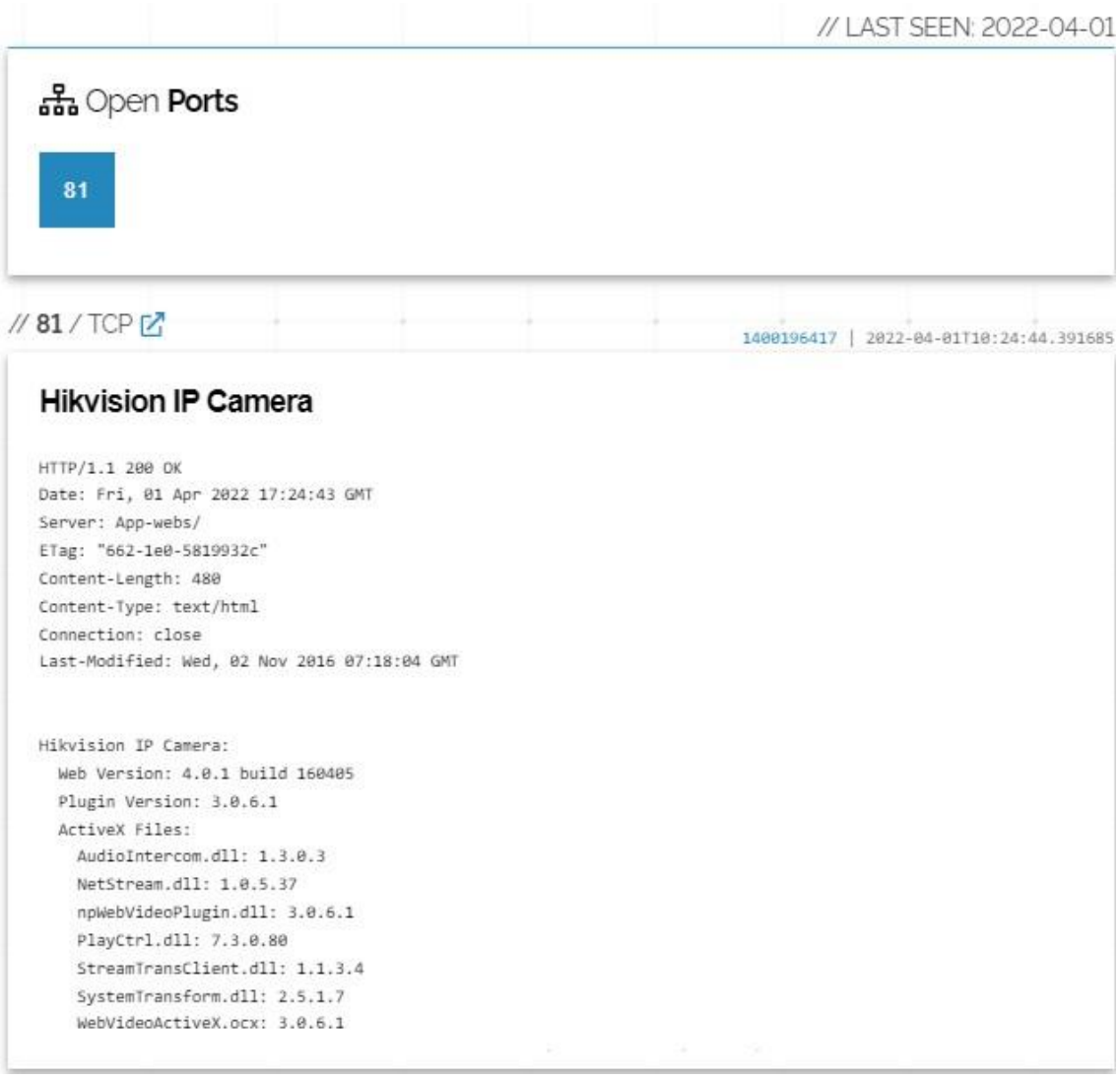


Рисунок 3.20 – Використання системи Shodan для IoT-пристроїв Hikvision

З рис. 3.20 видно, що хост має відкритий порт HTTP, а останнє оновлення програмного забезпечення виконувалося у 2016 році, що свідчить про потенційну вразливість пристрою. Аналіз інших досліджуваних IoT-пристроїв показав наявність кількох відкритих портів, при цьому щонайменше один сервіс використовував застаріле ПЗ, що вказує на значну поверхню атаки. Після збору необхідної інформації було проведено перевірку на наявність вразливості, результати якої наведено на рис. 3.21.

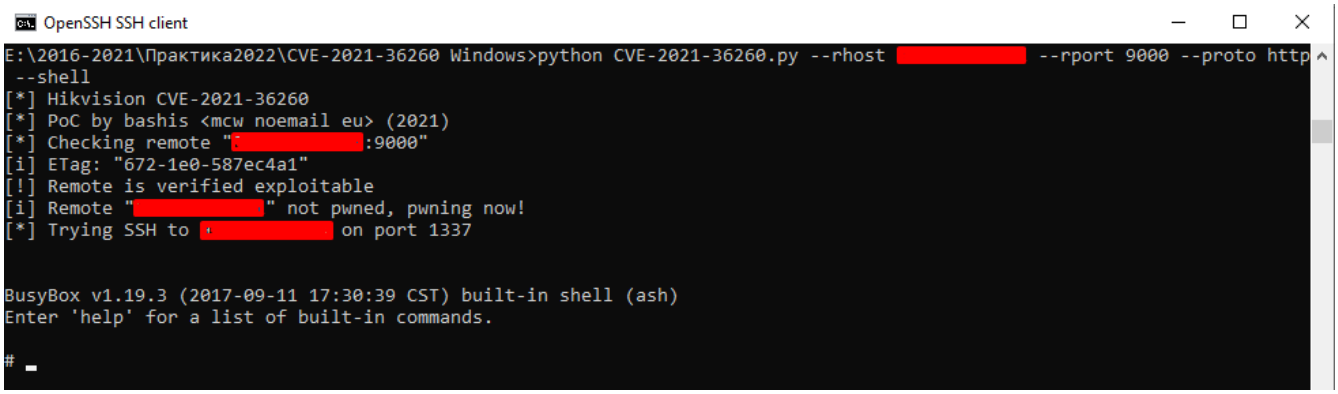


Рисунок 3.21 – Дослідження веб-серверу на вразливість CVE-2021-36260

З рис. 3.21 видно процес експлуатації вразливості. На початковому етапі програмне забезпечення перевіряє доступність цільового пристрою, після чого виконує двоетапну перевірку на наявність уразливості: визначає, чи є кінцева точка IP-камерою Hikvision, та аналізує її реакцію на спробу експлуатації. У розглянутому випадку пристрій виявився вразливим, унаслідок чого була виконана ін’єкція команд шляхом надсилання HTTP-запиту PUT з корисним навантаженням у форматі XML. Як команда могла використовуватися ініціалізація SSH-з’єднання або виконання сліпої команди. В результаті було отримано обмежену оболонку Almquist shell (ash), яка підтримує базовий набір вбудованих команд та параметрів і може застосовуватися для перевірки shell-скриптів на сумісність.

Таким чином зловмисник отримує можливість переглядати структуру каталогів та вміст файлів, що зберігаються на IoT-пристрої (приклад наведено на рис. 3.22). Доступ до системних файлів без проходження процедури автентифікації та можливість їх модифікації підтверджують критичний рівень уразливості, оскільки повністю порушуються механізми захисту інформації.

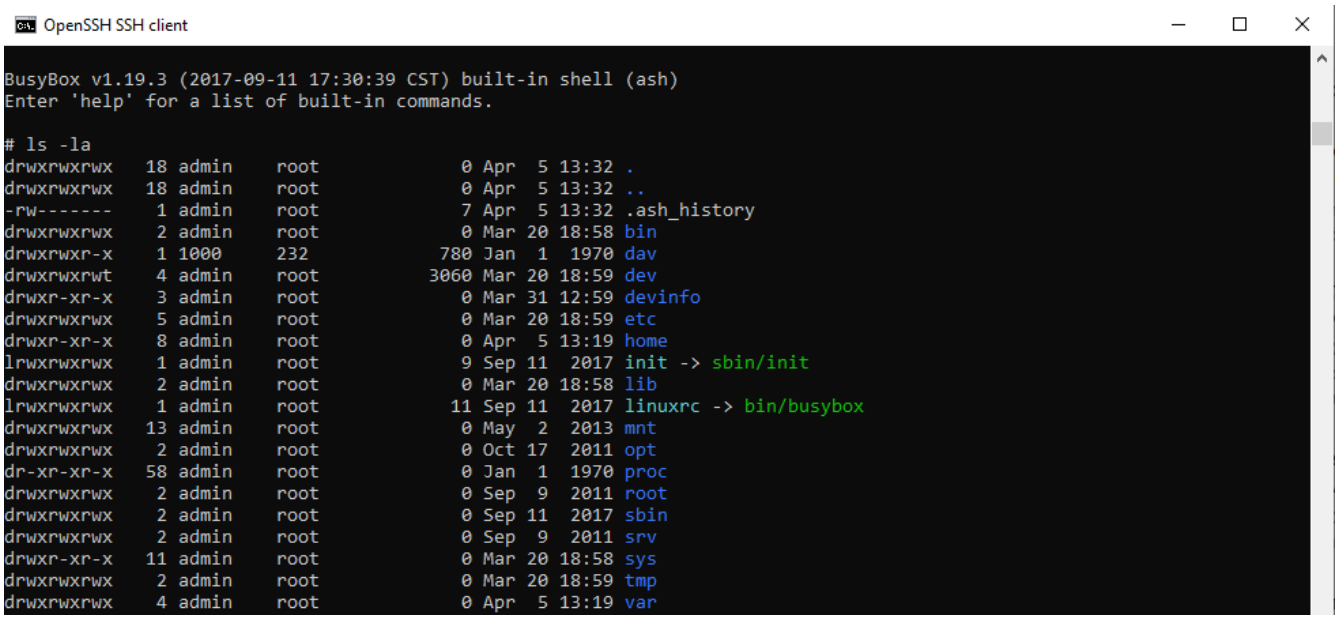


Рисунок 3.22 – Перегляд системних файлів

На рис. 3.22 наведено перелік системних файлів пристрою, доступ до яких не обмежено, а їх редагування не блокується жодними механізмами захисту. Така ситуація створює пряму загрозу основним властивостям інформації як об’єкта захисту, зокрема конфіденційності, цілісності та доступності. Особливу зацікавленість з погляду безпеки становлять каталоги /devinfo та /etc, які містять конфіденційні системні дані. Каталог /devinfo зберігає відомості про апаратну частину пристрою та інформацію, що на ньому розміщена.

Перегляд файлів, які містяться у каталозі /devinfo, наведено на рис. 3.23.

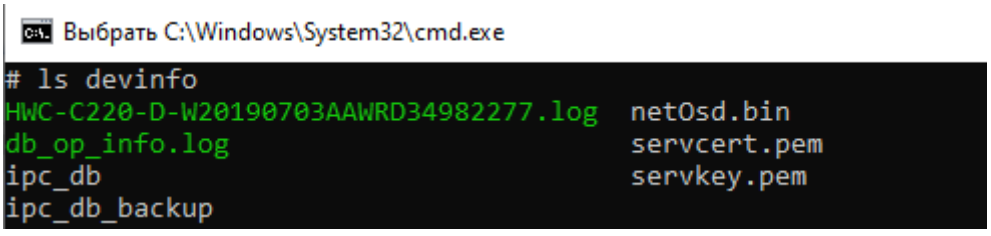


Рисунок 3.23 – Перегляд файлів у каталозі «/devinfo»

У каталозі /devinfo були виявлені файли ipc_db та ipc_db_backup, які є базами даних формату SQLite 3. Зазначені файли містять критично важливу інформацію, зокрема паролі у відкритому вигляді, параметри внутрішніх мереж, дані сервісів та інші конфіденційні відомості. Наявність таких даних без будь-якого механізму захисту свідчить про серйозні порушення вимог інформаційної безпеки. Вміст резервної бази ipc_db_backup наведено на рис. 3.24.

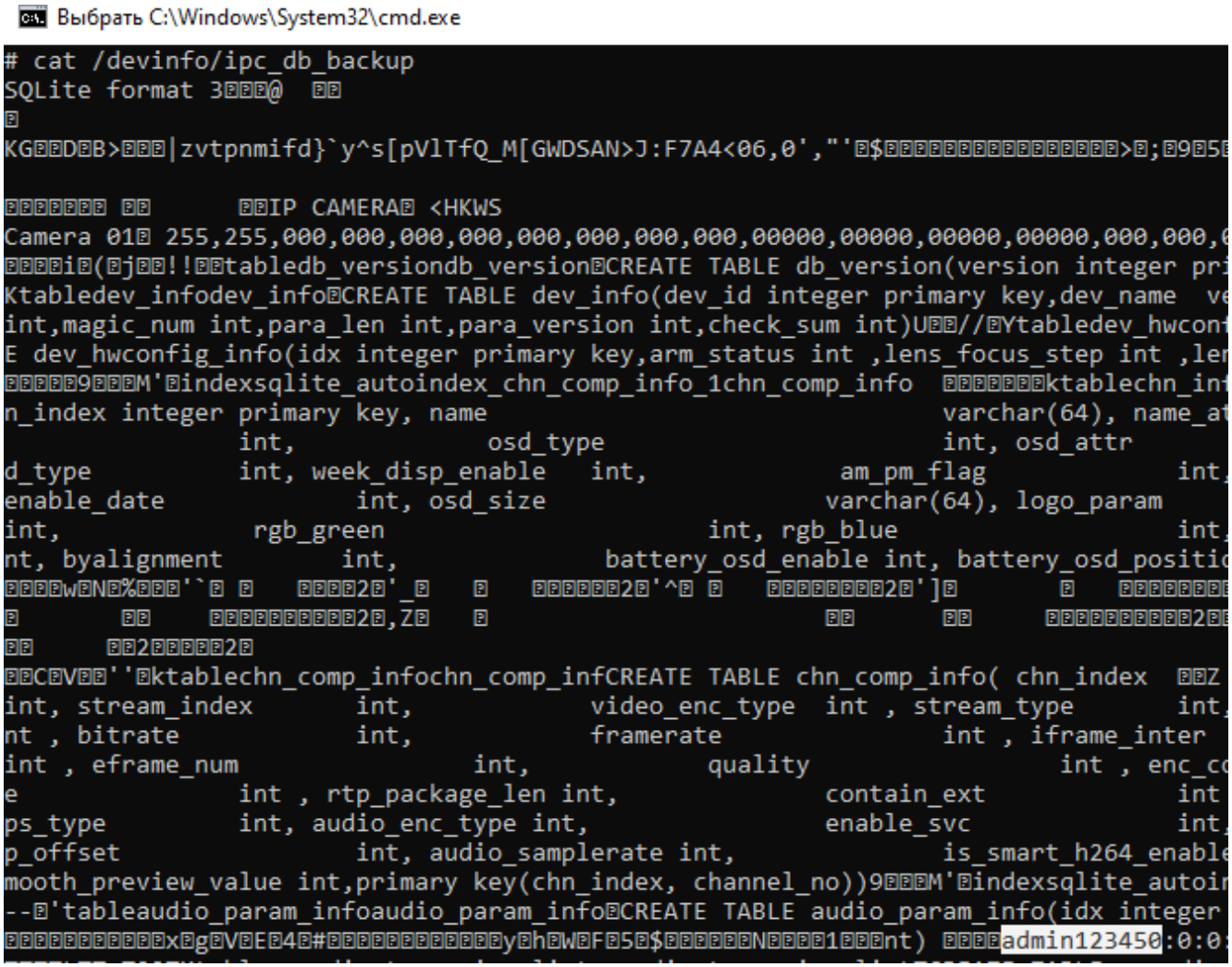


Рисунок 3.24 – Перегляд інформації, що зберігається в каталозі «ipc_db_backup»

З рис. 3.24 видно конфігураційні параметри IP-камери, а також відкритий стандартний пароль адміністратора – «admin123450», що свідчить про критичні недоліки захисту доступу.

Каталог «/etc» є важливою частиною файлової системи, оскільки містить конфігураційні файли системних служб і програм. Особливу зацікавленість для зловмисника становить файл «/etc/passwd», у якому зберігається перелік облікових записів користувачів у текстовому вигляді. Основне призначення цього файлу полягає у зіставленні імен користувачів з їх ідентифікаторами, а також збереженні хешів паролів, що використовуються під час автентифікації. Кожен запис у файлі відповідає окремому користувачеві та містить сім полів, розділених символом двокрапки: ім’я користувача, хеш пароля, ідентифікатор користувача, ідентифікатор групи, службову інформацію, домашній каталог та командну оболонку. Доступ до цього файлу без проходження автентифікації є прямою загрозою конфіденційності та цілісності системи.

Перегляд файлу «/etc/passwd», що містить список облікових записів користувачів наведено на рис. 3.25.

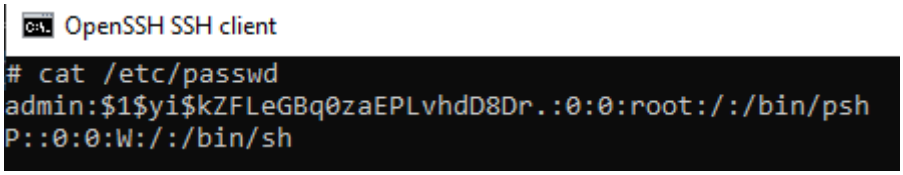


Рисунок 3.25 – Перегляд файлу «/etc/passwd», що містить список облікових записів користувачів

На рис. 3.25 представлено ім’я користувача та відповідний йому хеш пароля. Таким чином було отримано службову інформацію про пристрій, доступ до якої не повинен надаватися стороннім особам. Зокрема, файл «/etc/passwd» містить дані про облікові записи користувачів, при цьому пароль адміністратора системи, як правило, співпадає з паролем адміністратора веб-інтерфейсу IP-камери.

Після отримання відомостей про наявні облікові записи зловмисник може скористатися ними для несанкціонованого доступу або змінити існуючі дані, зокрема шляхом створення власних облікових записів із підвищеними привілеями. Один із можливих способів реалізації такої атаки полягає у внесенні змін до бази даних «ipc_db» або безпосередньо до файлу облікових записів «/etc/passwd», з подальшим збереженням змін для забезпечення постійного доступу. Приклад редагування файлу облікових записів «/etc/passwd» відображено на рис. 3.26.

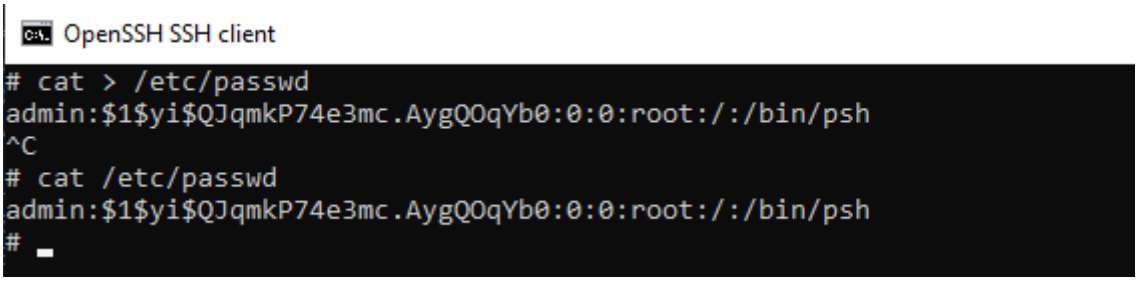


Рисунок 3.26 – Приклад редагування файлу облікових записів «/etc/passwd»

На рис. 3.26 представлено хеш пароля, сформований із використанням алгоритму MD5Crypt. Для визначення алгоритму хешування необхідно проаналізувати структуру самого хешу. Першим елементом є сигнатурне поле, у даному випадку 1, яке слугує ідентифікатором застосованого алгоритму. Так, значення ідентифікатора «1» відповідає алгоритму MD5, тоді як, наприклад, ідентифікатор «2a» вказує на використання алгоритму Blowfish. Друге поле відповідає за сіль (до восьми довільних символів, в цьому випадку «yi»). Третє поле є хешем.

Алгоритм формування дайджесту повідомлень MD5 є 128-бітовою криптографічною хеш-функцією, створеною Рональдом Рівестом у 1991 році. Протягом тривалого часу він активно застосовувався для хешування паролів і контролю цілісності файлів та виконуваних модулів. Проте на сьогодні MD5 вважається криптографічно ненадійним через доведені атаки на колізії, у зв'язку з чим його використання в системах інформаційної безпеки не рекомендується.

Функція crypt призначена для формування «солоних» хешів на основі відкритого тексту пароля та випадково згенерованої або заданої солі з метою безпечного зберігання облікових даних. Вона широко підтримується сучасними програмними бібліотеками та може застосовувати різні базові алгоритми хешування, зокрема MD5, Blowfish або алгоритми сімейства Secure Hash Algorithm (SHA).

Використання солі гарантує, що однакові паролі не призводять до однакових хеш-значень, що суттєво ускладнює застосування атак із використанням попередньо обчислених таблиць. Реалізація MD5Crypt додатково застосовує механізм багаторазового хешування (розтягнення), що значно підвищує обчислювальну складність атак перебором і знижує їх ефективність.

Алгоритм MD5Crypt умовно поділяється на три основні етапи: ініціалізацію, ітераційний цикл та завершальну фазу. Нижче наведено стислий опис принципу його роботи.

1) На початковому етапі формується базовий MD5-хеш, що обчислюється на основі комбінації пароля користувача та сольового значення.

2) Далі виконується багаторазовий ітераційний процес, який складається з тисячі повторень. Під час кожної ітерації створюється новий MD5-хеш на основі попереднього значення з чергуванням пароля та солі, що значно підвищує обчислювальну складність зламу.

3) На завершальному етапі отриманий результат кодується за допомогою спеціального варіанту Base64, унаслідок чого формується кінцевий рядок хешованого пароля.

Альтернативним способом проходження автентифікації для зловмисника є відновлення пароля у відкритому вигляді. З цією метою застосовуються спеціалізовані програмні засоби, що реалізують такі базові методи атак, як перебір усіх можливих комбінацій (brute-force) або словникова атака. Словникова атака передбачає поетапну перевірку паролів зі заздалегідь підготовленого списку, який може містити слова з мовних словників, поширені комбінації паролів або їх модифікації із заміною літер цифрами та спеціальними символами. Такий підхід є

різновидом атаки грубою силою, однак значно ефективніший з погляду витраченого часу. Основна відмінність між класичною атакою перебором і словниковою атакою полягає в обсязі перевірюваних варіантів: у першому випадку тестуються всі можливі комбінації символів, тоді як у другому — лише ті значення, які мають найбільшу ймовірність успішного підбору, що суттєво скорочує час атаки. Таким чином, маючи вхідні дані (алгоритм хешування, сіль та хеш) для підбору паролю було використано атаку за словником за допомогою вже згадуваного JtR, результати підбору паролів відображено на рис. 3.27.

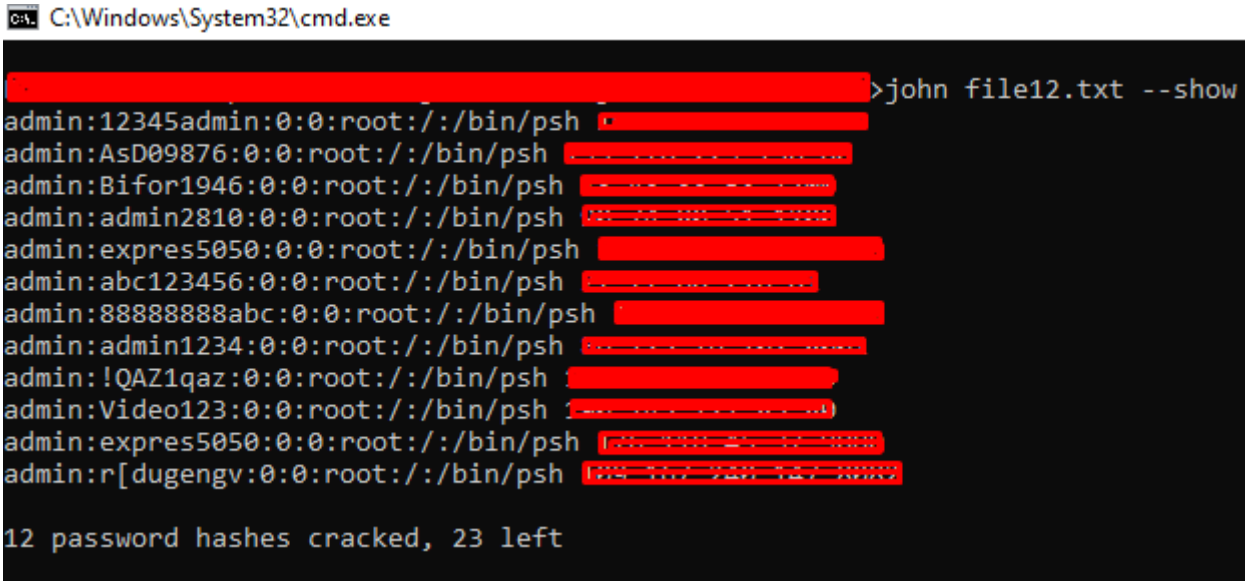


Рисунок 3.27 – Результати підбору паролів за словником

З рис. 3.27 видно результати підбору паролів, де загальна кількість проаналізованих хешів становить 35. Із них 12 паролів було успішно відновлено, тоді як 23 хеші не вдалося зламати, що свідчить про їх достатню криптографічну стійкість. Таким чином, можна зробити висновок, що переважна частина користувачів дотримувалася базових рекомендацій щодо створення надійних паролів, що позитивно вплинуло на рівень захисту облікових записів.

Використовуючи програмну реалізацію вразливості, пов’язаної з віддаленим виконанням коду, зловмисник отримує можливість автоматизувати процес атаки або здійснити зараження системи відеоспостереження шляхом впровадження шкідливого програмного забезпечення, зокрема типу Stealer, призначеного для викрадення конфіденційних даних.

Шкідливе програмне забезпечення класу Stealer належить до найбільш поширених типів сучасних кіберзагроз. Основною метою таких програм є максимальне вилучення персональних і службових даних користувача — від загальної системної інформації до локально збережених облікових записів і паролів

[2]. У розглянутому випадку застосування шкідливого ПЗ типу *Stealer* може призвести до несанкціонованого отримання бази даних віддалених користувачів разом з усіма обліковими даними, збережених параметрів автентифікації бездротових мереж, хмарних сервісів і служб, зокрема FTP, P2P, Telnet, електронної пошти та інших. Окрім цього, зловмисник може отримати відомості про топологію локальної мережі, а також доступ до відео- й аудіозаписів системи відеоспостереження. Використовуючи IP-камеру як точку входу, атака дозволяє сформувати уявлення про планування приміщення, наявні матеріальні цінності та підключені пристрої мережі. Отримання подібної інформації становить суттєву загрозу та є серйозним порушенням вимог щодо захисту конфіденційності даних.

У системах відеоспостереження компанії Hikvision передбачено низку базових параметрів безпеки, зокрема механізми автентифікації, фільтрацію IP-адрес та окрему службу безпеки.

Налаштування автентифікації фактично обмежується одним параметром — контролем доступу за протоколом Real Time Streaming Protocol (RTSP). RTSP є протоколом потокової передачі в реальному часі, який визначає набір команд для керування відеопотоками. Він використовується для трансляції зображення, наприклад, від IP-камери до відеореєстратора або серверної частини системи. У разі вимкнення автентифікації RTSP будь-який користувач, маючи IP-адресу пристрою, зможе отримати доступ до відеопотоку без додаткової перевірки прав доступу. Функція фільтрації IP-адрес дозволяє обмежити доступ до пристрою шляхом формування списків дозволених або заборонених адрес, що підвищує рівень контролю доступу. Для забезпечення безпечного віддаленого керування та додаткового захисту даних передбачено окрему службу безпеки. В її межах реалізовано механізм блокування несанкціонованого входу, який автоматично обмежує доступ з певної IP-адреси у випадку семи послідовних невдалих спроб введення облікових даних адміністратора.

Огляд параметрів безпеки, що налаштовані на IoT-пристрої наведені на рис. 3.28

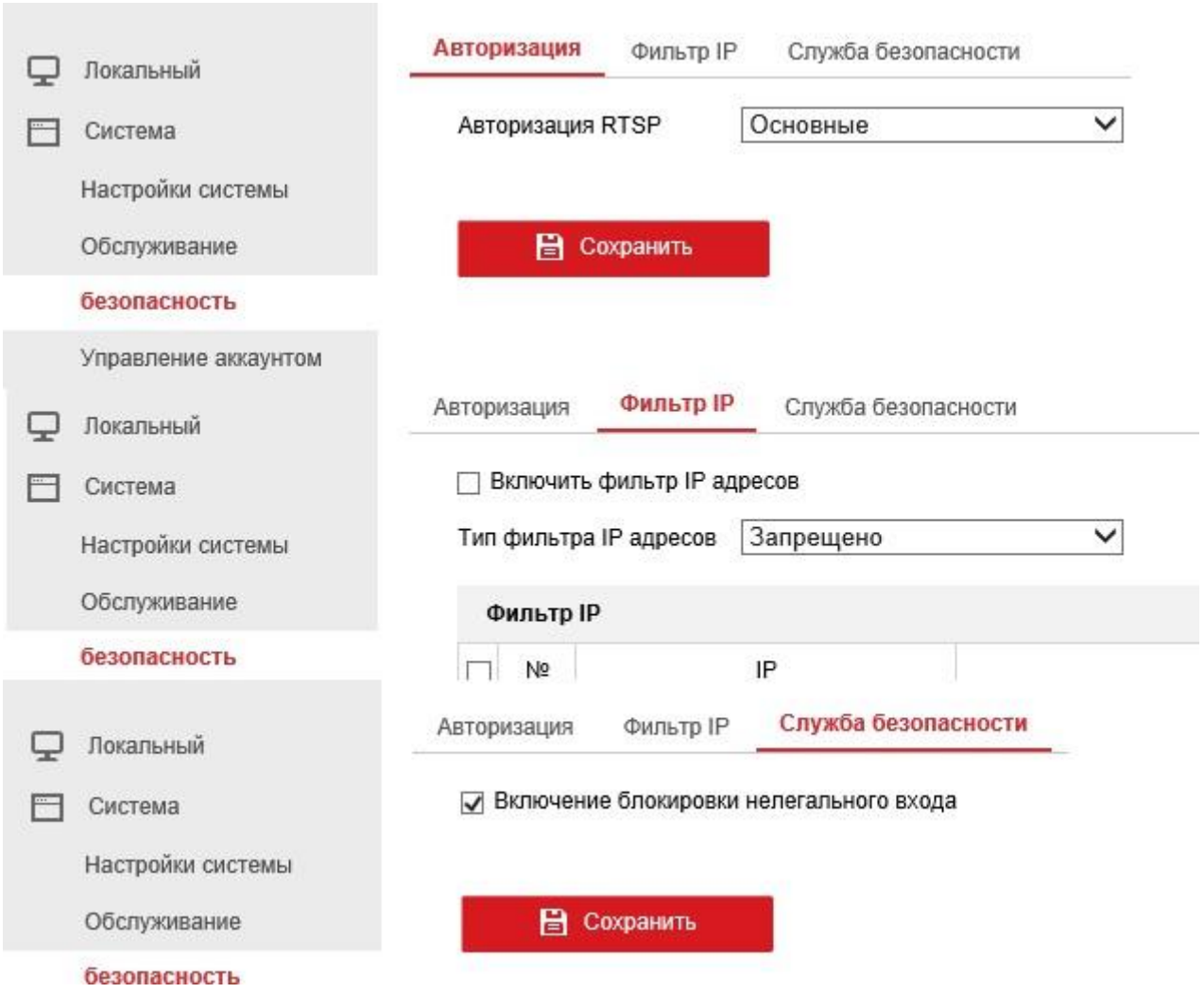


Рисунок 3.28 – Огляд налаштування параметрів безпеки

З рис. 3.28 видно, що пристрій підтримує базові механізми забезпечення контролю доступу, однак фільтрація IP-адрес фактично не застосовується. Окрім стандартних параметрів безпеки, система дозволяє налаштовувати додаткові функції, зокрема платформу віддаленого доступу та використання захищеного протоколу HTTPS, що безпосередньо впливає на загальний рівень захищеності передавання даних.

Платформа доступу реалізується через хмарний сервіс Hik-Connect, який надається компанією Hikvision на безоплатній основі. Даний сервіс дозволяє здійснювати віддалений перегляд відеопотоку з IP-камер у режимі реального часу, а також отримувати доступ до відеоархіву, що зберігається на відеореєстраторі. При цьому збереження відеоданих безпосередньо у хмарному середовищі не передбачене, що зменшує ризики витоку інформації, але водночас покладає відповідальність за захист архівів на локальну інфраструктуру користувача.

.

Компанія Hikvision, як і значна частина виробників з Китаю, здобула популярність не лише завдяки доступній вартості продукції, але й через системні проблеми у сфері кібербезпеки. Упродовж тривалого часу в продуктах та сервісах Hikvision неодноразово виявлялися різноманітні вразливості. Унаслідок цього відбувалися компрометації IP-камер, відеореєстраторів та програмного забезпечення, а також фіксувалися критичні уразливості хмарної інфраструктури компанії, зокрема у сервісах hiDDNS та hik-online. Хмарний сервіс Hik-Connect був запроваджений як рішення для усунення недоліків попередніх платформ. У ньому реалізовано механізми шифрування, а доступ до відеопотоку надається виключно користувачу, який володіє унікальним верифікаційним кодом пристрою. Фактично цей код виконує роль ключа шифрування потоку та розміщується на заводському пакуванні камери. Таким чином, концепція Hik-Connect передбачає вищий рівень захисту та конфіденційності. Проте під час впровадження нової хмарної платформи виникли суттєві експлуатаційні проблеми. Користувачі, які переходили зі старих сервісів на Hik-Connect, стикалися з нестабільною роботою системи, затримками з’єднання та періодичними розривами зв’язку. Як тимчасове рішення компанія Hikvision рекомендувала активувати UPnP та здійснювати пряме підключення до IP-камери, що, у свою чергу, істотно знижувало рівень інформаційної безпеки та відкривало додаткові вектори атак.

До речі, пристрої які використовують протокол без автентифікації, такий як UPnP або HTTP (використовується на незашифрованих веб-серверах) можуть мати вразливість пов’язаною з повторним прив'язуванням DNS.

Пристрої, які використовують протоколи без автентифікації, зокрема UPnP або HTTP (на незашифрованих веб-серверах), можуть бути вразливими до атак типу DNS rebinding. Дана техніка дозволяє віддаленому зловмиснику обходити мережевий брандмауер жертви та використовувати веб-браузер як проксі для безпосередньої взаємодії з пристроями у внутрішній мережі [3].

У разі успішної атаки DNS rebinding зловмисник отримує можливість сканувати локальний сегмент мережі на наявність IoT-пристроїв та здійснювати подальші цілеспрямовані атаки. Значна частина таких пристроїв має стандартні або слабкі паролі, а інколи взагалі не потребує автентифікації, оскільки розрахована на роботу лише в ізольованій мережі. У найбільш небезпечному сценарії зловмисник може повністю скомпрометувати один із пристроїв, встановити прихований канал доступу (наприклад, зворотну оболонку) та використати його як точку опори для атак на інші вузли в межах захищеного мережевого сегмента.

В ідеальному для зловмисника сценарії достатньо повністю скомпрометувати один IoT-пристрій і створити прихований канал доступу, наприклад зворотну

оболонку, до власного сервера керування. Надалі такий пристрій може використовуватися як точка опори для подальших атак на інші вузли в межах захищеного сегмента мережі.

Ефективним способом зменшення ризиків атак повторного прив’язування DNS є перевірка заголовка Host на всіх доступних веб-сервісах. Додатково доцільно застосовувати базові заходи кіберзахисту, зокрема сегментацію мережі та розмежування доступу. IoT-пристрої не повинні розміщуватися в одному мережевому сегменті з користувацькими робочими станціями, а доступ до їхніх інтерфейсів керування має бути обмежений. Відключення невикористовуваних служб зменшує поверхню атаки, а зміна стандартних облікових записів, паролів і портів суттєво ускладнює експлуатацію можливих вразливостей. Використання протоколу HTTPS із підтримкою SSL/TLS також сприяє пом’якшенню атак DNS rebinding не лише за рахунок шифрування, а й завдяки перевірці дійсності сертифіката, що унеможливлює підміну ресурсу. Окрему увагу необхідно приділяти регулярному оновленню програмного забезпечення.

З огляду на вищезазначене, використання хмарних сервісів для систем відеоспостереження потребує обережності, оскільки такі сервіси можуть виступати додатковим каналом витоку інформації та передбачають передачу частини контролю над системою сторонньому постачальнику.

Огляд налаштування платформи доступу Hik-connect та протоколу HTTPS наведені на рис. 3.29.

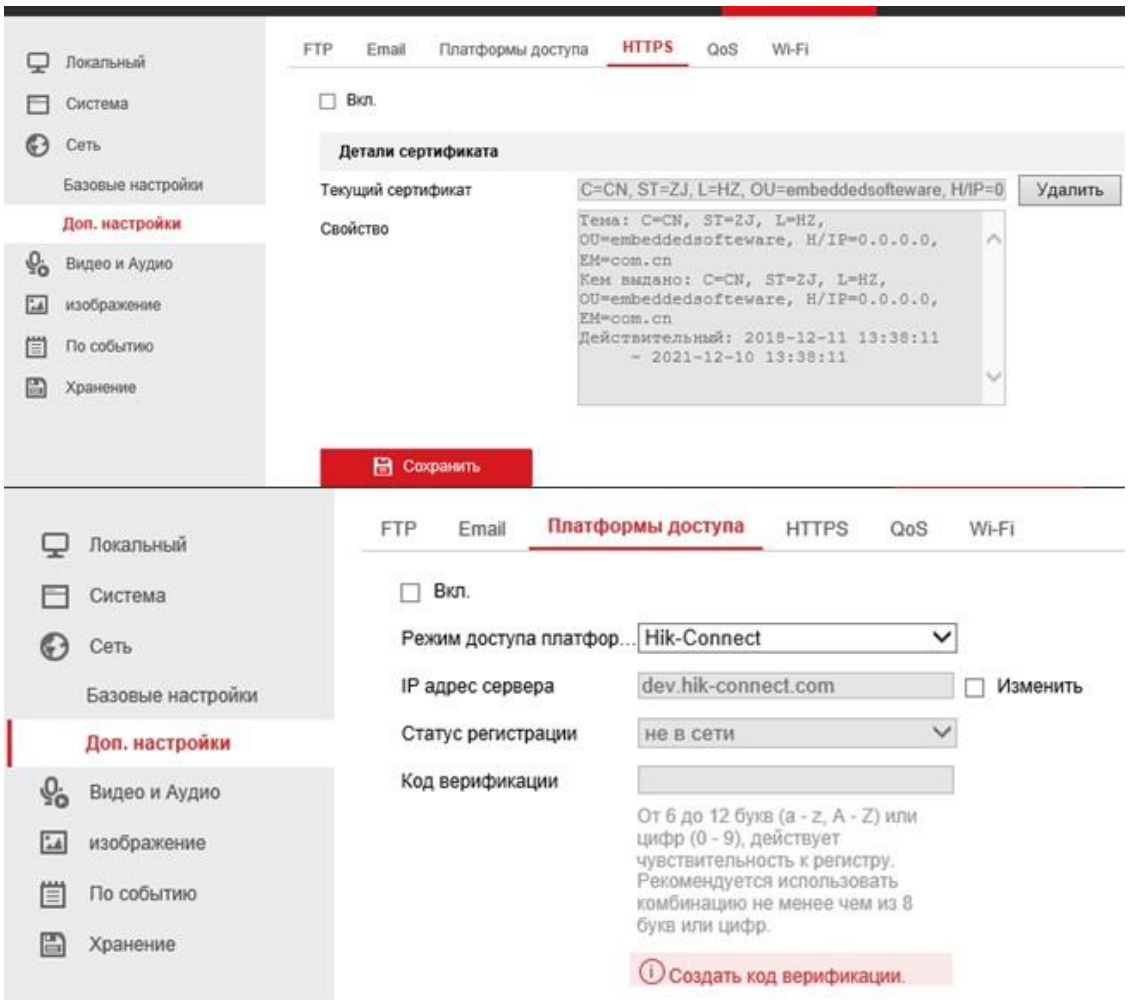


Рисунок 3.29 – Огляд налаштування платформи доступу Hik-connect та протоколу HTTPS

З рис. 3.29 видно, що хмарна платформа доступу Hik-Connect та захищений протокол HTTPS у даній конфігурації не задіяні. Станом на сьогодні безкоштовних рішень, які б одночасно забезпечували аналогічний функціонал і рівень зручності, як Hik-Connect, практично не існує. Водночас існує значна кількість альтернативних технічних підходів для організації віддаленого доступу до IP-камер, зокрема із застосуванням VPN-з’єднань, пробросу портів або спеціалізованих серверних рішень.

Найбільш доцільним рішенням для організації віддаленого доступу є використання Virtual Private Network (VPN). Його перевага полягає не у вартості, а в тому, що застосування VPN забезпечує один із найвищих рівнів захисту передаваних даних і доступу до мережевих ресурсів.

Virtual Private Network (VPN) не замінює підключення до Інтернету, а функціонує поверх нього. Перед передачею дані шифруються на стороні користувача, після чого передаються провайдеру та спрямовуються на VPN-сервер. На сервері трафік розшифровується й надсилається кінцевому отримувачу. Такий підхід значно підвищує рівень конфіденційності та захисту даних. На сьогодні існує декілька VPN-протоколів, однак найбільш рекомендованим з точки зору безпеки та надійності є OpenVPN.

Існує поширене уявлення, що після виявлення вразливості достатньо випустити нову версію прошивки, і проблема буде вирішена. Проте на практиці це не так. По-перше, оновлення програмного забезпечення для більшості IoT-пристроїв не відбувається автоматично. Користувач повинен самостійно дізнатися про наявність вразливості, дочекатися виходу нової прошивки, що інколи триває місяцями, знайти відповідний файл та виконати оновлення вручну. Упродовж цього часу пристрій залишається уразливим і фактично небезпечним для використання. По-друге, більшість пересічних користувачів не відстежують новини у сфері інформаційної безпеки та не реагують на загрози доти, доки вони безпосередньо не торкнуться їх особисто. Відсутність механізмів автоматичного оновлення суттєво знижує рівень захищеності IoT-пристроїв і робить їх легкою ціллю для зловмисників. Таким чином, проблема вразливостей є значно глибшою та серйознішою, ніж може здаватися на перший погляд.

Пристрої IoT часто не оновлюються протягом тривалого часу, інколи роками. Це створює сприятливі умови для зловмисників, які можуть експлуатувати відомі вразливості у власних цілях — від несанкціонованого спостереження за користувачами до формування масштабних ботнет-мереж. У зв’язку з цим особливої актуальності набуває питання відповідальності виробників за безпеку власних продуктів та впровадження надійних механізмів захисту від модифікації й підміни програмного забезпечення.

Для оцінювання рівня ризику необхідно визначити, чи доступні HTTP/HTTPS-сервіси пристрою (зазвичай порти 80/443) безпосередньо з глобальної мережі Інтернет (WAN). У такому випадку пристрій може бути атакований віддалено, що значно підвищує рівень загрози.

Натомість пристрої, розміщені виключно у локальній мережі (LAN) без прямого доступу до Інтернету, мають суттєво нижчий рівень ризику. Для експлуатації вразливостей у цьому випадку зловмиснику необхідно спочатку отримати доступ до внутрішньої мережі, що значно ускладнює реалізацію атаки.

Мережа WAN, у якій HTTP/HTTPS-сервер пристрою захищений брандмауером і недоступний з глобальної мережі, характеризується низьким рівнем ризику, оскільки потенційний зловмисник не має можливості ініціювати з'єднання з пристроєм з Інтернету. За таких умов система все ще вважається такою, що має мінімальну ймовірність успішної атаки.

Використання VPN-мережі для доступу до пристроїв також відноситься до низького рівня ризику. VPN забезпечує доступ лише для автентифікованих та перевірених користувачів, дозволяючи їм підключатися до пристроїв з внутрішньої мережі об'єкта. Такий підхід значно ускладнює проведення атак і вважається одним із найбезпечніших способів віддаленого доступу.

Застосування переадресації портів без додаткових механізмів захисту несе високий рівень ризику. Переадресація портів є простим і економічно доступним способом забезпечення віддаленого доступу, однак вона створює суттєві загрози безпеці. У такій конфігурації брандмауер дозволяє вхідний трафік з Інтернету до конкретного пристрою через визначені порти. За наявності поточної вразливості, поки зловмисник має можливість звертатися до HTTP/HTTPS-портів через механізм переадресації, пристрій перебуває під серйозною загрозою компрометації.

Використання Dynamic Domain Name System (DDNS) також відповідає високому рівню ризику. DDNS є сервісом, що дозволяє отримувати доступ до ресурсів локальної мережі навіть за умови постійної зміни зовнішньої IP-адреси. Найчастіше такими ресурсами виступають веб-сервери або IP-камери для дистанційного керування. Інтернет-провайдери зазвичай динамічно змінюють IP-адреси своїх клієнтів, що унеможливлює прямий доступ із зовнішньої мережі. Клієнтське програмне забезпечення DDNS фіксує зміну IP-адреси та передає оновлені дані провайдеру DDNS. Оскільки DDNS зазвичай функціонує у поєднанні з переадресацією портів, це відкриває пристрій для доступу з Інтернету та, відповідно, піддає його високому ризику атак.

Пряме підключення пристрою до глобальної мережі Інтернет також має високий рівень ризику. У деяких випадках пристрої встановлюються безпосередньо в мережі WAN. Якщо пристрій має публічну IP-адресу, а його HTTP/HTTPS-порти відкриті для зовнішнього доступу, він стає вразливим до широкого спектра кібератак.

На поточний момент, коли оновлення програмного забезпечення вже випущені, а інформація про вразливість стала відомою, зловмисники активно здійснюють її пошук та експлуатацію. Якщо спостерігається несанкціонований рух

камери, надходять сповіщення системи безпеки або під час аналізу системних журналів виявляються підозрілі дії, зокрема спроби підбору паролів, за умови що HTTP/HTTPS-служба пристрою доступна з Інтернету, наполегливо рекомендується негайно встановити відповідні виправлення та перейти на більш захищені рішення, такі як VPN, або комбінувати декілька методів захисту.

Отже, найпростішим способом оцінки рівня ризику системи є перевірка можливості доступу до веб-інтерфейсу пристрою без виконання будь-яких додаткових налаштувань мережі. Якщо такий доступ можливий, система повинна розглядатися як така, що перебуває під високим рівнем ризику.

4 АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ТА ОЦІНКА РИЗИКІВ ІНФОРМАЦІНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

4.1 Загальні положення

Метою аналізу інформаційних ризиків є формування обґрунтованої та економічно доцільної системи забезпечення інформаційної безпеки. Такий аналіз дозволяє визначити оптимальне співвідношення між рівнем захисту інформації та витратами на його реалізацію.

Основними завданнями аналізу інформаційних ризиків є проведення комплексної оцінки рівня захищеності інформаційної системи, визначення цінності інформаційних ресурсів та можливих обсягів потенційних збитків у разі їх компрометації, оцінка ймовірності реалізації загроз, а також розробка ефективної системи заходів щодо забезпечення інформаційної безпеки з урахуванням виявлених ризиків.

Проведення аналізу інформаційних ризиків є необхідним для визначення можливих наслідків втрати, порушення цілісності або доступності цінної інформації, порівняння рівня ризику з витратами на впровадження засобів захисту, а також для оцінювання доцільності та ефективності вкладень у систему інформаційної безпеки.

Для оцінювання рівня захищеності інформаційних систем можуть застосовуватися як кількісні, так і якісні методи аналізу. Вибір конкретного методу залежить від складності системи, наявності вихідних даних та цілей дослідження.

Критерії проведення аудиту інформаційної безпеки формуються на основі міжнародних стандартів, загальноприйнятих методик, внутрішніх стандартів аудиторських організацій, а також чинних національних і галузевих нормативних документів.

Якісний аналіз ризиків являє собою процес визначення пріоритетності ризиків для подальшого детального аналізу або прийняття управлінських рішень шляхом оцінювання ймовірності їх виникнення та можливого впливу. Такий аналіз зазвичай здійснюється з використанням описових характеристик або умовних шкал оцінювання, наприклад у вигляді балів або рівнів.

4.2 Аналіз ефективності методів захисту методом матриці ймовірності та наслідків

Одним із ключових інструментів оцінювання інформаційних ризиків, їх рівня та впливу на інформаційну систему є матриця ймовірності та наслідків. Даний підхід широко застосовується в управлінні ризиками для візуалізації загроз і визначення пріоритетності заходів реагування.

Матриця ймовірності та наслідків являє собою аналітичну методику, що дозволяє визначити рівень ризику окремо для кожної цілі процесу або проєкту, зокрема з урахуванням функціональності, часових обмежень, фінансових або інших ресурсів. Визначений ранг ризику дає змогу оперативно приймати управлінські рішення щодо реагування на загрози, залежно від їх розташування у відповідній зоні матриці. Кожна зона матриці фактично виконує роль індикатора пріоритетності ризиків.

Зазвичай цей метод використовується на етапі попереднього аналізу, особливо у випадках, коли ідентифіковано декілька різних ризиків. З його допомогою забезпечується можливість визначити, які ризики потребують детальнішого подальшого аналізу, а також які з них необхідно опрацьовувати в першу чергу з огляду на потенційні наслідки.

Для проведення оцінки ризику кожного потенційного інциденту визначається поєднання двох основних параметрів — ймовірності виникнення загрози та рівня її впливу. На основі цієї комбінації кожному ризику присвоюється певний ранг: дуже низький, низький, середній, високий або дуже високий. Така класифікація дозволяє систематизувати ризики та забезпечити структурований підхід до планування заходів інформаційної безпеки.

На рис. 4.1 наведено приклад визначення рівнів ризику.

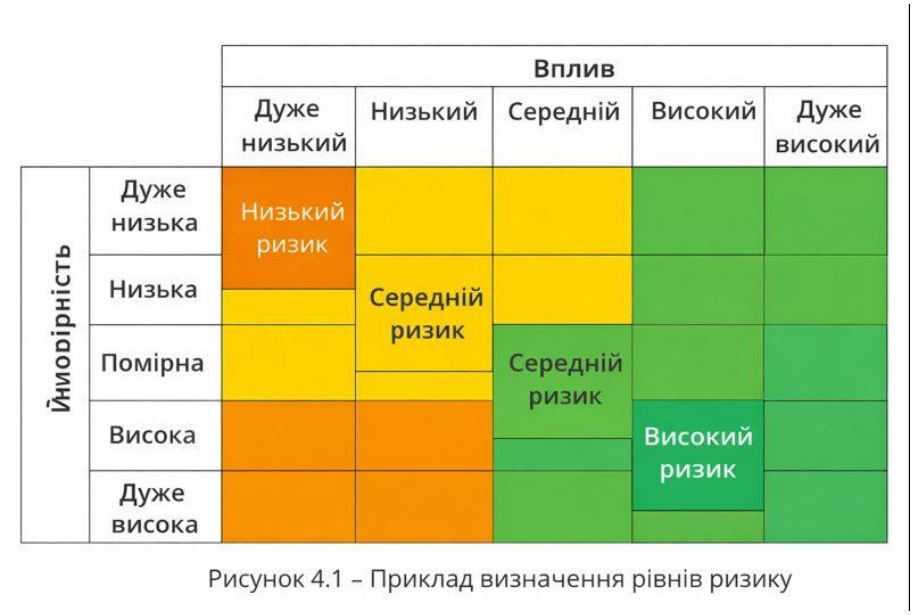


Рисунок 4.1 – Приклад визначення рівнів ризику

Для визначення ймовірності реалізації кожного ризику та оцінки можливих наслідків з метою правильного розміщення ризику в матриці необхідно застосовувати експертний підхід. Значення ймовірності виникнення ризиків і рівень їх впливу були встановлені на основі методів експертних оцінок.

У таблиці 4.1 наведено приклад якісної оцінки окремих потенційних ризиків інформаційної безпеки в мережах Інтернету речей.

Таблиця 4.1 – Якісна оцінка можливих ризиків інформаційної безпеки IoT

Ризик	Ймовірність	Вплив	Результуючий ризик
1	2	3	4
Отримання несанкціонованого доступу через слабкі паролі, паролі, які можна вгадати або жорстко закодовані	Дуже висока	Дуже високий	Високий
Отримання несанкціонованого доступу через мережеві сервіси	Висока	Дуже високий	Високий
Отримання несанкціонованого доступу через інтерфейси	Висока	Дуже високий	Високий
Отримання несанкціонованого доступу через неоновлене програмне забезпечення	Висока	Дуже високий	Високий
Зараження шкідливим програмним забезпечення при оновлені	Низька	Високий	Середній
Перехоплення облікових даних через прослуховування незахищеного каналу зв’язку	Низька	Високий	Середній

Як можливо побачити з таблиці 4.1, проведено якісну оцінку декількох ризиків пов’язаних з IoT-пристроями. Отже, можливо визначити перелік пріоритетних ризиків, а саме звернути увагу, де ймовірність наслідків висока.

До визначених ризиків можливо застосувати методи безпеки, що спрямовані на зменшення ризиків. У таблиці 4.2 наведено якісну оцінку визначених ризиків з урахуванням методів захисту.

Таблиця 4.2 – Якісна оцінка ризиків з урахуванням методів захисту

Ризик	Методи захисту	Кінцевий ризик
1	2	3
Отримання несанкціонованого доступу через слабкі паролі, паролі, які можна вгадати або жорстко закодовані	Встановити довжину, складність та періодичність зміни паролів відповідно до галузевого стандарту NIST SP800-63 B. Для кожного пристрою паролі повинні бути унікальними. Жорстко закодовані паролі повинні бути видаленими.	Низький
Отримання несанкціонованого доступу через мережеві сервіси	Забезпечити доступ лише до необхідних портів з використанням IP, MAC фільтрації портів. Використовувати невразливі сервіси до переповнення буферу. Виконувати налаштування переадресації портів самостійно та повністю відключити підтримку UPnP. Виконати перевірку сервісів інструментами автоматичного тестування для виявлення вразливостей з їх подальшим усуненням.	Низький
Отримання несанкціонованого доступу через інтерфейси	Використовувати двофакторну автентифікацію за можливістю. Логіни та паролі користувачів за замовчуванням необхідно змінити. Забезпечення надійності механізмів відновлення пароля та недопущення надання зловмиснику інформації, що вказує на чинний обліковий запис. Ввімкнути та налаштувати поріг блокування облікового запису.	Низький

Продовження таблиці 4.2

1	2	3
Отримання несанкціонованого доступу через неоновлене програмне забезпечення	Забезпечити регулярне оновлення. Ввімкнути функцію автоматичного оновлення за можливістю або підписатися на повідомлення про оновлення ПЗ на веб-сайті постачальника пристрою. Виконати перевірку на наявність вразливості ПЗ інструментами автоматичного тестування.	Низький
Перехоплення облікових даних через прослуховування незахищеного каналу зв’язку	Забезпечити шифрування даних за допомогою протоколів SSL та TLS. Забезпечити використання інших стандартних галузевих методів шифрування для захисту даних під час транспортування, якщо SSL або TLS недоступні. Не використовувати власних протоколів шифрування. Перевірити сервер оновлень, щоб переконатися, що методи транспортного шифрування оновлені та правильно налаштовані, а сервер не вразливий.	Низький
Зараження шкідливим програмним забезпечення при оновлені	Використовувати загальноприйняті методи шифрування для файлу оновлення ПЗ. Використовувати зашифроване з'єднання під час передачі файлу оновлення ПЗ. Перевірити, чи оновлення ПЗ підписано та перевірено, перш ніж дозволяти завантаження та застосування оновлення. Перевірити сервер оновлень, щоб переконатися, що методи транспортного шифрування оновлені та правильно налаштовані, а сервер не вразливий.	Низький

Як можна побачити з таблиці 4.2, кінцевий рівень ризику істотно знизився за умови впровадження запропонованих методів захисту. Визначений перелік пріоритетних ризиків було піддано кількісній оцінці з урахуванням застосованих заходів забезпечення інформаційної безпеки.

Запропоновані методи захисту є базовими, однак навіть їх використання демонструє суттєвий позитивний вплив на зменшення рівня ризиків. Таким чином, відносно невеликий набір вимог і заходів уже здатний помітно підвищити загальний рівень безпеки пристроїв Інтернету речей. Запропоновані основні вимоги інформаційної безпеки можна вважати реалістичним та практичним першим кроком на шляху до значного підвищення рівня захищеності споживчих IoT-систем.

4.3 Аналіз ефективності методів захисту методом Return of Security Investment

Return of Security Investment (ROSI) – це показник рентабельності інвестицій у сферу інформаційної безпеки, який відображає ефективність використання фінансових ресурсів, вкладених у захисні заходи. ROSI дає змогу оцінити, яку економічну вигоду приносить кожна грошова одиниця, інвестована в безпеку. Фактично, рентабельність інвестицій у безпеку дозволяє визначити доцільність впровадження конкретних засобів захисту з фінансової точки зору. Захід інформаційної безпеки вважається економічно обґрунтованим лише за умови, що рівень зниження ризику перевищує витрати на його реалізацію.

Основним недоліком розрахунку ROSI є складність досягнення високої точності оцінки, оскільки відсутній універсальний підхід до визначення реальної вартості та частоти інцидентів кібербезпеки. Показники таких інцидентів можуть суттєво відрізнятися залежно від середовища, типу організації та рівня зрілості системи захисту.

Попри це, ROSI залишається корисним аналітичним інструментом для обґрунтування інвестицій у безпеку. Його застосування базується на порівнянні фінансової вигоди від запобігання інцидентам інформаційної безпеки із сумарними витратами на впровадження захисних механізмів. Таким чином, показник ROSI дозволяє оцінити чистий економічний ефект від реалізації заходів інформаційної безпеки.

Інститут SANS пропонує підхід до кількісного аналізу ризиків для розрахунку показника ROSI, який отримав широке застосування на практиці. На відміну від класичних формул розрахунку рентабельності інвестицій, цей підхід ґрунтується на оцінюванні конкретних загроз інформаційної безпеки, з якими

пов’язані відповідні інвестиції. Ключовим елементом розрахунку є показник очікуваних річних втрат (Annualized Loss Expectancy, ALE), що використовується для прогнозування можливих фінансових збитків певного активу внаслідок реалізації конкретного ризику протягом одного календарного року.

Застосування ALE дозволяє більш обґрунтовано оцінити економічну доцільність впровадження заходів захисту, оскільки воно враховує як імовірність виникнення інциденту, так і масштаб потенційних втрат. У зв’язку з цим важливо чітко визначити рівень схильності організації до ризиків інформаційної безпеки, а також об’єктивно оцінити вартість кожного критично важливого активу, на захист якого спрямовуються інвестиції в систему безпеки.

Розрахунок оцінки ROSI запропонованої інститутом SANS визначається за формулою [13]:

$$\mathrm{ROSI} = \frac{\mathrm{ALE} \cdot \mathrm{Mitigation\ Ratio} - \mathrm{Cost\ of\ Solution}}{\mathrm{Cost\ of\ Solution}}, \tag{4.1}$$

де ALE – це загальний річний грошовий збиток за рік, очікуваний у результаті певного фактора ризику, якщо інвестиції в цінні папери не будуть зроблені;

Mitigation Ratio – коефіцієнт зниження, відсоток ризиків, які можна усунути за допомогою інвестицій у безпеку;

Cost of Solution – вартість рішень виділених на зниження ризику.

Щоб розрахувати ALE, потрібно помножити очікування одиничного збитку (Single loss expectancy, SLE) на річну частоту виникнення (Annualized rate of occurrence, ARO) [13]:

$$\mathrm{ALE} = \mathrm{SLE} \cdot \mathrm{ARO}, \tag{4.2}$$

де SLE – це сума грошей, яка буде втрачена внаслідок одного інциденту, пов'язаного з безпекою;

ARO – це передбачувана частота або очікувана можливість виникнення загрози протягом року.

Потрібно оцінити ALE та коефіцієнт пом'якшення для невеликих підприємств, що мають вразливості пов’язані з ризиками через неоновлене ПЗ. Наприклад пов’язаними з CVE-2021-33044 або CVE-2021-36260 та використати їх для розрахунку ROSI для пропонованих інвестицій у безпеку.

Прогнозується, що за відсутності впроваджених заходів інформаційної безпеки на підприємстві в середньому може виникати п’ять інцидентів протягом року (ARO = 5). При цьому слід враховувати, що такі числові оцінки мають орієнтовний характер, оскільки точне визначення частоти інцидентів є складним через залежність від специфіки організації, рівня її захищеності та активності зловмисників.

Тому кожен інцидент може призвести до злому, який коштуватиме приблизно вісім тисяч доларів США у вигляді втрати даних, штрафів, втрати продуктивності або навіть втрати бізнесу (SLE = 8 000).

Таким чином, можливо підрахувати ALE за формулою (4.2):

$$\mathrm{ALE} = 8000 \cdot 5 = 40000.$$

Очікується, що запропоновані рішення виявлення даних знизять цей ризик на 90% (коефіцієнт зниження = 90%). Рішенням безпеки пов’язаними з неоновленим ПЗ, що потребує грошових витрат є використання сканеру вразливості. Орієнтовна вартість купівлі та управління рішенням становить тисячу доларів США.

Таким чином, можливо розрахувати ROSI, використовуючи формулу (4.1):

$$\mathrm{ROSI} = \frac{40000 \cdot 0.9 - 1000}{1000} = 35 \cdot 100 = 3500\%.$$

Використовуючи розрахунок ROSI, можливо стверджувати, що ці інвестиції заощадять компанії близько тридцяти п’яти тисяч доларів за окупності 3500%, тобто у тридцять п’ять раз. Ці результати здаються досить високими для звичайної рентабельності інвестицій, однак це переважно стосується інвестицій у безпеку, коли потрібна лише одна скоординована атака, щоб вартість активу різко знизилася. Оцінка суми грошей, заощаджених від втрат, які можуть бути ніколи не трапляється – це важке завдання, яке в реальному світі вимагає більш ніж простого застосування простих формул.

Таким чином, витрати на безпеку виправдані з точки зору сприяння бізнесу. Проблема безпеки полягає в тому, що діяльність, обумовлена витратами, безпосередньо впливає на прибутковість організації.

ВИСНОВКИ

У кваліфікаційній роботі «Аналіз безпеки протоколів зв’язку для інтернету речей IoT» поставлені завдання виконано в повному обсязі.

У межах роботи розглянуто та вирішено задачу розроблення і обґрунтування методів забезпечення інформаційної безпеки в мережах Інтернету речей. Поставлену мету досягнуто шляхом зниження рівня ризиків за рахунок застосування найбільш результативних методів захисту інформації. Ефективність запропонованих рішень підтверджена результатами якісної та кількісної оцінки ризиків.

Проведено детальний аналіз загроз і проблем інформаційної безпеки в IoT-середовищі. Визначено актуальні та найбільш небезпечні загрози для IoT-пристроїв у мережах, а також сформульовано базові рекомендації щодо їх нейтралізації. З огляду на мережеву природу IoT-пристроїв, що суттєво підвищує поверхню атак і знижує загальний рівень захищеності системи, обґрунтовано доцільність застосування методів активного та пасивного сканування.

Для оцінювання стану інформаційної безпеки рекомендовано використання інструментів аналізу мереж, зокрема Nmap, який дозволяє здійснювати аудит безпеки та ідентифікацію сервісів, а також альтернативного засобу Router Scan, що орієнтований на пошук вразливостей у мережевих пристроях. Окрему увагу приділено пошуковій системі Інтернету речей Shodan, основною перевагою якої є наявність уже сформованої глобальної бази IoT-пристроїв з детальними відомостями про хости, включно з IP-адресами, відкритими портами, сервісами, алгоритмами шифрування та відомими уразливостями. Як типового представника IoT-середовища для дослідження обрано IP-камери, що є одними з наймасовіших IoT-пристроїв.

Дослідження інформаційної безпеки IoT-пристроїв базувалося на аналізі загальновідомих уразливостей. У ході експериментальної частини роботи підтверджено актуальність розглянутих методів забезпечення інформаційної безпеки в IoT-мережах. Показано, що більшість виявлених загроз є реальними та можуть бути успішно реалізовані на практиці. Встановлено, що ключовими проблемами безпеки IoT-пристроїв залишаються використання слабких або стандартних паролів, наявність жорстко закодованих облікових даних, вразливі мережеві сервіси й інтерфейси, а також експлуатація застарілого програмного забезпечення.

Доведено, що окремі загальновідомі уразливості становлять критичний рівень загрози для інформаційної безпеки IoT-пристроїв з таких причин:

1) відносно недавня публікація уразливостей свідчить про масову відсутність актуальних оновлень програмного забезпечення на мільйонах пристроїв;

2) значна частина користувачів ігнорує базові вимоги та рекомендації з інформаційної безпеки;

3) експлуатація уразливостей призводить до порушення всіх основних властивостей інформації — конфіденційності, цілісності та доступності;

Для ефективного та безпечного впровадження IoT-пристроїв у промислових умовах необхідно заздалегідь враховувати галузеву специфіку, а також вимоги до вартості, рівня безпеки, конфіденційності та допустимого рівня ризиків ще на етапі проєктування та розгортання систем Інтернету речей.

З цією метою в роботі проведено аналіз і оцінку ризиків інформаційної безпеки IoT-систем. Для оцінювання рівня захищеності застосовано поєднання якісних і кількісних методів. Якісний аналіз ризиків із використанням матриці ймовірності та наслідків дозволив сформувати перелік пріоритетних загроз. Надалі ці ризики були піддані кількісній оцінці з використанням показника ROSI з урахуванням запропонованих заходів захисту. У результаті доведено економічну доцільність впровадження методів інформаційної безпеки, оскільки вкладені інвестиції окупилися більш ніж у тридцять п’ять разів.

Запропонований комплекс базових заходів захисту є реалістичним та практичним початковим кроком на шляху до суттєвого підвищення рівня безпеки споживчих і корпоративних IoT-систем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мазепа А. Д. Безпечна автентифікація до веб-додатку з використанням JWT та browser fingerprinting / А. Д. Мазепа, А. С. Тарасов. // Харків, ХНУРЕ, Матеріали XXII Міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті". Том 4. – 2021. – С. 60–61.

2. Тарасов А. С. Проблеми захисту персональних даних в комп'ютерних системах від шкідливого програмного забезпечення stealer / А. С. Тарасов, А. Д. Мазепа. // Харків, ХНУРЕ, Матеріали XXII Міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті". Том 4. – 2021. – С. 64–65.

3. Мазепа А. Д. Розуміння та захист від атаки DNS rebinding / А. Д. Мазепа, А. С. Тарасов. // Харків, ХНУРЕ, Матеріали XXII Міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті". Том 4. – 2021. – С. 62–63.

4. The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID [Електронний ресурс] – Режим доступу до ресурсу: https://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf.

5. Наукове дослідження Інтернету речей Hewlett Packard Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://json.tv/tech_trend_find/nauchnoe-issledovanie-interneta-veschey-ot-hewlett-packard-enterprise-20160503115845.

6. Xiang Y. Low-rate DDoS attacks detection and traceback by using new information metrics / Y. Xiang, K. Li, W. Zhou. // IEEE Transactions on Information Forensics and Security. – 2011. – С. 426–437.

7. Що таке Шодан? [Електронний ресурс] – Режим доступу до ресурсу: https://help.shodan.io/the-basics/what-is-shodan.

8. Shodan: The scariest search engine on the Internet [Електронний ресурс] – Режим доступу до ресурсу: https://money.cnn.com/2013/04/08/technology/security/shodan/index.html.

9. Dahua IP Camera 3.200.0001.6 access control [Електронний ресурс] – Режим доступу до ресурсу: https://vuldb.com/?id.99110.

10. John the Ripper [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/John_the_Ripper.

11. Vulnerability Details CVE-2021-33045 [Електронний ресурс] – Режим доступу до ресурсу: https://www.cvedetails.com/cve/CVE-2021-33045/.

12. Vulnerability Details CVE-2021-36260 [Електронний ресурс] – Режим доступу до ресурсу: https://www.cvedetails.com/cve/CVE-2021-36260/.

13. Quantitative Risk Analysis Step-By-Step [Електронний ресурс] – Режим доступу до ресурсу: https://sansorg.egnyte.com/dl/arTGfdKrUg/.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Магістерська кваліфікаційна робота

Аналіз безпеки протоколів зв'язку для інтернету речей IoT

ВИКОНАВ
студент гр. ТСДМ-61
Дужик Д.Є.

КЕРІВНИК
КДН, Професор
Гетьманець О.В.

Київ — 2026

Актуальність теми

Зростання ризиків в умовах глобалізації IoT

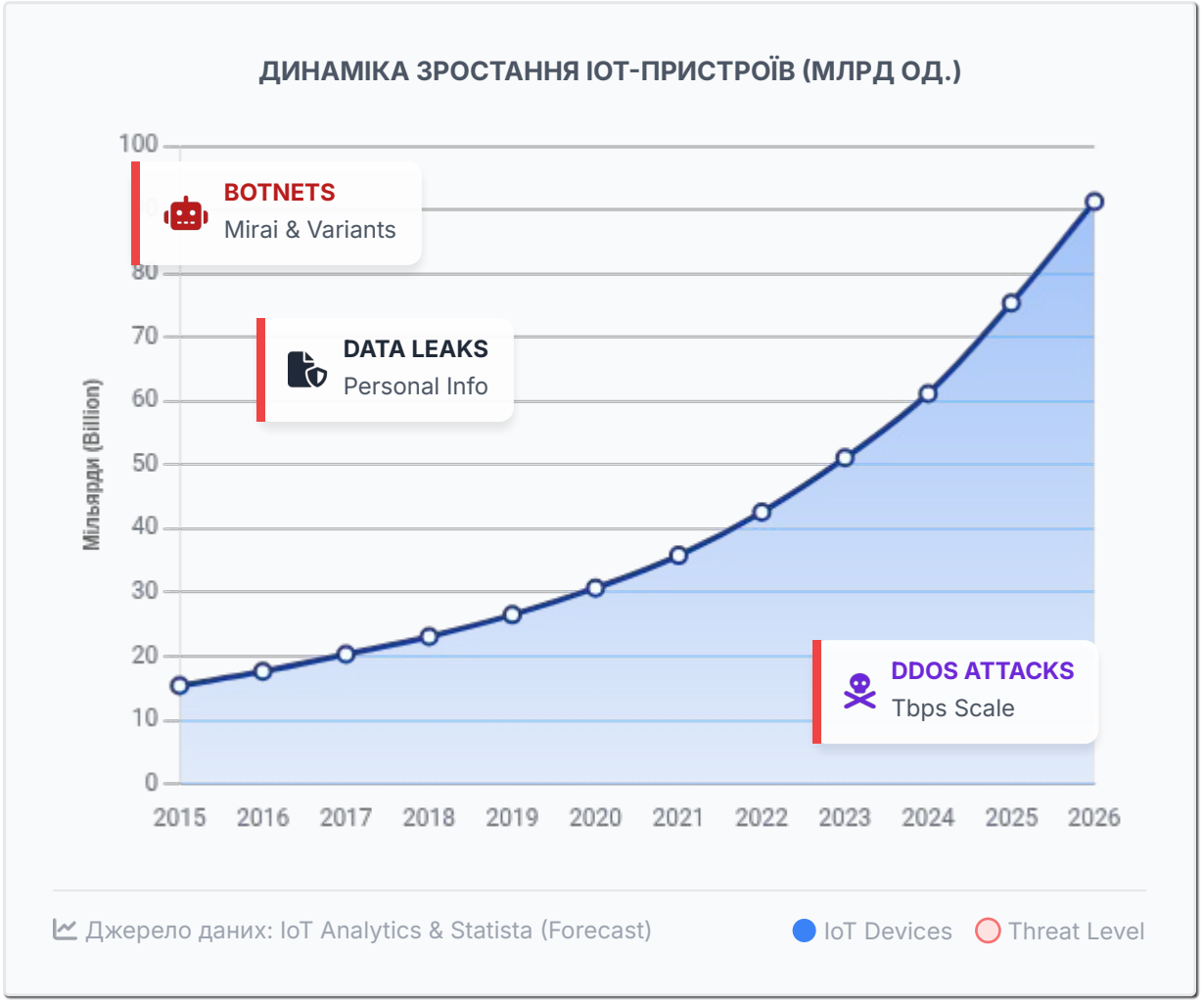
Стрімке зростання кількості підключених IoT-пристроїв.

Масове підключення критичних систем до глобальної мережі.

Критично низький рівень захисту у споживчому сегменті.

Реальні інциденти: ботнети (Mirai), витоки приватних даних, DDoS.

Високі ризики для бізнесу та критичної інфраструктури.



Мета та завдання роботи

Стратегія дослідження безпеки IoT-мереж

Мета роботи

Аналіз методів забезпечення інформаційної безпеки в сучасних IoT-мережах.

Зниження інформаційних ризиків шляхом застосування ефективних методів захисту.

Основні завдання

Аналіз загроз і вразливостей IoT-середовища.

Дослідження реальних CVE (Common Vulnerabilities).

Комплексна оцінка ризиків (якісна та кількісна).

Обґрунтування економічної ефективності методів захисту.

ЕТАПИ ДОСЛІДЖЕННЯ

1 **Загрози та вразливості**
Ідентифікація векторів атак на IoT

2 **Аналіз CVE**
Розбір конкретних кейсів (Hikvision, Dahua)

3 **Оцінка ризиків**
Матриця ризиків, розрахунок ALE та ROSI

4 **Вибір методів захисту**
Сегментація, шифрування, політики паролів

5 **Перевірка ефективності**
Підтвердження зниження ризиків

Основні загрози безпеки IoT

Класифікація векторів атак та вразливостей

Ключові фактори ризику:

Специфіка IoT (обмежені ресурси, завжди онлайн) робить пристрої ідеальною ціллю для автоматизованих атак та створення ботнетів.

Масштабованість атак: мільйони пристроїв використовуються як зброя.

Складність виявлення: компрометація часто непомітна для користувача.

Каскадний ефект: злом одного датчика може відкрити доступ до всієї мережі.



Ботнети & DDoS

Mirai, Gafgyt, масові атаки на відмову



Man-in-the-Middle

Перехоплення та підміна трафіку



Крадіжка даних

Витік конфіденційної інформації



Соціальна інженерія

Фішинг персоналу та користувачів



Ransomware

Шифрування файлів та вимагання викупу



APT Загрози

Цільові, тривалі атаки на інфраструктуру



Слабкі паролі

Brute-force, словникові атаки



Вразливе ПЗ

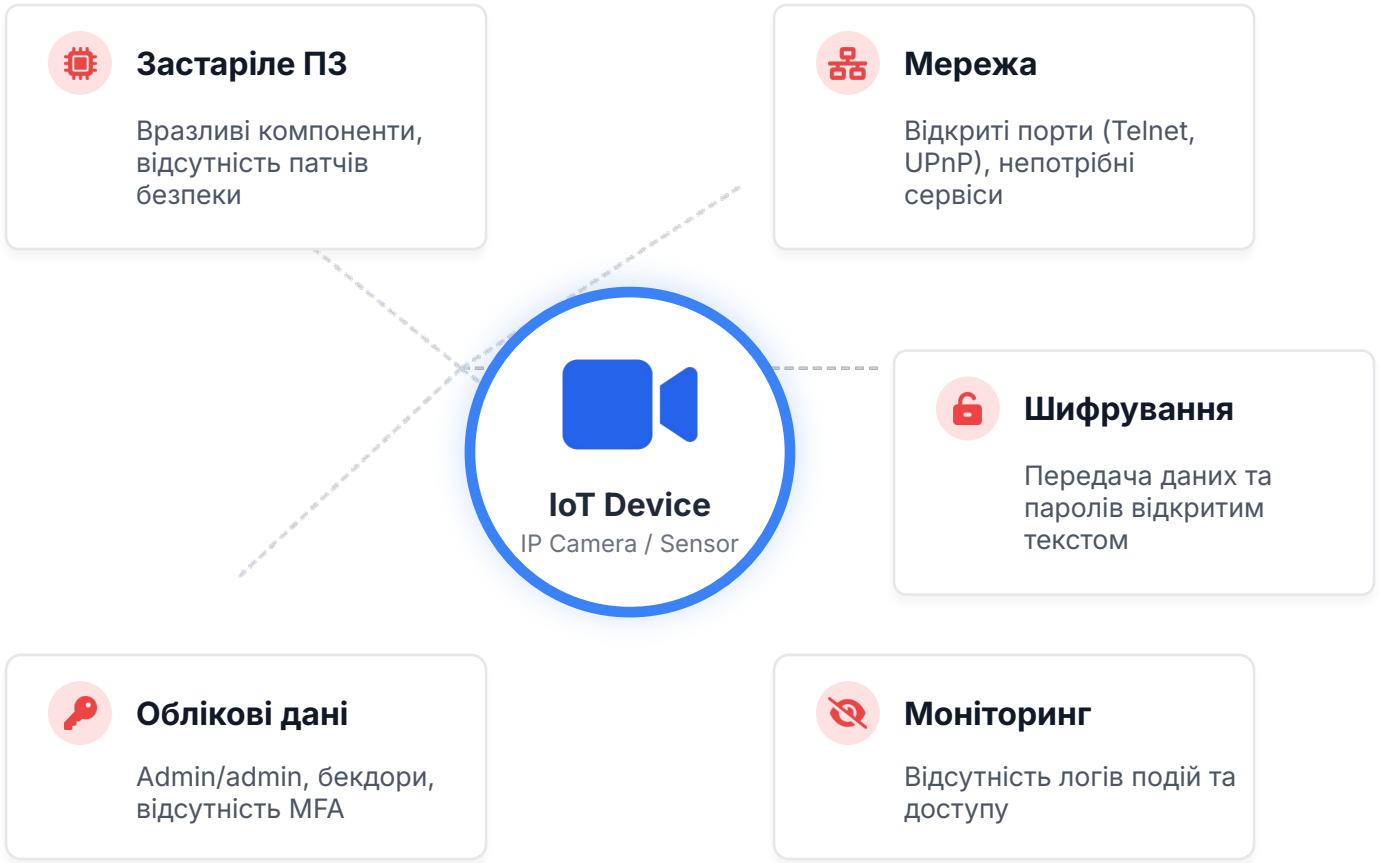
Застарілі прошивки та бібліотеки

Типові проблеми IoT-пристроїв

Аналіз вразливостей архітектури та конфігурації

Основні недоліки

- Відсутність автоматичних оновлень ПЗ
- Жорстко закодовані облікові дані
- Незахищені мережеві сервіси
- Відсутність шифрування трафіку
- Велика поверхня атак
- Відсутність журналювання та моніторингу



Методи виявлення IoT-пристроїв

Інструментарій аудиту безпеки та розвідки

Nmap / Zenmap

Глибоке сканування портів і сервісів.

Виявлення типу ОС та версій ПЗ за допомогою TCP/IP fingerprinting.

Router Scan

Спеціалізований аудит мережевих пристроїв (роутери, камери).

Автоматизований підбір облікових даних (brute-force).

Shodan

Пошук IoT-пристроїв у відкритому Інтернеті (OSINT).

Аналіз банерів сервісів та виявлення відомих вразливостей без прямого контакту.

ПРОЦЕС СКАНУВАННЯ ТА ІДЕНТИФІКАЦІЇ

1

1. Вибір вектору атаки

ЛОКАЛЬНО
Цільова мережа

ГЛОБАЛЬНО
Інтернет

2

2. Застосування інструментів

NMAP R.SCAN
Активне сканування

SHODAN
Пошук по базах

3

3. Результати розвідки

- ✓ Перелік хостів
- ✓ Банери сервісів
- ✓ Відкриті порти
- ✓ Типи пристроїв

4

4. Аналіз вразливостей

Ідентифікація версій → **Зіставлення з CVE**

Пошук відомих експлойтів для знайденого обладнання

Досліджені вразливості (Dahua)

Аналіз механізмів експлуатації критичних помилок безпеки

CVE-2017-7253

Backdoor Access

- Підвищення привілеїв через бекдор
- Отримання конфігураційних даних без авторизації
- Вразливість у DHCP сервісі

CVE-2021-33044 / 33045

Auth Bypass

- Повний обхід механізмів автентифікації
- Доступ до системи з правами адміністратора
- Збереження паролів у відкритому вигляді (cleartext)

СЦЕНАРІЙ АТАКИ (ATTACK FLOW)



1. Розвідка
Сканування портів (37777, 80)

2. Запит
HTTP запит до уразливого API

3. Обхід
Bypass Auth / Витік хешів

4. Привілеї
Підвищення прав до Admin/Root

5. Контроль
Повний доступ до системи

Механізм експлуатації

Атакуючий використовує спеціально сформовані HTTP-запити до інтерфейсів керування камерою, що дозволяє отримати доступ до файлу конфігурації або хешів паролів, минаючи перевірку авторизації.

Досліджені вразливості (Hikvision)

Аналіз критичної вразливості CVE-2021-36260

CVE-2021-36260

Remote Code Execution (Unauthenticated)

Віддалене виконання коду без автентифікації

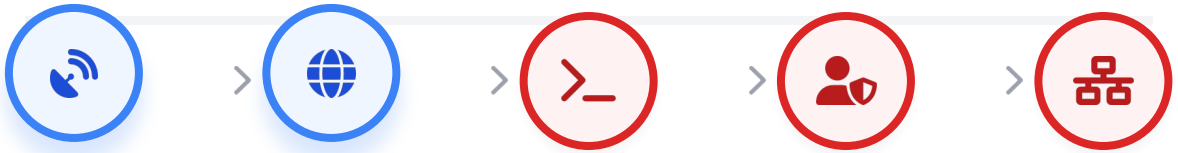
Командна ін'єкція через HTTP PUT запит

Отримання повного root-доступу

Повна компрометація пристрою

Доступ до внутрішніх мереж підприємства

СЦЕНАРІЙ АТАКИ (ATTACK FLOW)



1. Виявлення
Пошук вразливих камер

2. HTTP PUT
Відправка шкідливого запиту

3. Ін'єкція
Виконання OS команд

4. Root
Отримання адмін-прав

5. Мережа
Рух вглиб інфраструктури

Механізм вразливості

Вразливість існує через недостатню валідацію вхідних даних у веб-сервері пристрою. Атакуючий може надіслати спеціально сформований XML-пакет у тілі запиту PUT, що містить системну команду, яка буде виконана операційною системою камери з правами root.

Наслідки експлуатації вразливостей

Вплив на інформаційну безпеку та бізнес-процеси

Ключові загрози

Повне порушення конфіденційності (витік даних).

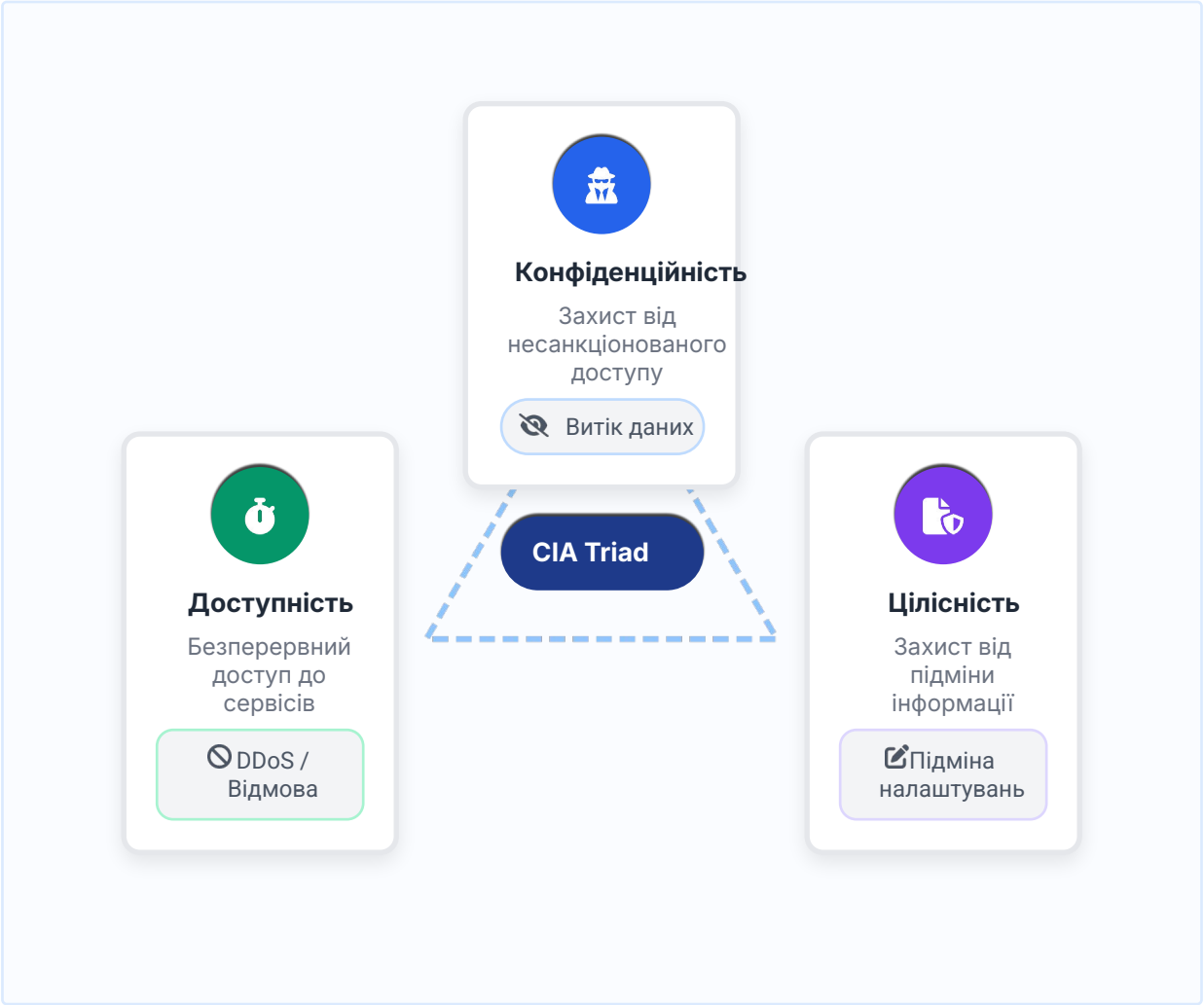
Компрометація цілісності системних файлів.

Повна втрата доступності ресурсів.

Створення масштабних ботнетів.

Крадіжка відеопотоків, аудіо та облікових даних.

Пряма загроза бізнес-процесам та репутації.



Аналіз ризиків

Оцінка ймовірності інцидентів та економічне обґрунтування захисту

Якісний аналіз

Побудова матриці ймовірності та наслідків для класифікації загроз.

Визначення пріоритетних ризиків (критичні вразливості камер та роутерів).

Ранжування загроз за рівнем впливу на бізнес-процеси.

Кількісна оцінка

Застосування методу ROSI (Return on Security Investment).

Розрахунок показника ALE (Annual Loss Expectancy).

Доведення економічної доцільності впровадження систем захисту.

ЙМОВІРНІСТЬ (PROBABILITY)					
	Med	High	High	Crit	Crit
	Med	Med	High	Crit	Crit
	Low	Med	Med	High	Crit
	Low	Low	Med	Med	High
	Low	Low	Low	Med	Med

КЛЮЧОВІ МЕТРИКИ

Очікувані річні втрати: $ALE = SLE \times ARO$

Ефективність інвестицій: $ROSI = (ALE_{old} - ALE_{new} - Cost) / Cost$

Основні рекомендації з безпеки

Комплексний підхід до побудови захищеної архітектури IoT

Унікальні паролі: Відмова від дефолтних облікових даних, MFA.

Мінімізація сервісів: Вимкнення Telnet, UPnP, невикористовуваних портів.

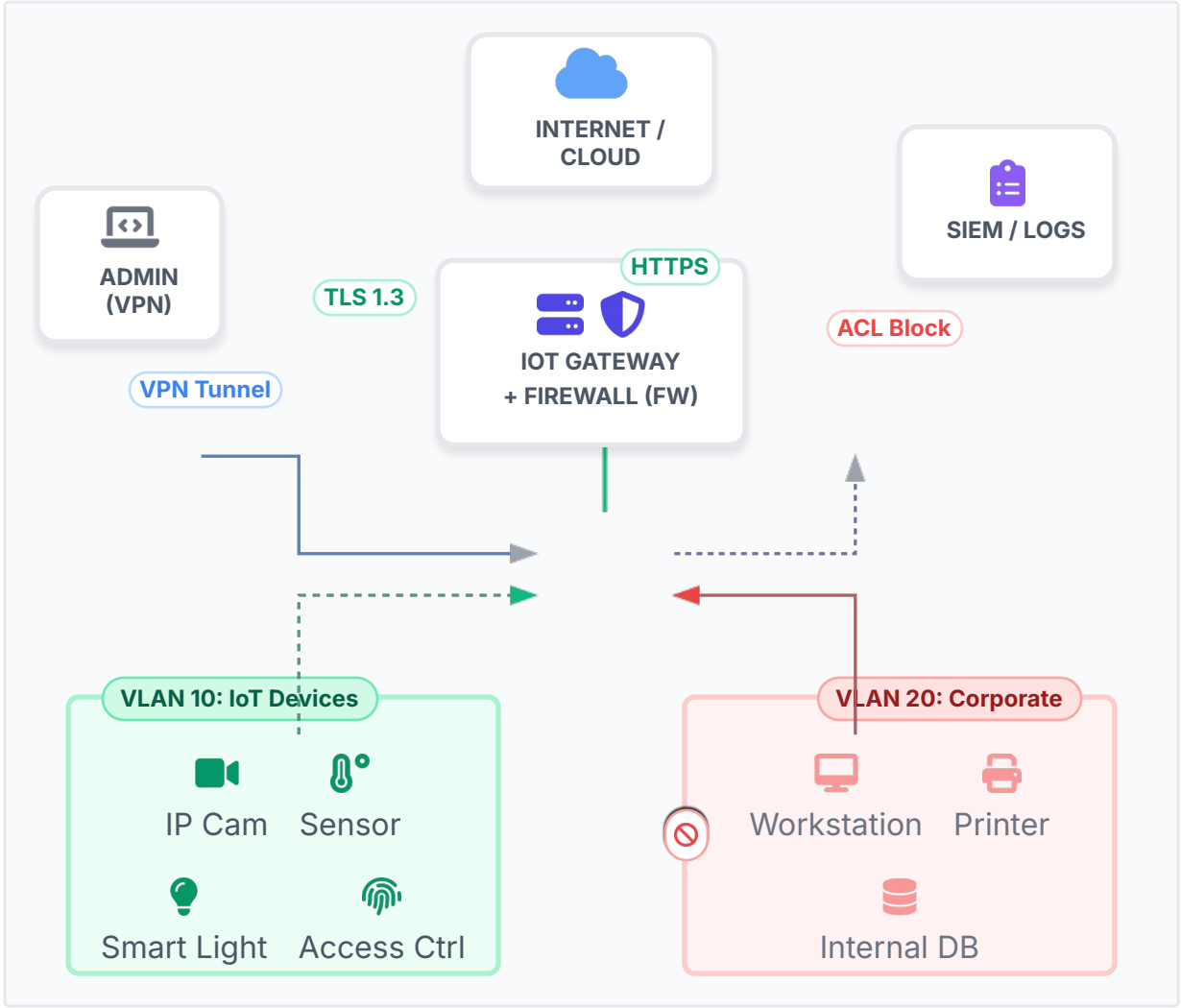
Сегментація (VLAN): Ізоляція IoT від корпоративної мережі.

Шифрування: Використання TLS 1.2/1.3, HTTPS для адмін-панелей.

VPN-доступ: Безпечний віддалений доступ замість Port Forwarding.

Оновлення ПЗ: Регулярний патч-менеджмент firmware.

Моніторинг: Централізований збір логів (SIEM), виявлення аномалій.



Висновки

Підсумки дослідження безпеки IoT-мереж

Критичні вразливості: Більшість IoT-пристроїв мають фундаментальні проблеми безпеки.

Ключові фактори: Застаріле ПЗ та відсутність культури кібергігієни (людський фактор).

Ефективність захисту: Навіть базові заходи (сегментація, паролі) знижують ризик на ~80%.

Економічне обґрунтування: Вартість впровадження захисту значно менша за потенційні збитки (ALE).

Системність: Точкових рішень недостатньо, потрібна комплексна архітектура.



ПРОБЛЕМИ

Велика поверхня атак, hardcoded паролі, відсутність шифрування, застарілі прошивки.



НАСЛІДКИ

Компрометація мережі, ботнети (DDoS), крадіжка конфіденційних даних, зупинка бізнесу.



РІШЕННЯ

Сегментація (VLAN), VPN, моніторинг трафіку, регулярні оновлення, політики доступу.