

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему:

«Дослідження вразливостей і методів неавторизованого
отримання доступу до систем відеоспостереження»

Виконав студент II-го курсу, групи КБм22-1
спеціальності 125 «Кібербезпека»

 Тальченко Д.О.

Керівник

завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Єфіменко А.А.

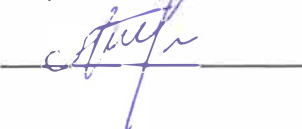
Консультант

професор кафедри комп'ютерної інженерії
та кібербезпеки, доктор технічних наук, доцент

 Воротніков В.В.

Рецензент

доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук,

 Шелуха О.О.

Житомир 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.

«13» жовтня 2023 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу

Студента **Тальченка Дмитра Олександровича**

Тема роботи: **Дослідження вразливостей і методів неавторизованого отримання доступу до систем відеоспостереження**

Затверджена Наказом по університету від «13» жовтня 2023 р. №572/с

Термін здачі студентом закінченої роботи «11» грудня 2023 р.

Вихідні дані для роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є безпека систем відеоспостереження. Об'єктом дослідження роботи є системи відеоспостереження, які використовуються для забезпечення безпеки, контролю та нагляду.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А. 	16.10.2023	 16.10.2023
2	Єфіменко А.А. 	31.10.2023	 31.10.2023
3	Єфіменко А.А. 	10.11.2023	 10.11.2023

Керівник  Єфіменко А.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	16 жовтня 2023 – 16 жовтня 2023	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо вразливостей систем відеоспостереження	17 жовтня 2023 – 19 жовтня 2023	Виконано
3	Аналіз принципів та технологій побудови систем відеоспостереження	20 жовтня 2023 – 23 жовтня 2023	Виконано
4	Аналіз вразливостей систем відеоспостереження	24 жовтня 2023 – 26 жовтня 2023	Виконано
5	Аналіз підходів та методів підвищення рівня захищеності систем відеоспостереження	27 жовтня 2023 – 30 жовтня 2023	Виконано
6	Аналіз актуальних вразливостей систем відеоспостереження	31 жовтня 2023 – 2 листопада 2023	Виконано
7	Аналіз та застосування виявлення вразливостей в системах відеоспостереження	3 листопада 2023 – 4 листопада 2023	Виконано
8	Аналіз технологій та заходів протидії вразливостям в системах відеоспостереження	5 листопада 2023 – 9 листопада 2023	Виконано
9	Створення стратегій та плану забезпечення кібербезпеки в системах відеоспостереження	10 листопада 2023 – 13 листопада 2023	Виконано
10	Аналіз потреб для фахівців у галузі кібербезпеки та захисту інформації	16 листопада 2023 – 20 листопада 2023	Виконано
11	Аналіз ролі штучного інтелекту в системах відеоспостереження	23 листопада 2023 – 25 листопада 2023	Виконано
12	Аналіз міжнародного глобального співробітництва у впровадженні систем відеоспостереження	26 листопада 2023 – 30 листопада 2023	Виконано
13	Написання пояснювальної записки	31 листопада 2023 – 3 грудня 2023	Виконано
14	Підготовка презентації та виступу	5 грудня 2023 – 6 грудня 2023	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	7 грудня 2023 – 8 грудня 2022	Виконано
16	Захист	11 грудня 2023	Виконано

Студент Тальченко Д.О.

Керівник Єфіменко А.А.

АНОТАЦІЯ

Кваліфікаційна робота містить 63 сторінки, 22 ілюстрації, 13 таблиць, список використаних джерел із 30 найменувань.

Метою роботи є процес дослідження вразливостей та методів неавторизованого доступу до систем відеоспостереження.

В ході дослідження проведено аналіз принципів побудови та проблем захисту сучасних систем відеоспостереження. Особлива увага була приділена аналізу принципів та технологій побудови таких систем. Висвітлено важливість усунення вразливостей та застосування сучасних методів для підвищення рівня захищеності систем відеоспостереження. Результатом цього етапу є детальні висновки, спрямовані на оптимізацію принципів та технологій побудови систем відеоспостереження..

Проведено аналіз актуальних вразливостей, методів виявлення та протидії у системах відеоспостереження. Розглянуті методи, технології та заходи для запобігання та усунення вразливостей, приділяючи увагу їх практичній застосовності. Останній етап дослідження включає розробку практичних рекомендацій для забезпечення захисту систем відеоспостереження. Представлені рекомендації охоплюють власників бізнесів, фахівців з кібербезпеки та захисту інформації. Також висвітлені перспективи застосування штучного інтелекту та машинного навчання у сфері кібербезпеки систем відеоспостереження та роль глобального співробітництва в цьому контексті. Загальний аналіз інформації та розроблені рекомендації є ключовими компонентами для розвитку ефективних стратегій безпеки в області відеоспостереження.

Ключові слова: СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ, ШТУЧНИЙ ІНТЕЛЕКТ, ВРАЗЛИВОСТІ

ANNOTATION.

The qualification work contains 63 pages, 22 illustrations, 13 tables, and a list of 30 references.

The purpose of the work is to study vulnerabilities and methods of unauthorised access to video surveillance systems.

The study analysed the principles of construction and security problems of modern video surveillance systems. Particular attention was paid to the analysis of the principles and technologies for building such systems. The importance of eliminating vulnerabilities and applying modern methods to increase the security of video surveillance systems was highlighted. The result of this stage is detailed conclusions aimed at optimising the principles and technologies of building video surveillance systems.

An analysis of current vulnerabilities, methods of detection and counteraction in video surveillance systems was carried out. Methods, technologies and measures to prevent and eliminate vulnerabilities are considered, paying attention to their practical applicability. The last stage of the research includes the development of practical recommendations for securing video surveillance systems. The recommendations presented cover business owners, cybersecurity and information protection specialists. The prospects for the use of artificial intelligence and machine learning in the field of video surveillance cybersecurity and the role of global cooperation in this context are also highlighted. The general analysis of information and the developed recommendations are key components for the development of effective security strategies in the field of video surveillance.

Keywords: VIDEO SURVEILLANCE SYSTEM, AI, VULNERABILITIES

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	4
ВСТУП	5
1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОБЛЕМ ЗАХИСТУ СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ	7
1.1. Аналіз принципів та технології побудови систем відеоспостереження	7
1.2. Аналіз вразливостей систем відеоспостереження	10
1.3. Аналіз сучасних та перспективних підходів та методів підвищення рівня захищеності систем відеоспостереження	14
2. АНАЛІЗ АКТУАЛЬНИХ ВРАЗЛИВОСТЕЙ, МЕТОДІВ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВРАЗЛИВОСТЯМ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.....	16
2.1. Аналіз актуальних вразливостей систем відеоспостереження	16
2.2. Аналіз та застосування методів дослідження та виявлення вразливостей в системах відеоспостереження.....	24
2.3. Методи, технології та заходи протидії та усунення вразливостей систем відеоспостереження.....	33
3. РОЗРОБКА ТА ЗАПРОВАДЖЕННЯ ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ	38
3.1. Практичні рекомендації власникам бізнесів при впровадженні систем відеоспостереження.....	38
3.2. Рекомендації для фахівців з кібербезпеки та захисту інформації.....	43
3.3. Перспективні питання застосування штучного інтелекту та машинного навчання при забезпеченні кібербезпеки та роль глобального співробітництва в системах відеоспостереження.....	51
3.4. Практична реалізація рекомендацій з усунення вразливостей	54
ВИСНОВКИ	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MITM – Man-in-the-Middle

ПЗ – Програмне забезпечення

ШІ – Штучний інтелект

CVSS - Common Vulnerability Scoring System

CVE - Common Vulnerabilities and Exposures

SAST- Static Application Security Testing

DAST - Dynamic Application Security Testing

SIEM - Security Information and Event Management

XSS - Cross-Site Scripting

IoT - Internet of Things

ВСТУП

Системи відеоспостереження, які раніше використовувалися головним чином для забезпечення безпеки та контролю, стали необхідними складовими сучасного суспільства. Завдяки технологічному розвитку, вони перетворилися на потужні інструменти, які допомагають вирішувати різноманітні завдання, починаючи від нагляду за громадським порядком та підвищення безпеки об'єктів до використання у комерційних та промислових сферах. Разом із зростанням популярності та поширеністю систем відеоспостереження, з'явилися і загрози їх безпеці.

В останні роки випадки неавторизованого отримання доступу до систем відеоспостереження та їх вразливості стали дедалі актуальнішими. Це може включати в себе несанкціонований доступ до відеопотоків, зловмисне використання записів для шантажу, або навіть потенційну загрозу для особистої приватності громадян.

Мета кваліфікаційної роботи полягає в дослідженні основних вразливостей систем відеоспостереження та методів неавторизованого отримання доступу до них. В роботі описано не лише теоретичні аспекти, пов'язані з цією проблемою, але й практичні аспекти, аналізуючи сучасні приклади вразливостей та розглядаючи можливі заходи для запобігання та виправлення вразливостей.

Об'єктом дослідження роботи є системи відеоспостереження, які використовуються для забезпечення безпеки, контролю та нагляду. Розглянуто вразливості та загрози, що ставлять під загрозу конфіденційність, цілісність та доступність даних, збережених в таких системах.

Методологія роботи полягає в розробці практичних рекомендацій для власників систем відеоспостереження та фахівців з інформаційної безпеки. Визначення майбутньої тенденції та завдання у сфері безпеки відеоспостереження, що враховуватимуть ростову складність цієї галузі та потреби користувачів у захисті.

Встановлена мета обумовлює наступні завдання:

- аналіз принципів побудови та проблеми захисту сучасних систем відеоспостереження
- аналіз актуальних вразливостей, методів виявлення та протидії вразливостям систем відеоспостереження;
- перспективні питання застосування штучного інтелекту та машинного навчання при забезпеченні кібербезпеки та роль глобального співробітництва в системах відеоспостереження;

Предметом дослідження є безпека систем відеоспостереження.

Апробація результатів:

1. Vakaliuk T., Talchenko D., Osadchyi V., Bailiuk Ye., Pokotylo O. Vulnerabilities and Methods of Unauthorized Gaining Access to Video Surveillance Systems. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, February 28, 2023. Edited by Volodymyr Sokolov, Tamara Radivilova, Vasyl Ustimenko, Mariya Nazarkevych. CEUR Workshop Proceedings, ISSN 1613-0073. Vol-3421, 2023. Pp. 174-181. – Access mode: <https://ceur-ws.org/Vol-3421/short2.pdf>

1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОБЛЕМ ЗАХИСТУ СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1. Аналіз принципів та технологій побудови систем відеоспостереження

Зазвичай системи відеоспостереження складаються з комплексу обладнання та програмного забезпечення, спрямованих на фіксування, передачу, аналіз і збереження відео та аудіозаписів з навколишнього середовища. Основними компонентами таких систем є камери спостереження, системи передачі даних, сервери для зберігання і обробки інформації, монітори для перегляду та управління, а також програмне забезпечення для налаштування та керування процесом відеоспостереження.

Центральним елементом будь-якої системи відеоспостереження є камери, які призначені для фіксування відео та аудіозаписів. Їх розташовують у точках, які потребують нагляду, і вони можуть бути різних типів, таких як стаціонарні, рухомі, приховані або камуфльовані. Камери можуть мати різний діапазон огляду та роздільну здатність для реєстрації відео в реальному часі.

Дані, зібрані камерами, передаються через мережу до центрального сервера або системи зберігання. Для передачі даних використовуються різні технології, такі як провідна мережа Ethernet, бездротова Wi-Fi, мережа передачі даних через кабельну телевізію (CCTV), а також мережі зв'язку, наприклад, Інтернет.

Отримані відеодані передаються до центрального сервера або системи зберігання, де вони зберігаються, обробляються і доступні для подальшого використання. Ці сервери мають велику обчислювальну потужність і великі обсяги зберігання, щоб забезпечити ефективну роботу системи відеоспостереження. Оператори системи відеоспостереження мають доступ до моніторів для перегляду відеопотоків та управління камерами. Сучасні системи включають інтерфейси з віддаленим доступом, що дозволяють операторам керувати системою відеоспостереження з будь-якого місця через Інтернет або мобільні пристрої.

Програмне забезпечення системи відеоспостереження дозволяє налаштовувати режими роботи камер, визначати правила аналізу відеоданих

(наприклад, розпізнавання руху, обличчя або номерів автомобілів), а також здійснювати запис та архівування відеоданих.

Важливість відеоспостереження для безпеки та контролю в сучасному світі важко переоцінити, оскільки ця технологія відіграє критичну роль в забезпеченні безпеки людей, майна і суспільних об'єктів. Опираючись на проаналізовану інформацію можна виділити основні фактори важливості систем відеоспостереження:

1. Проактивне запобігання злочинам.
2. Підвищення безпеки громадських місць.
3. Збільшення ефективності розслідування злочинів
4. Контроль за доступом та безпекою об'єктів.
5. Захист особистої безпеки.
6. Контроль за дотриманням закону та безпекою на робочих місцях.
7. Моніторинг та управління критично важливими інфраструктурними об'єктами.

Системи відеоспостереження надають змогу відслідковувати події в реальному часі та реагувати на них. Проактивне запобігання злочинам може включати в себе виявлення підозрілих осіб або незвичайних подій, які можуть служити попередженням потенційних злочинів, таких як крадіжки, напади, вандалізм і інші правопорушення.

Для підвищення безпеки громадських місць відеоспостереження розміщується в громадських місцях, таких як торгові центри, вокзали, аеропорти, парки і вулиці міст. Вони відіграють роль у запобіганні злочинності і важливі для реагування на події навколишнього середовища.

Також відеосистеми грають велику роль в збільшення ефективності розслідування злочинів. В разі виникнення злочину або інциденту системи відеоспостереження надають важливі докази. Вони можуть допомагати правоохоронним органам в розслідуванні і викритті злочинців, що значно підвищує ймовірність їх покарання.

Відеоспостереження використовується для контролю за доступом до об'єктів, таких як промислові об'єкти, офіси, багатоквартирні будинки, інфраструктурні

об'єкти тощо. Це дозволяє визначати і авторизовувати осіб, які мають доступ до певних приміщень або ресурсів, і попереджати несанкціонований доступ.

Щодо захист особистої безпеки системи відеоспостереження можуть бути також корисними. Вони можуть використовуватися в особистих машинах, на житлових ділянках або навіть на мобільних пристроях для стеження за навколишнім середовищем і надавати спокій та відчуття безпеки особам.

Додатково відеоспостереження використовується в багатьох сферах праці, включаючи виробничі підприємства, склади та інші робочі місця, для забезпечення безпеки працівників, контролю дотримання стандартів безпеки, вирішення спорів та зниження ризику нещасних випадків на роботі.

Ключову роль відеосистеми складають в моніторингу та управлінні критично важливими інфраструктурними об'єктами. Важливі інфраструктурні об'єкти, такі як електростанції, водні джерела, транспортні вузли тощо, використовують системи відеоспостереження для контролю за роботою та збереженням безпеки цих об'єктів (рис.1.1)

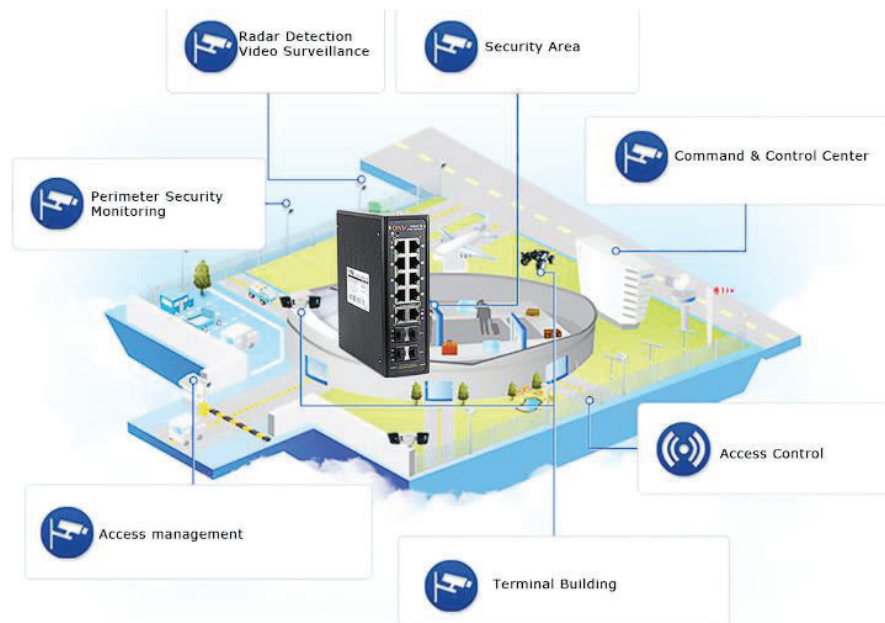


Рисунок 1.1 – Ілюстрація встановлення відеосистем на критично важливому інфраструктурному об'єкті

Усі ці аспекти вказують на те, що відеоспостереження є необхідним інструментом для забезпечення безпеки та контролю в різних сферах життя, від особистої безпеки до загальної безпеки суспільства.

1.2. Аналіз вразливостей систем відеоспостереження

Огляд загальних вразливостей відеосистем - це важлива частина дослідження в галузі безпеки відеоспостереження [9]. Відеосистеми, незважаючи на свою корисність, також можуть мати певні вразливості, які потенційно можуть бути використані зловмисниками для отримання несанкціонованого доступу, а також порушення конфіденційності інформації. Виходячи з огляду загальних вразливостей відеосистем можна вивести основні:

1. Необхідність правильної конфігурації.
2. Брак системних оновлень.
3. Атаки на мережевий рівень.
4. Вразливості в програмному забезпеченні.
5. Фізична безпека.
6. Недостатність журналів подій.
7. Слабка аутентифікація і авторизація.
8. Атаки на апаратне забезпечення.
9. Недостатність шифрування.
10. Вплив зовнішніх факторів.

Важливу роль у забезпеченні безпеки систем відеоспостереження відіграє необхідність правильної конфігурації. Багато вразливостей відеосистем починаються з неправильної конфігурації. Забутий пароль, слабка автентифікація або залишені за замовчуванням налаштування можуть стати вхідними воротами для несанкціонованого доступу [1].

Не менш важливим аспектом є брак системних оновлень. Виробники систем відеоспостереження регулярно випускають поновлення для свого обладнання і програмного забезпечення для виправлення виявлених вразливостей. Недостатнє оновлення обладнання може призвести до збільшення ризику злому інших систем. Також зловмисники можуть намагатися перехопити відеопотік або вкрати дані на мережевому рівні. Це може бути досягнуто через атаки MITM (Man-in-the-Middle), атаки на DNS або використання недостатньо захищених мереж.

Однією з найпопулярніших вразливостей є вразливість програмного забезпечення. Відеосистеми часто використовують вбудовані програми, які можуть

мати вразливості. Наприклад, веб-інтерфейси для керування системою можуть бути атаковані через вразливості в веб-додатках, такі як SQL-ін'єкція або XSS. Слід також не забувати про фізичну безпеку обладнання. Недостатня фізична безпека обладнання, така як недостатньо захищені сервери або камери, може дозволити зловмисникам отримати фізичний доступ і втрутитися в систему.

Недостатність журналів подій становить важливу проблему для систем відеоспостереження. Журнали подій є ключовим інструментом для виявлення несанкціонованого доступу або аномальних подій. Однак, якщо вони не є достатньо деталізованими чи неактивованими, це може значно ускладнити процес виявлення порушень безпеки. Удосконалення систем журналювання та їхнє належне налаштування є критичним етапом для забезпечення ефективного моніторингу та реагування на події в системах відеоспостереження.

Проблеми з аутентифікацією та авторизацією стають значущими вразливостями для відеосистем спостереження. Якщо системи не вимагають достатньо сильних паролів або не володіють ефективними механізмами контролю доступу, це може стати причиною атак та порушень безпеки. Удосконалення процесів аутентифікації та авторизації стає критичним для забезпечення надійного захисту відеосистем від несанкціонованого доступу.

Запобігання атакам на апаратне забезпечення, такі як камери чи сервери, важливо для забезпечення безпеки систем відеоспостереження. Фізичні атаки на обладнання можуть призвести до виявлення недоліків чи навіть викрадення інформації. Реалізація ефективних заходів захисту апаратної частини є ключовим завданням для забезпечення цілісності та безпеки систем відеоспостереження.

Недостатність шифрування може відкрити можливості для несанкціонованого доступу до відеопотоку та архівів. Забезпечення належного шифрування даних є обов'язковим кроком для захисту від небажаних втручань та конфіденційного витоку інформації.

Враховуючи вплив зовнішніх факторів, таких як погодні умови, вандалізм чи фізичні пошкодження, стає очевидним, що системи відеоспостереження повинні бути розроблені та встановлені з урахуванням можливих загроз зовнішнього

середовища. Застосування відповідних заходів захисту може уникнути відмов та пошкодження обладнання у непередбачених ситуаціях.

Загальний огляд цих загроз важливий для розуміння можливих слабких місць у відеосистемах і розробки стратегій захисту від них. Безпека відеоспостереження вимагає постійного моніторингу, оновлення та вдосконалення для забезпечення надійності та конфіденційності інформації [8].

Велику увагу слід приділити вразливостям пов'язаним із апаратним та програмним забезпеченням в системах відеоспостереження. Апаратні вразливості включають фізичний доступ до обладнання. Зловмисники можуть отримати доступ до камер або серверів, вимкнути обладнання, внести зміни в налаштування або викрасти його. Крім того, камери, розташовані на вулицях або в громадських місцях, піддаються ризику вандалізму та фізичного пошкодження.

Програмні вразливості можуть бути пов'язані зі слабкою аутентифікацією та авторизацією, що дозволяє несанкціонованим особам отримувати доступ до системи [2]. Також можуть існувати проблеми з недостатнім контролем доступу до функціоналу системи. Важливо також враховувати вразливості в програмному забезпеченні камер, такі як відмови в обслуговуванні (DoS), вразливості в мережевих протоколах або піддатливість до атак на переповнення буфера. Недостатнє оновлення програмного забезпечення систем відеоспостереження може призвести до використання вразливостей, які були виправлені в нових версіях.

Крім того, брак або недостатній рівень шифрування в відеопередачі та зберіганні відеоданих може призвести до їх перехоплення та використання несанкціонованими особами. Незахищені мережі можуть бути вразливі до атак MITM, що дозволяє атакувати передачу даних.

Загалом, вирішення цих вразливостей вимагає комплексного підходу, який включає в себе фізичну та логічну безпеку обладнання, актуальні оновлення програмного забезпечення та належні заходи контролю доступу і шифрування.

Не слід виключати також ризики, пов'язані із зловмисним використанням систем відеоспостереження, які можуть створювати серйозні загрози для особистої

приватності та безпеки людей та організацій. Ці ризики охоплюють широкий спектр потенційних негативних наслідків.

Однією з головних загроз є порушення особистої приватності осіб. Зловмисники можуть використовувати відеоспостереження для незаконного перехоплення зображень або записування відео без згоди та знання жертв. Це може призвести до викриття особистих деталей життя людей та порушити їх право на конфіденційність [7].

Відеоспостереження, яке використовується для спостереження за особистим життям, особливо в приватних місцях, може створювати серйозні етичні та правові проблеми. Люди мають право на приватність в своїх особистих просторах, і незаконне спостереження може бути надто нав'язливим.

Співробітники та персонал, які мають доступ до систем відеоспостереження, можуть зловживати цим доступом для власних цілей. Вони можуть відправляти або зберігати відеозаписи, що порушує конфіденційність або використовують їх для власної користі [9].

Злочинці можуть використовувати відеоспостереження для планування та виконання різних злочинів. Вони можуть отримувати інформацію про слабкі місця в системах безпеки та обставини, які сприяють вчиненню злочинів. Політичні організації або конкуруючі підприємства можуть використовувати відеоспостереження для збору компрометуючої інформації про опонентів або конкурентів, що може призвести до політичних або комерційних конфліктів.

Вразливості в системах відеоспостереження можуть призвести до витоку важливих відеоданих. Ці дані можуть потрапити до незаконних рук та бути використані для шантажу, публічного розголошення або навіть використання в злочинних цілях.

З метою захисту від цих ризиків необхідно вживати відповідні заходи безпеки, включаючи захист від несанкціонованого доступу до системи, шифрування важливих даних, регулярний аудит та дотримання вимог до конфіденційності та приватності.

1.3. Аналіз сучасних та перспективних підходів та методів підвищення рівня захищеності систем відеоспостереження

Для запобігання вище описаних вразливостей можна сформувати основні стратегії та підходи, які спрямовані на запобігання несанкціонованому доступу, забезпечення конфіденційності та збереження цілісності відеоданих.

Один із важливих аспектів безпеки - це контроль фізичного доступу. Дане рішення включає в себе встановлення фізичних бар'єрів, таких як замки і бар'єри, а також обмежені зони доступу. Особливу увагу слід приділити безпеці приміщень, де розташовані камери відеоспостереження, щоб запобігти можливим вандалізмом та викраденням обладнання [2].

Ще однією важливою складовою є шифрування даних. Воно застосовується як для захисту відеопотоків під час їх передачі по мережі, так і для шифрування збережених відеоданих. Використання протоколів шифрування, таких як SSL/TLS, дозволяє захистити дані від несанкціонованого доступу та перехоплення [7]. Управління доступом та аутентифікація грають важливу роль у забезпеченні безпеки. Системи багаторівневого контролю доступу обмежують права користувачів і дозволяють встановлювати рівні доступу для різних функцій системи. Важливо також вимагати сильну аутентифікацію, наприклад, використовуючи паролі, біометричні дані або картки доступу для входу в систему. Аудит та моніторинг включають в себе ведення журналів дій користувачів та подій у системі. Це допомагає виявляти незвичайну активність або спроби несанкціонованого доступу. Регулярний аудит системи дозволяє вчасно виявляти можливі загрози та вразливості.

Апаратне забезпечення також має значення у забезпеченні безпеки систем відеоспостереження. Використання захищених камер з фізичними заходами захисту, такими як корпуси, допомагає запобігти вандалізму та фізичним пошкодженням обладнання. Апаратні міжмережні екрани допомагають захистити мережу відеоспостереження від зовнішніх атак.

Оновлення та патчі є важливими для підтримки безпеки. Регулярне оновлення програмного забезпечення і встановлення офіційних патчів допомагають усувати

вразливості і залишати систему безпечною [28]. Системи автоматичних оновлень спрощують цей процес і забезпечують своєчасну установку оновлень безпеки.

Не останню роль в забезпеченні безпеки систем відеоспостереження відіграє навчання та освіта персоналу. Свідомість персоналу щодо правил безпеки та процедур реагування на можливі загрози є важливою частиною всього комплексу заходів безпеки.

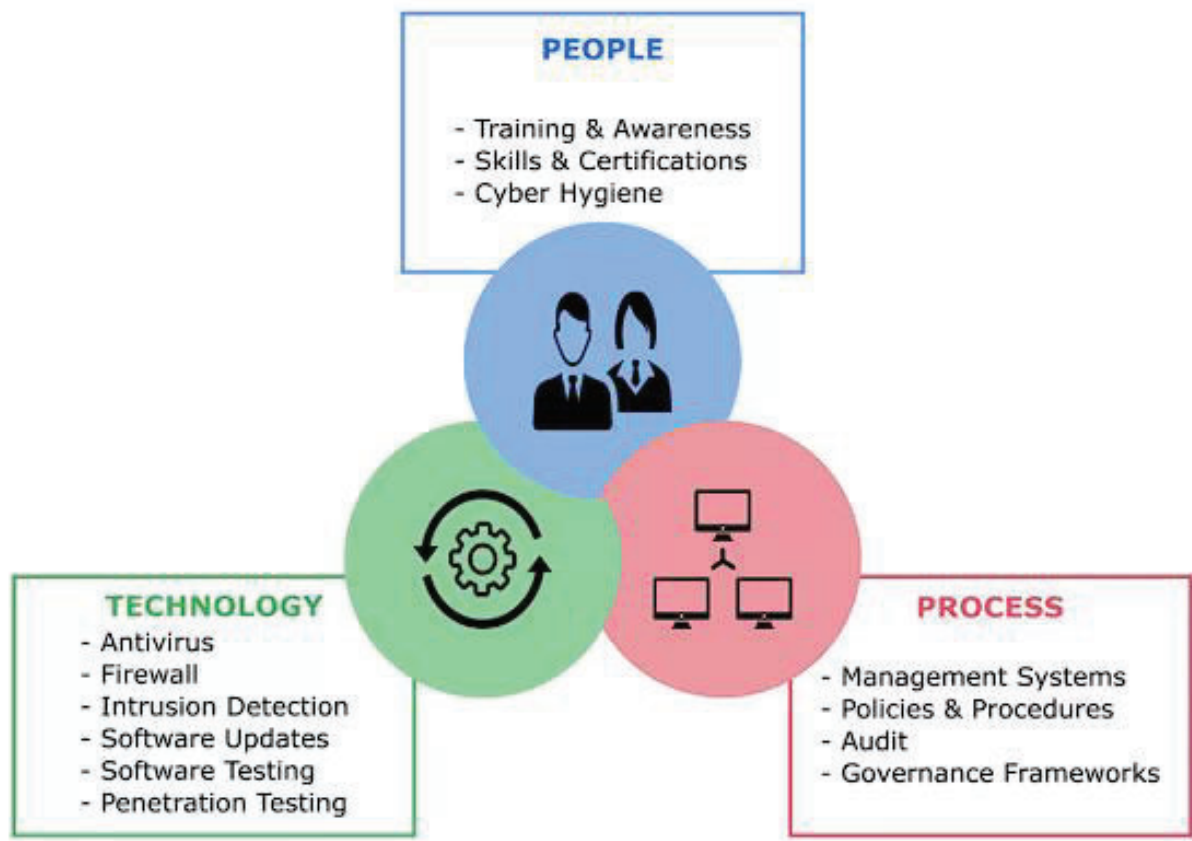


Рисунок 1.2 – Ілюстрація тактики безпеки

Ці класичні методи захисту становлять основу безпеки систем відеоспостереження та допомагають запобігти різноманітним загрозам. Розуміння, впровадження та постійне вдосконалення цих методів є критичним для забезпечення ефективної та надійної роботи систем відеоспостереження.

2. АНАЛІЗ АКТУАЛЬНИХ ВРАЗЛИВОСТЕЙ, МЕТОДІВ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВРАЗЛИВОСТЯМ СИСТЕМ ВІДЕОПОСТЕРЕЖЕННЯ

2.1. Аналіз актуальних вразливостей систем відеоспостереження

Аналізування вразливостей систем відеоспостереження є невід'ємною частиною дослідження. Аналіз розглядає потенційні вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до цих систем, а моделювання різних сценаріїв атак та їх можливі наслідки допоможе краще зрозуміти загрози, які можуть стати реальністю у виробничому та особистому використанні систем відеоспостереження [1]. Найпопулярнішими вразливостями є:

- Використання слабких паролів.
- Відсутність оновлень безпеки.
- Недостатній контроль доступу
- Використання застарілого обладнання
- Незахищена мережа передачі даних.

Використання слабких паролів у відеосистемах є однією з основних вразливостей, яка може призвести до серйозних проблем безпеки. Слабкий пароль - це пароль, який легко вгадати або підібрати шляхом перебору.

Таблиця 2.1 – Сценарій атаки за допомогою використання вразливих паролів

	Опис
Приклад	Адміністратор системи встановлює простий пароль "12345", для доступу до керування системою відеоспостереження.
Сценарій атаки	Зловмисники можуть використовувати перебір паролів або здійснювати атаки "брутфорс" для отримання доступу до системи.

Наслідки	Несанкціоновані особи отримують контроль над системою відеоспостереження, можуть видаляти або змінювати відеозаписи та отримувати доступ до приватних зображень і відео.
-----------------	--



Рисунок 2.1 – Ілюстрація найпопулярніших паролів

За статистикою 2022 року майже 5 мільйонів людей мали пароль password.

Обираючи слабкі паролі зловмиснику не потрібно витратити багато часу на проникнення до систем користувача.

Система відеоспостереження зазвичай постачається з іменем користувача та паролем, які встановлено за замовчуванням. І часто споживачі залишають ці дані без змін до першого випадку злому. Щоправда, деякі виробники обладнання для відеоспостереження змушують змінювати пароль при першому підключенні пристрою. При цьому система аналізує заданий пароль на ефективність і часто вимагає використання комбінації цифр та літер у різних регістрах, чим викликає невдоволення користувача. Але подібні рамки позитивно позначаються на безпеці та дозволяють дати доступ до інформації саме тим, кому це дійсно дозволено [2].

Залежно від виробника, деякі камери (наприклад, фірми Samsung) взагалі не дають можливості залишити заводський пароль, а камери фірми Axis дозволяють власнику вибрати, чи задавати новий пароль користувача, чи зупинитися на звичайному pass. В результаті, лінівi власники та адміністратори систем відеоспостереження наражають свою інформацію на великий ризик. Компанія Dahua взагалі пропонує всім відому комбінацію "admin/admin", а в деяких моделях цифрових відеореєстраторів, включаючи обладнання останнього покоління, взагалі відсутня можливість зміни цього логіну та паролю. Не кажучи вже про те, що в їх IP-камерах є два облікові записи (один з них з правами адміністратора), видалення яких не передбачено (це 666666/666666 та 888888/888888) [30].

Неуважне ставлення багатьох виробників до процесу переконання користувачів змінити дані входу, в принципі, зрозуміле. Адже якщо людина вирішила встановити систему відеоспостереження, щоб убезпечити своє майно та життя, то невже вона не подбає про безпеку самої системи?

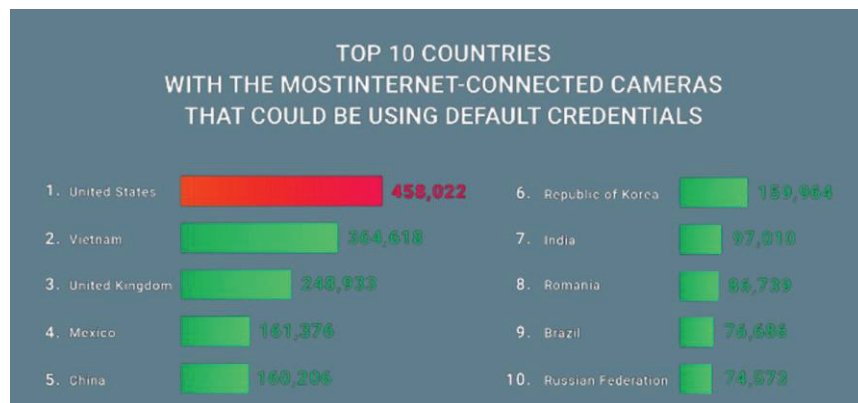


Рисунок 2.2 – Ілюстрація рейтингу країн з найбільшою кількістю підключених систем відеоспостереження, які використовують облікові дані за замовчуванням

На деяких мережевих ресурсах спеціально публікуються повні списки логінів та паролів за замовчуванням для усіх популярних марок обладнання. Це ненав'язливе нагадування тим, хто ще не спромігся подумати про захист своєї інформації. Нижче наведено табл.2.2, яка містить значення за замовчуванням логінів та паролів відомих фірм-розробників IP-обладнання [30].

Таблиця 2.2 - Значення за замовчуванням логінів та паролів відомих фірм-розробників ір-обладнання

Фірма-розробник ІР-камер	Логін/пароль за замовчуванням	Фірма-розробник ІР-камер	Логін/пароль за замовчуванням
ACTi	admin/123456 або Admin/123456	JVC	admin/jvc
Arecont Vision	-	Mobotix	admin/meinsm
Avigilon	admin/admin	Panasonic	admin/12345
Axis	root/pass, в нових моделей немає пароля за замовчуванням	Pelco Sarix	admin/admin
Basler	admin/admin	Pixord	admin/admin
Bosch	-	Samsung Electronics	root/root або admin/4321
Brickcom	admin/admin	Samsung Techwin (стара модель)	admin/1111111
Cisco	Пароль за замовчуванням відсутній, задається під час першого налаштування	Samsung Techwin (нова модель)	admin/4321
Dahua	admin/admin	Sanyo	admin/admin
Digital Watchdog	admin/admin	Scallop	admin/password
DRS	admin/1234	Sentry360 (mini)	admin/1234
DVTel	Admin/1234	Sentry360 (pro)	-
DynaColor	Admin/1234	Sony	admin/admin
FLIR	admin/fliradmin	Stardot	admin/admin
Foscam	admin/ -	Starvedia	admin/ -
GeoVision	admin/admin	Trendnet	admin/admin
Grandstream	admin/admin	Toshiba	root/ikwd
Hikvision	admin/12345	VideoIQ	supervisor/supervisor
Honeywell	admin/1234	Vivotek	root/ -
IQinVision	root/system	Ubiquiti	ubnt/ubnt
IPX-DDK	root/admin або root/Admin	Wodsee	admin/ -

Відсутність оновлень безпеки у системах відеоспостереження створює серйозні ризики для їх безпеки. Незавчасні оновлення програмного забезпечення та відсутність виправлення вразливостей можуть призвести до можливостей несанкціонованого доступу та компрометації відеоданих [28].

Таблиця 2.3 -Сценарій атаки за відсутності своєчасних оновлень

	Опис
Приклад	Власник системи відеоспостереження не встановлює оновлення програмного забезпечення та не виправляє відомі вразливості.
Сценарій атаки	Зловмисники використовують відомі вразливості для отримання доступу до системи.
Наслідки	Атакуючі можуть отримати контроль над системою відеоспостереження та отримувати доступ до відеоданих.

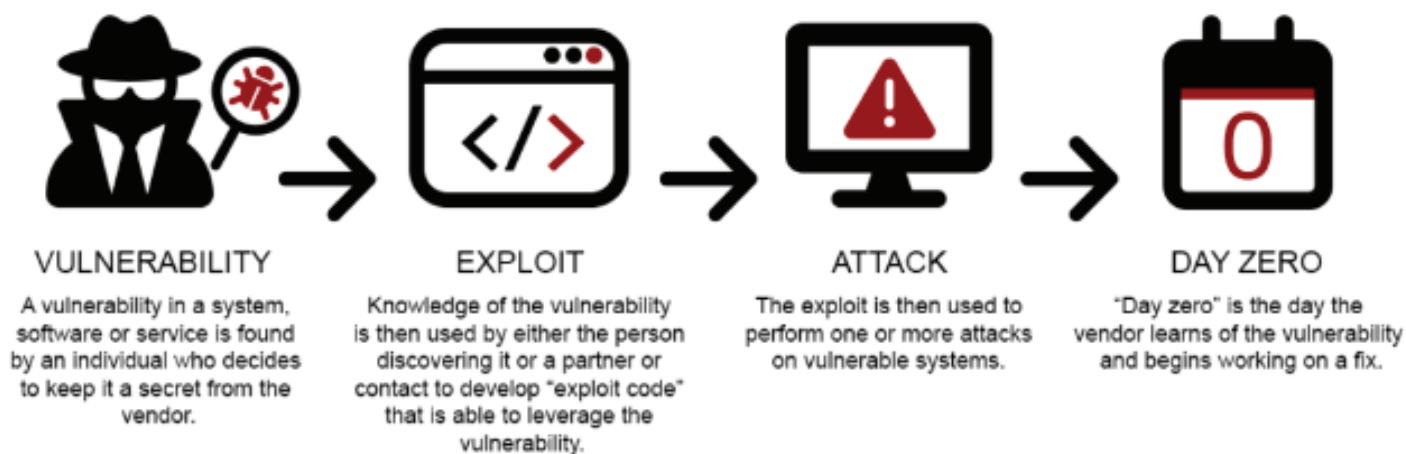


Рисунок 2.3 – Ілюстрація можливої атаки

Недостатній контроль доступу в системах відеоспостереження може призвести до незабезпеченого доступу різних користувачів до важливих ресурсів та відеоданих [8].

Таблиця 2.4 - Сценарій атаки за відсутності достатнього контролю доступу

	Опис
Приклад	Система відеоспостереження допускає доступ до всіх користувачів без належного контролю або обмежень [15].
Сценарій атаки	Зловмисники можуть легко отримати доступ до відеопотоків і зображень без авторизації.
Наслідки	Приватність осіб та конфіденційність даних порушуються, і зловмисники можуть використовувати ці дані для різних цілей.

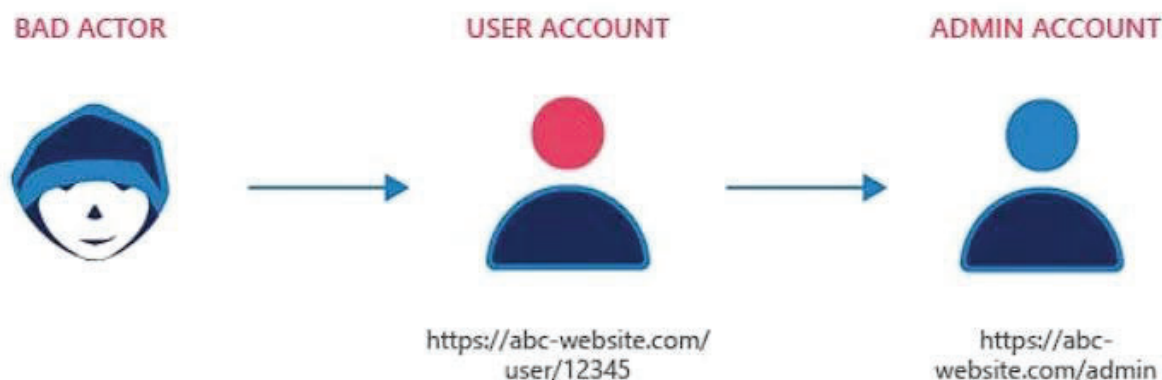


Рисунок 2.4 – Ілюстрація можливої атаки через недостатній контроль доступу

Використання застарілого обладнання в системах відеоспостереження може створювати серйозні проблеми безпеки. Застаріле обладнання може мати відомі вразливості, які не були виправлені через відсутність оновлень, що робить його легким мішенню для зловмисників і загрожує якості та надійності системи відеоспостереження [17].

Таблиця 2.5 - Сценарій атаки через використання застарілого обладнання

	Опис
Приклад	Власник системи не оновлює камери та обладнання протягом багатьох років, залишаючи їх застарілими.
Сценарій атаки	Зловмисники можуть використовувати відомі вразливості, які були виправлені в новіших версіях обладнання.
Наслідки	Відеоспостереження стає вразливим до великої кількості атак, і якість спостереження може значно зменшитися.



Рисунок 2.5 – Приклад застарілого обладнання

Використання незахищеної мережі передачі даних у системах відеоспостереження може призвести до ризику перехоплення та несанкціонованого доступу до важливих відеоданих. Відсутність шифрування під час передачі відеопотоків може дозволити зловмисникам переглядати або вкратити конфіденційну інформацію [15].

Таблиця 2.6 - Сценарій атаки через відсутність шифрування трафіку

	Опис
Приклад	Відеопотоки передаються через незахищену мережу без шифрування.
Сценарій атаки	Атакуючі можуть перехоплювати відеодані та отримувати доступ до зображень.
Наслідки	Конфіденційність відеозаписів порушується, і важлива інформація може бути використана зловмисниками.

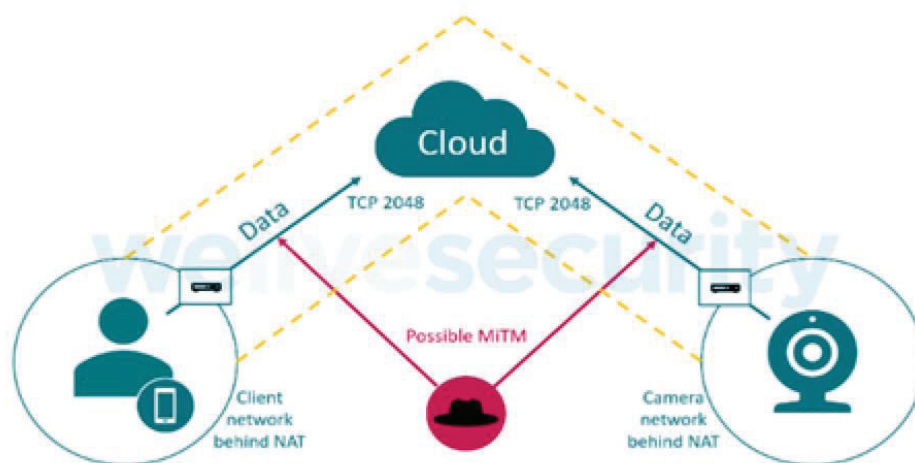


Рисунок 2.6 – Ілюстрація перехоплення інформації

Ці приклади ілюструють, як вразливості в системах відеоспостереження можуть призвести до різних видів атак та негативних наслідків. Для запобігання таким сценаріям атак необхідно вживати відповідні заходи безпеки та ретельно відстежувати стан системи відеоспостереження.

2.2. Аналіз та застосування методів дослідження та виявлення вразливостей в системах відеоспостереження

У змінному та швидкозмінному цифровому світі інформаційної безпеки використання інструментів для тестування на проникнення визначається як ключовий елемент стратегії протидії кіберзагрозам. Спрямовані на ідентифікацію та усунення потенційних вразливостей, ці інструменти виступають не тільки як технічні рішення, але й як стратегічні складові в системах забезпечення безпеки.

Інструменти для тестування на проникнення стають невід'ємною складовою в кібербезпеці. Вони використовуються для систематичного виявлення та аналізу слабких місць у мережах та програмному забезпеченні, що піддають ризику конфіденційність, цілісність та доступність даних. Важливою частиною їх функціоналу є проведення етичного вторгнення в систему для виявлення вразливостей та оцінки реакції на можливі загрози.

Один із найпоширеніших інструментів у цьому контексті — Metasploit. Він володіє широким набором готових експлойтів та можливостей, що дозволяють не лише виявляти вразливості, але й використовувати їх для демонстрації атак та розробки стратегій захисту [18].

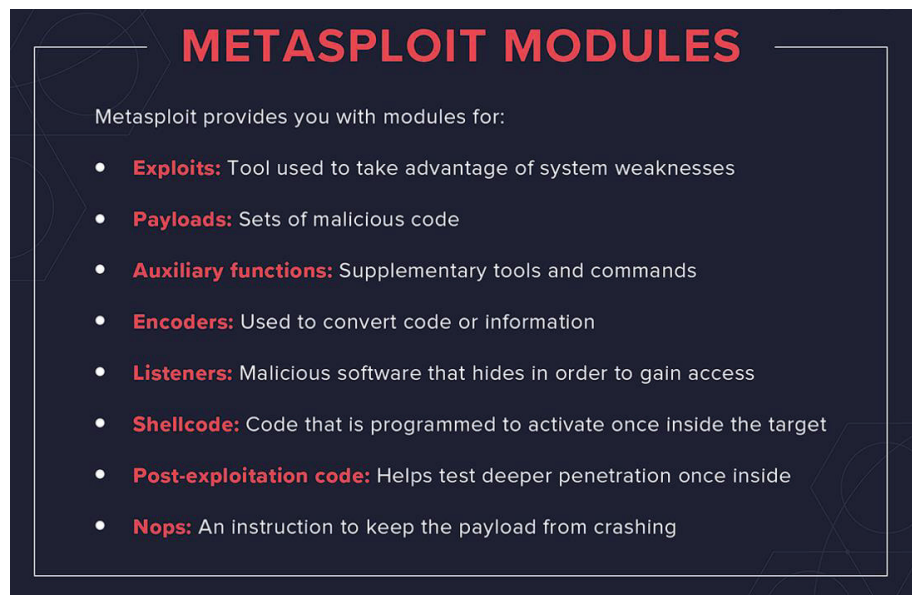


Рисунок 2.7 – Ілюстрація основних модулів Metasploit

Невід'ємним інструментом також є – Nmap. Він використовується для сканування мережі та виявлення активних пристроїв, а також аналізу портів та

використовуваних служб. Його високий рівень гнучкості дозволяє інженерам безпеки ефективно сканувати мережу та відображати її структуру [19].

```
root@kali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:43 EST
Nmap scan report for dsldevice.lan (192.168.1.1)
Host is up (0.0012s latency).
MAC Address: 18:45:93:69:A5:10 (Taicang T&W Electronics)
Nmap scan report for 192.168.1.3
Host is up (0.00030s latency).
MAC Address: 8C:EC:4B:71:C5:DE (Dell)
Nmap scan report for 192.168.1.4
Host is up (0.024s latency).
MAC Address: 2A:84:98:9F:E5:5E (Unknown)
Nmap scan report for 192.168.1.5
Host is up (0.012s latency).
MAC Address: 30:24:32:1F:89:AC (Intel Corporate)
Nmap scan report for 192.168.1.8
Host is up (0.0058s latency).
MAC Address: 44:CB:8B:C2:20:DA (LG Innotek)
Nmap scan report for 192.168.1.12
Host is up (0.00027s latency).
MAC Address: 00:0C:29:78:20:90 (VMware)
Nmap scan report for 192.168.1.108
Host is up (0.00017s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap scan report for 192.168.1.9
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 23.67 seconds
root@kali:~#
```

Рисунок 2.8 – Сканування мережі через Nmap через протокол ARP

Інструмент для аналізу мережевого трафіку Wireshark також є досить популярним у проведенні тесту на проникнення. Це програмне забезпечення дозволяє ретельно аналізувати дані, що передаються по мережі, і виявляти потенційні слабкі місця, а також аномальну активність, що може свідчити про можливі атаки чи порушення безпеки.

No.	Time	Source	Destination	Protocol	Length	Info
64	0.550463087	TaicangT_69:a5...	Dell_71:c5:de	ARP	60	Who has 192.168.1.3? Tell 192.168.1.1
65	0.550463118	Dell_71:c5:de	TaicangT_69:a5:10	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
209	1.589157998	TaicangT_69:a5...	VMware_b2:bb:77	ARP	60	Who has 192.168.1.9? Tell 192.168.1.1
210	1.589181561	VMware_b2:bb:77	TaicangT_69:a5:10	ARP	42	192.168.1.9 is at 00:0c:29:b2:bb:77
228	1.974212283	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.9
229	1.974288490	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.9
230	1.974336247	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.9
231	1.974396043	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.9
232	1.974433312	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.9
233	1.974456184	Dell_71:c5:de	VMware_b2:bb:77	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
234	1.974463392	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.9
235	1.974494541	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.7? Tell 192.168.1.9
236	1.974541930	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.9
237	1.974575204	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.9
238	1.974604008	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.9

▶ Frame 64: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: TaicangT_69:a5:10 (18:45:93:69:a5:10), Dst: Dell_71:c5:de (8c:ec:4b:71:c5:de)
 ▶ Address Resolution Protocol (request)

0000	8c	ec	4b	71	c5	de	18	45	93	69	a5	10	08	06	00	01	...	Kq	...	E	...	i	...
0010	08	00	06	04	00	01	18	45	93	69	a5	10	c0	a8	01	01	...	...	...	...	...	...	
0020	00	00	00	00	00	00	c0	a8	01	03	00	00	00	00	00	00	...	...	...	...	...	...	
0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...	...	...	...	...	...	

Рисунок 2.9 – Перегляд попереднього запиту Nmap через Wireshark

Не менш важливим та популярними рішеннями є - Burp Suite та OWASP Zed Attack Proxy (ZAP). Вони представляють собою важливий набір інструментів у сфері тестування безпеки, що використовується для ефективного аналізу та захисту веб-додатків від потенційних загроз. Burp Suite є широко визнаним та використовуваним інструментом для виявлення та аналізу вразливостей веб-застосунків. Зокрема, він забезпечує можливість ідентифікації потенційних слабкостей у безпеці веб-додатків та надає засоби для їхнього виправлення [20].

З іншого боку, OWASP Zed Attack Proxy (ZAP) володіє схожим функціоналом, спрямованим на тестування вразливостей веб-застосунків. Цей інструмент включає в себе широкий набір функцій для виявлення різноманітних загроз, включаючи атаки типу "Cross-Site Scripting" (XSS), "Cross-Site Request Forgery" (CSRF) та інші. Разом, Burp Suite та OWASP ZAP стають потужним дуєтом для тестування та забезпечення безпеки веб-додатків. Вони доповнюють один одного, надаючи аналітичні інструменти та сканування для виявлення потенційних уразливостей та надійні засоби для їхнього подальшого виправлення.

Ці інструменти є невід'ємною частиною процесу забезпечення безпеки веб-додатків та допомагають забезпечити високий рівень захисту від широкого спектру загроз в онлайн середовищі.

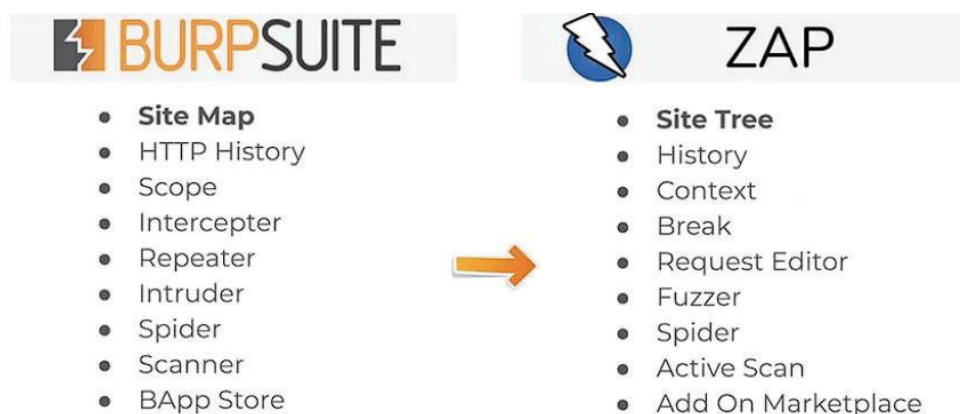


Рисунок 2.10 – Ілюстрація відмінностей інструментів BurpSuite та ZAP

Враховуючи різноманіття інструментів для тестування на проникнення, важливо враховувати, що їх використання повинно дотримуватися високих етичних стандартів та правових норм, а також здійснюватися з узгодженням із власниками систем чи мереж. Етичне хакерство передбачає здійснення тестування

на проникнення з відповідальністю та суворим дотриманням принципів конфіденційності та приватності. Використання цих інструментів повинно мати чіткі межі, що визначаються обраною методологією етичного хакерства, та не має порушувати законні права та інтереси власників систем.

Іншими словами, етичне хакерство покликане забезпечити безпеку та надійність систем, але це повинно відбуватися шляхом дотримання визначених правил і взаємодії з відповідальними сторонами. Застосування інструментів для тестування на проникнення має сприяти вдосконаленню захисту від кіберзагроз та ефективному запобіганню потенційним атакам, зберігаючи при цьому високі стандарти етики та законності.

Аналіз вразливостей програмного забезпечення є критичним етапом в стратегії інформаційної безпеки. Програми, використовувані в інформаційних системах, часто мають слабкі місця, через які можуть виникнути потенційні загрози безпеки. Завдяки скануванню вразливостей, за допомогою різноманітних інструментів, автоматизується процес пошуку та ідентифікації цих слабких місць у програмному коді. Ці інструменти визначають вразливості, такі як неправильна обробка введених даних, відсутність аутентифікації та авторизації, або використання застарілих бібліотек [16].

Пентестинг, що включає контрольовані атаки на систему чи додаток, також є важливим елементом аналізу вразливостей. Ці контрольовані атаки допомагають виявляти слабкі місця та можливі точки входу для несанкціонованого доступу. Професійні пентестери моделюють дії потенційного зловмисника, сприяючи виявленню та усуненню можливих загроз.

Аналіз коду доповнює цей процес, дозволяючи виявляти вразливості та потенційні помилки в роботі програм. Використання спеціалізованих інструментів для аналізу програмного коду стає ще однією важливою складовою цього процесу. Такий комплексний підхід дозволяє ефективно забезпечувати високий рівень інформаційної безпеки та запобігати потенційним кіберзагрозам [11]. Для ефективного виявлення та усунення вразливостей, команди розробників також можуть використовувати SAST та DAST підходи. SAST використовує аналіз

статичного коду для пошуку вразливостей, тоді як DAST оцінює додаток в реальному часі, використовуючи імітацію атак [13].

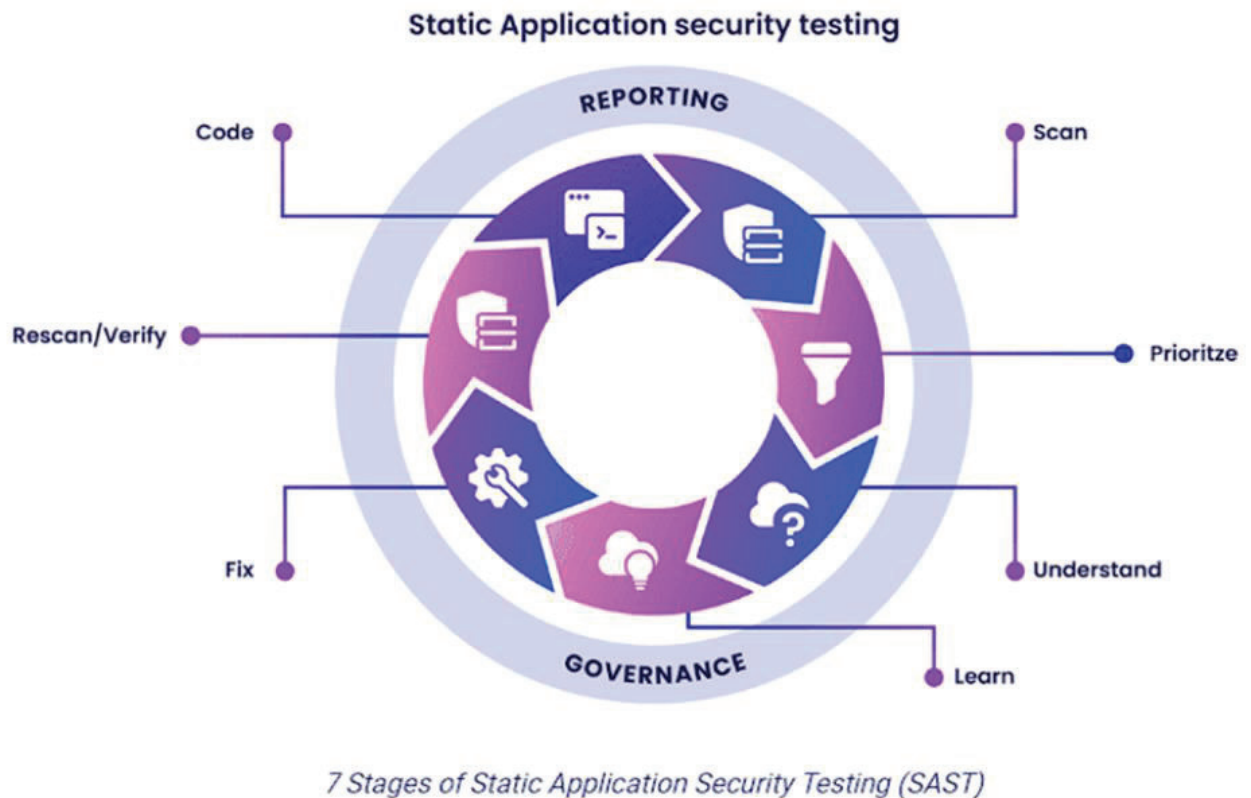


Рисунок 2.11 – Ілюстрація етапів тестового сканування додатків SAST

Важливо підкреслити, що аналіз вразливостей програмного забезпечення в комп’ютерних системах відеоспостереження – це постійний та динамічний процес, оскільки програмне забезпечення систем регулярно оновлюється та змінюється. Виявлення та усунення вразливостей стає необхідним етапом у забезпеченні безпеки інформаційних систем і захисті від можливих кіберзагроз [14].

Моніторинг мережі та виявлення незвичайних активностей є ключовою складовою систем відеоспостереження, спрямованою на оперативне реагування на потенційно небезпечні ситуації. Основна мета цього процесу полягає в ранньому виявленні аномальних подій, які можуть свідчити про можливий несанкціонований доступ чи атаку на систему.

Сучасні системи моніторингу мережі використовують різноманітні інструменти та технології для аналізу трафіку та ідентифікації нормальної та аномальної активності. Ці системи можуть виявляти незвичайні підключення,

надмірні запити, а також зміни в патернах поведінки користувачів, що можуть свідчити про можливу компрометацію системи.

Один із підходів до моніторингу мережі в комп'ютеризованих системах відеоспостереження - використання систем SIEM. SIEM інтегрує в себе збір, аналіз та реагування на події в реальному часі, дозволяючи виявляти та вирішувати проблеми безпеки ефективно. Такі системи можуть автоматично реагувати на певні типи подій, або ж надсилати сповіщення та звіти безпековим адміністраторам для подальшого аналізу та дій [12]. Серед найпопулярніших систем SIEM на ринку варто відзначити Splunk, IBM QRadar, ArcSight, Wazuh та ELK Stack (Elasticsearch, Kibana).

Splunk відзначається винятковою ефективністю у зборі та аналізі об'ємних даних, гарантуючи розширені можливості в сфері кібербезпеки.

IBM QRadar представляє потужну систему з вражаючим масштабуванням та розширеним функціоналом, спеціально адаптованим для потреб великих корпорацій.

ArcSight, в якості ключового компонента Micro Focus, славиться великою масштабованістю та розширеними можливостями, призначеними для великих підприємств.

Wazuh унікальний своєю гнучкістю та відкритістю коду, надаючи ефективні засоби моніторингу та виявлення аномалій. ELK Stack, об'єднуючи Elasticsearch та Kibana, представляє собою відкрите рішення, що вирізняється гнучкістю та можливістю налаштування відповідно до конкретних потреб користувача.

Кожна із зазначених систем SIEM здатна забезпечити надійний рівень безпеки в сфері відеоспостереження, враховуючи високу швидкодію, адаптованість до різноманітних умов та можливість розширення функціоналу відповідно до зростаючих потреб користувача.

Важливо також враховувати масштаби мережі в якій знаходиться система відеоспостереження, тому що використання та обслуговування систем моніторингу може бути недоцільним в мережі маленької організації, а використання таких систем у середніх або великих дає змогу поєднувати аналіз всіх комп'ютеризованих пристроїв.

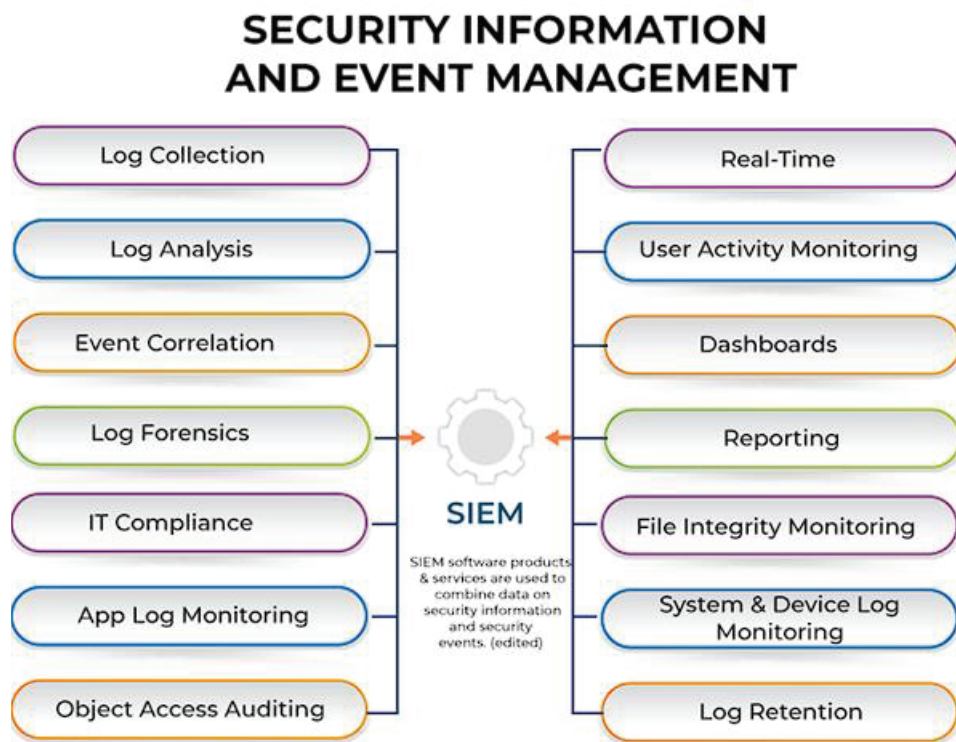


Рисунок 2.12 – Ілюстрація компонентів та можливостей SIEM систем

Ці SIEM-системи володіють рядом переваг, таких як інтеграція з іншими системами безпеки, зручний інтерфейс користувача, а також широкий спектр функцій для ефективного виявлення та реагування на події в мережі.

В контексті неперервного моніторингу мережі, важливо розглянути не лише внутрішні вразливості, але й зовнішні аспекти, що можуть стати джерелом потенційних загроз. Один із підходів до зовнішнього аналізу — використання систем, таких як Shodan, які спеціалізуються на ідентифікації публічно доступних пристроїв та ресурсів.

Shodan, визнаний світовим інтернет-пошуком для IoT та інших підключених пристроїв, грає важливу роль у контексті зовнішнього аналізу мережі та забезпечення безпеки інформаційних систем. Цей інструмент дозволяє вчасно виявляти відкриті порти, підключені пристрої та їх характеристики, надаючи важливі відомості для аналізу потенційних загроз [29].

Однією з ключових можливостей Shodan є сканування великої кількості пристроїв у реальному часі, що дозволяє забезпечити актуальну картину експозицій вашої мережі. Використовуючи цей інструмент, можна отримати інформацію, яка допомагає виявляти можливі недоліки в конфігурації мережі та

пристроїв. Щодо конкретних функцій, Shodan надає можливість фільтрації результатів за різними параметрами, такими як країна розташування, тип пристрою, відкриті порти та інші. Це дозволяє точно визначати та аналізувати публічно доступні ресурси, що може бути корисним при оцінці загроз та впровадженні відповідних заходів безпеки.

Будуючи правильний запит, пошуковик може знайти камери з стандартним логіном та паролем, з указаними вразливостями, тощо. Ввівши простий запит на пошук IP-камер марки Hikvision, Shodan знайшов 3,095,840 пристроїв по всьому світу [4].

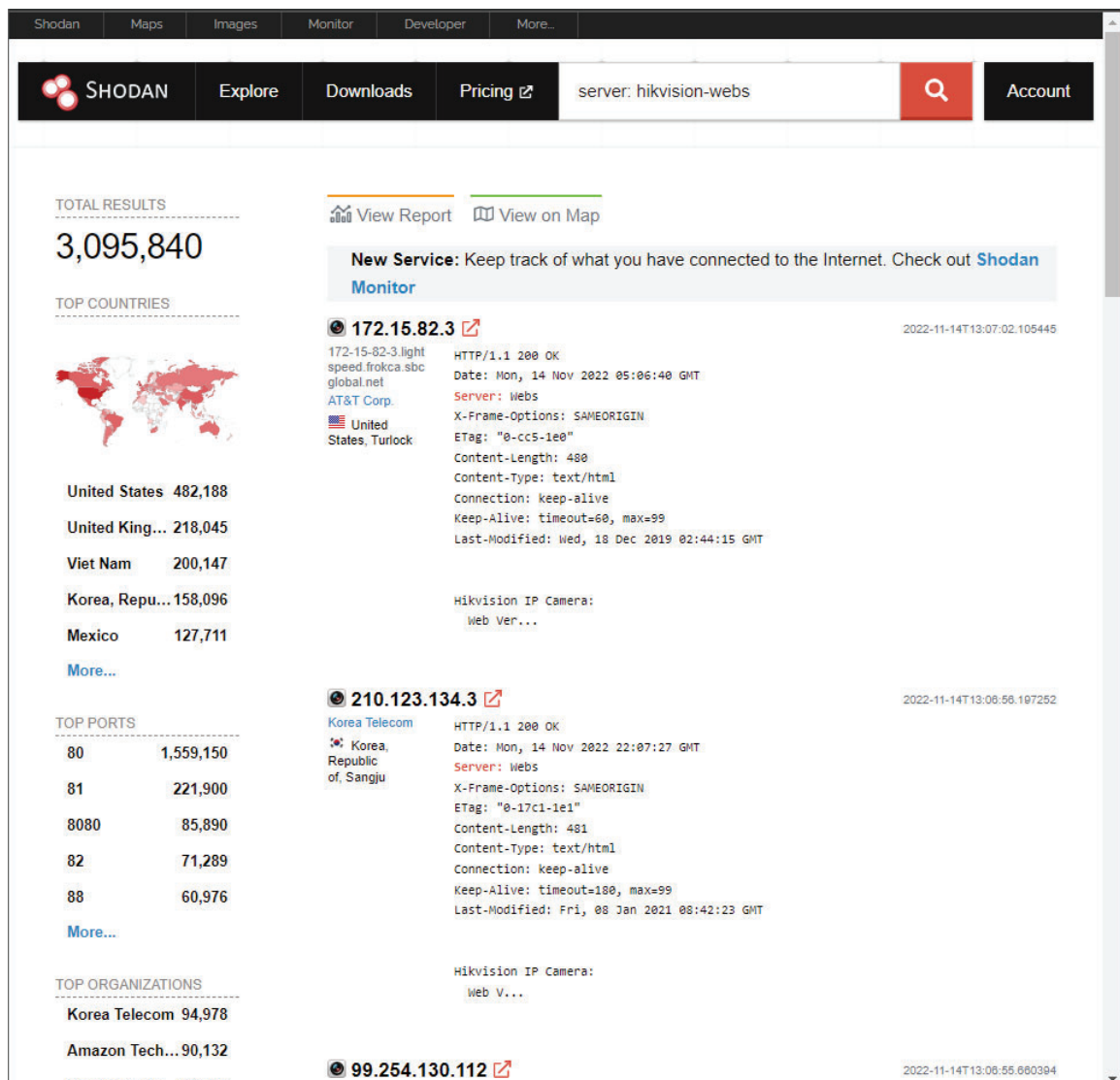


Рисунок 2.13 – Результат пошуку IP-камер марки Hikvision

На сторінці з результатами можна побачити безпосередньо знайдені IP-адреси, на кожен з яких можна натиснути та переглянути конкретні метадані цього пристрою, відповідь від певного пристрою на запит сервера Shodan, та додаткові

оператори, які допомагають відфільтрувати відповіді по наступним категоріям: порти (рис.2.14), провайдери, операційні системи, продукти, країни (рис.2.15).

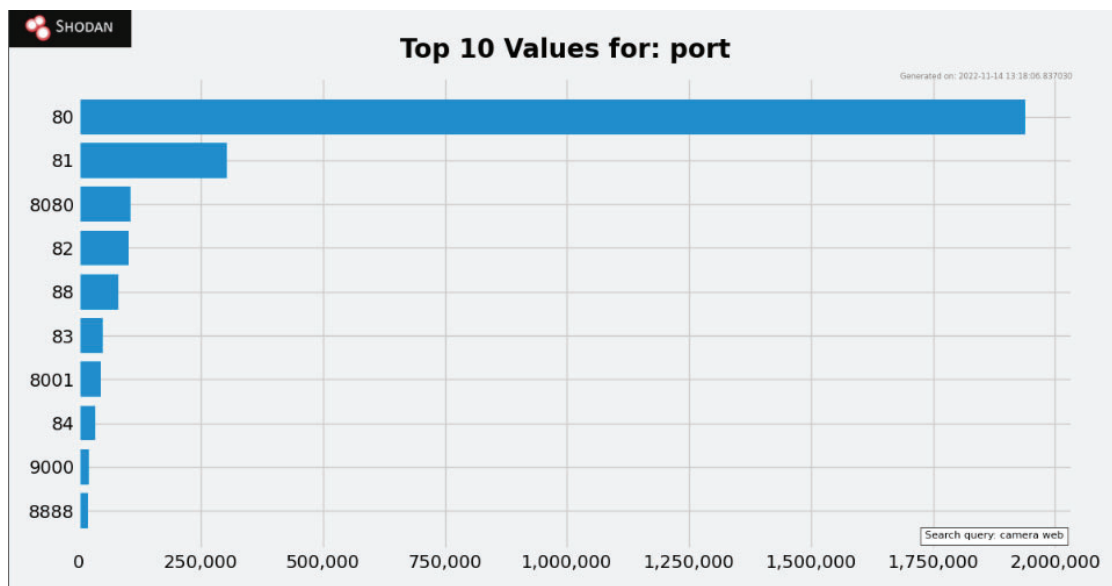


Рисунок 2.14 – Результат фільтрування по портам

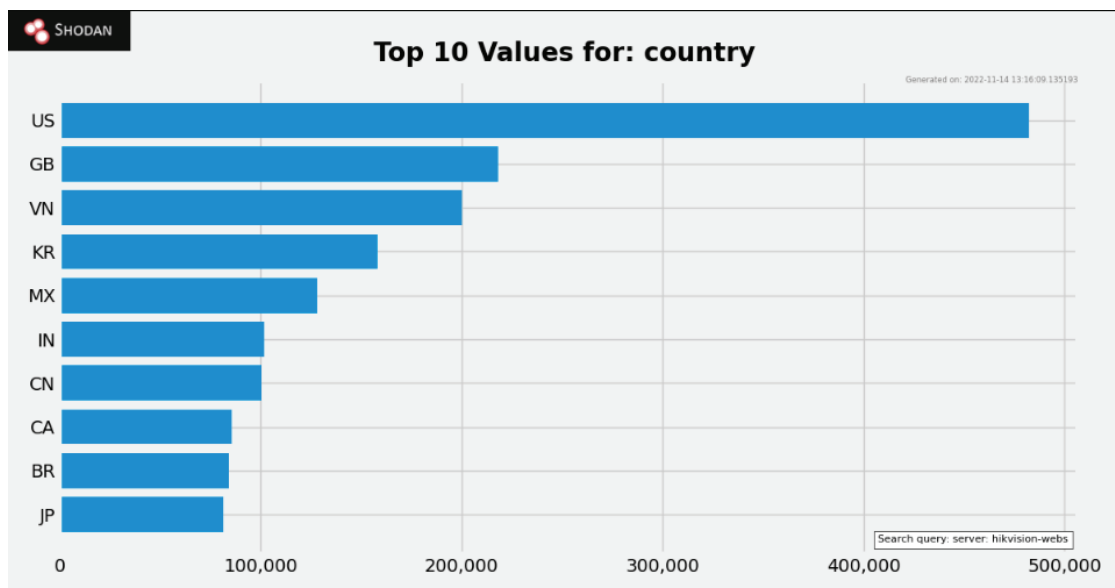


Рисунок 2.15 – Результат фільтрування по країнам

Отримані результати показують, що за обраним запитом перше місце займає порт 80, та найбільше пристроїв Hikvision виявлено в США.

2.3. Методи, технології та заходи протидії та усунення вразливостей систем відеоспостереження

Впровадження патчів та оновлень є ключовою складовою стратегії безпеки систем в яких наявне відеоспостереження, оскільки дозволяє усувати вразливості та підвищувати стійкість системи до потенційних загроз. Цей процес є невід'ємною частиною обслуговування інфраструктури та важливий для забезпечення стабільності та безпеки відеосистем [26].

В рамках комплексного підходу до безпеки інформаційних систем, важливо враховувати роль SIEM. SIEM є центральним інструментом для аналізу та виявлення подій в реальному часі в системах безпеки. Аналізуючи дані з різних джерел, SIEM дозволяє ефективно виявляти потенційні загрози та координувати заходи забезпечення безпеки. Використання SIEM дозволяє автоматизувати процес виявлення незвичайних активностей, а також відстежувати та реагувати на потенційні інциденти. Враховуючи складність та обсяг інформації в інформаційних системах, SIEM стає необхідним інструментом для вчасного реагування на кіберзагрози та підвищення загального рівня безпеки.

Принциповим елементом ефективної безпеки є виявлення та усунення вразливостей. Інтеграція CVSS і CVE дозволяє належним чином оцінювати та вирішувати питання безпеки [25]. CVSS надає числову оцінку серйозності вразливостей, допомагаючи визначити пріоритети для впровадження патчів та заходів безпеки, тоді як CVE створює унікальний ідентифікатор для кожної конкретної вразливості [27].

Додатково, важливо використовувати інтегровані рішення, такі як Microsoft 365 Defender, які надають комплексний підхід до моніторингу та усунення вразливостей. Ці системи допомагають виявляти, аналізувати та вирішувати проблеми безпеки в реальному часі, забезпечуючи ефективний захист від кіберзагроз [28].

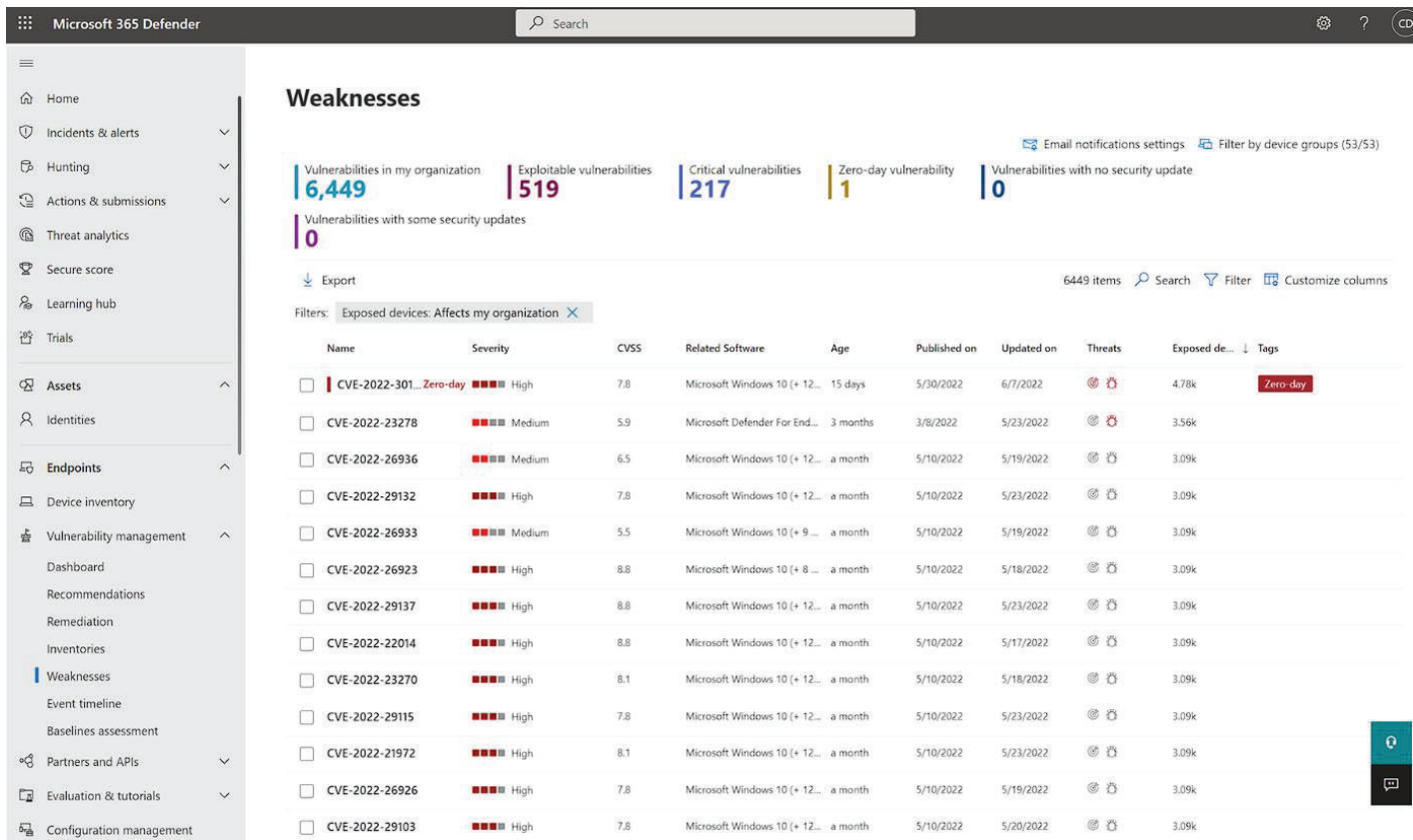


Рисунок 2.16 – Моніторинг вразливостей компанії в Microsoft 365 Defender

Впровадження патчів та оновлень є критично важливою складовою стратегії безпеки інформаційних систем. Вчасне оновлення програмного забезпечення дозволяє усувати вразливості та збільшувати стійкість системи до потенційних атак. Процес виявлення та усунення вразливостей може бути ініційований внутрішнім аудитом безпеки чи виробниками програмного забезпечення під час регулярних оновлень. Важливо мати ефективну систему впровадження патчів, яка забезпечує тестування, резервне копіювання та сумісність оновлень.

Не менш важливим аспектом є конфігурація інформаційних систем. Незважаючи на впровадження патчів та оновлень, недостатня чи неправильна конфігурація системи може стати джерелом вразливостей та потенційних ризиків. Важливо вдосконалити конфігурацію, щоб уникнути можливих атак та забезпечити оптимальний рівень безпеки. В процесі конфігурації слід враховувати принципи найменших привілеїв, обмежуючи доступ до ресурсів лише необхідним користувачам та процесам. Правильна настройка прав доступу та політик безпеки гарантує, що лише авторизовані користувачі мають доступ до необхідних ресурсів, мінімізуючи ризик несанкціонованого доступу [14].

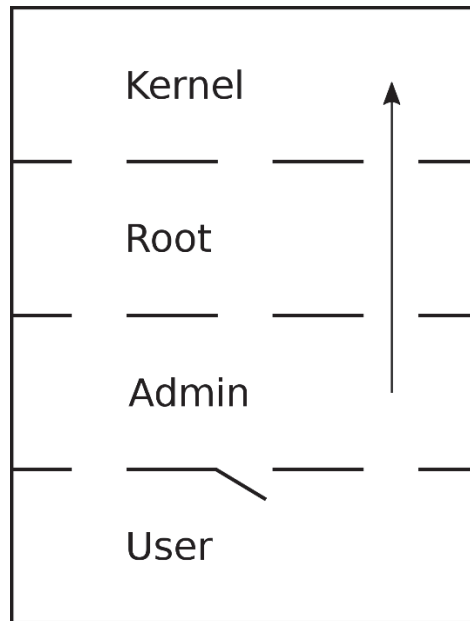


Рисунок 2.17 – Ілюстрація кроків атаки при хибній конфігурації привілеїв

Зокрема, Security Information and Event Management може використовуватися для моніторингу та аналізу подій, пов'язаних із конфігурацією системи. SIEM дозволяє виявляти незвичайні зміни в конфігураціях, які можуть свідчити про потенційні атаки або вразливості [12].

Застосування принципів "білий список" для програм та служб, що використовуються, сприяє зменшенню поверхні атаки. Такий підхід передбачає дозвіл лише на використання програм, які виражено в "білому списку", уникнення використання неперевіраних додатків.

Конфігурація систем також включає у себе встановлення та налаштування заходів антивірусного захисту, щоб ефективно виявляти та блокувати шкідливі програми. Враховуючи високу динаміку загроз у кіберпросторі, зміцнення конфігурації є постійним процесом, і регулярна перевірка та оновлення є важливим етапом у збереженні оптимального рівня безпеки.

Навчання персоналу щодо безпеки в комп'ютерних системах є важливою ланкою в стратегії кібербезпеки організацій. Цей процес охоплює різноманітні аспекти, які наведені у таблиці 2.6.

Таблиця 2.7 - Основні аспекти навчання персоналу

Назва аспекту	Опис
Свідомість щодо загроз	Навчання персоналу розпізнавати кіберзагрози, включаючи фішингові атаки, шкідливі програми та соціальну інженерію. Користувачі отримують основи кібергігієни та вивчають, як уникати сумнівних посилань та програм.
Безпека паролів та автентифікація	Працівники отримують інструкції щодо створення міцних паролів та важливості їх регулярної зміни. Вводяться основи двофакторної автентифікації для додаткового захисту облікових записів.
Освіта щодо електронної пошти	Підвищення усвідомленості про ризики, пов'язані з відкриванням вкладень та переходом за сумнівними електронними листами. Навчання ефективним методам виявлення та уникнення фішингових електронних листів.
Безпека мережі	Посилення правил безпеки при роботі з публічними мережами та використанні VPN. Користувачі навчаються ризикам від відкритих мереж та правильно налаштовувати паролі для доступу до бездротових мереж.
Управління даними	Навчання персоналу про правила конфіденційності та відповідального використання конфіденційної інформації. Підкреслення важливості регулярного архівування та резервного

	копіювання даних для запобігання втратам.
Актуальність та виявлення загроз	Навчання персоналу вчасно виявляти та повідомляти про незвичайні або підозрілі активності на їхніх робочих станціях чи в мережі. Слід зауважити, що цей цикл навчання є постійним, оскільки кіберзагрози постійно змінюються. Ефективна програма допомагає підтримувати високий рівень кібербезпеки та зменшувати ризик інцидентів в організації.

3. РОЗРОБКА ТА ЗАПРОВАДЖЕННЯ ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1. Практичні рекомендації власникам бізнесів при впровадженні систем відеоспостереження

Проаналізувавши інформацію з попереднього розділу можна підбити підсумки та сформулювати чіткі рекомендації для впровадження систем відеоспостереження. Для створення безпечної системи виділено основні ступені, які наведені в таблиці 3.1..

Таблиця 3.1 - Ступені організації безпеки підприємства

Назва аспекту	Опис
Перший ступінь	Систематичне навчання персоналу. Це не лише періодичні тренінги, але й постійний процес освіти щодо сучасних загроз та стратегій безпеки. Рівень усвідомлення має ставати вищим, оберігаючи від соціального інженерінгу, фішингу та інших потенційних загроз.
Другий ступінь	Вибір правильного обладнання та програмного забезпечення. Вчасне оновлення та патчі для апаратних та програмних компонентів - це ключ до стійкості. Моніторинг вразливостей допомагає швидко реагувати на нові атаки, забезпечуючи непохитність системи.
Третій ступінь	Контроль за доступом та шифруванням даних. Строгий контроль доступу та використання шифрування є важливим фактором для цілісності, доступності та конфіденційності інформаційних резервів.
Четвертий ступінь	Систематичний моніторинг безпеки, спрямований на виявлення незвичайних або підозрілих активностей. Ці заходи мають бути поєднані з ретельно розробленим планом реагування на інциденти, що забезпечує швидке виправлення потенційних загроз.

П'ятий ступінь	Регулярне резервне копіювання важливих даних та тестування процесів відновлення. Це є запорукою ефективності під час відновлення в разі виникнення інциденту.
Шостий ступінь	Фізичний захист обладнання та інфраструктури. Вона оберігає від фізичного доступу до системи та забезпечує надійність та можливість відновлення в разі відмови.
Сьомий ступінь	Систематичні аудити для перевірки відповідності стандартам та внутрішнім політикам. Тести на проникнення допоможуть виявити слабкі місця та вразливості, забезпечуючи надійність обраного шляху безпеки.

Ці ступені не просто ізолюють від потенційних загроз, вони взаємодіють, створюючи потужний захист. Така стратегія забезпечення безпеки є віддзеркаленням ретельного балансу між навчанням, технологією та відповідальністю.

Та всі зазначені ступені можуть бути менш ефективні без правильно підбраного обладнання та програмного забезпечення. Слід оператися на загальні рекомендації під час вибору обладнання:

- Відповідність завданням системи.
- Масштабованість.
- Стандарти безпеки та стійкість до пошкоджень
- Системи резервного живлення

Вибір обладнання для систем відеоспостереження повинен бути відповідним конкретним завданням, яке передбачає врахування чітких вимог до функціональності та кількості камер та мережевого обладнання. Забезпечення відповідності обладнання поставленим завданням є ключовим етапом при впровадженні систем відеоспостереження.

Масштабованість системи є важливим аспектом при її плануванні, оскільки апаратний комплекс повинен бути готовим до безпроблемного розширення у разі змін потреб та завдань системи. Здатність до ефективного масштабування грає важливу роль у забезпеченні довгострокової функціональності системи.

Дотримання сучасних стандартів безпеки та забезпечення стійкості до пошкоджень – важливий критерій при виборі обладнання для систем відеоспостереження. Обладнання повинно відповідати вимогам стандартів, забезпечуючи безперебійну роботу та надійність навіть в умовах непередбачуваних ситуацій. Придільення уваги системам резервного живлення є актуальним аспектом у сучасних умовах. Вибір обладнання, яке включає системи резервного живлення, гарантує неперервну роботу обладнання та збереження цілісності інформації при відмові основного живлення.

При виборі програмного забезпечення для комплексних систем відеоспостереження важливо враховувати кілька ключових аспектів, які забезпечать його ефективну та надійну роботу в різних умовах:

- Сумісність та інтеграція.
- Функціональність та розширюваність.
- Аналітика та звіти.
- Централізоване управління.
- Безпека та шифрування.

Сумісність та інтеграція представляють собою ключовий аспект обраного програмного забезпечення, оскільки від цього залежить повна сумісність та безперешкодна інтеграція з іншими системами безпеки. Такий підхід сприяє спрощенню управління та підвищує ефективність всієї системи.

Функціональність та розширюваність є важливими критеріями при виборі програмного забезпечення, оскільки вони повинні відповідати поточним вимогам та легко розширюватися для адаптації до зростання потреб у майбутньому.

Аналітика та звіти відіграють ключову роль у підвищенні ефективності відеоспостереження. Програмне забезпечення повинно надавати розширені

можливості для аналізу зібраних даних та вивчення патернів, сприяючи ефективному використанню інформації.

Наявність централізованого управління є важливим аспектом ефективної системи відеоспостереження. Програмне забезпечення повинно забезпечувати зручний інтерфейс для конфігурації та моніторингу всієї системи в єдиному місці.

Безпека та шифрування є важливими аспектами обраного програмного забезпечення, оскільки вони забезпечують високий рівень захисту. Програмне забезпечення повинно включати вбудовані заходи захисту, такі як шифрування даних та доступ за паролем, для забезпечення захисту конфіденційної інформації від несанкціонованого доступу. Обираючи апаратне та програмне забезпечення для відеоспостереження, важливо враховувати ці аспекти для забезпечення безпеки та ефективності всієї системи.

Підсумовуючи всю цю інформацію можна створити план післяпродажного обслуговування такої системи. Такий стратегічний план має бути розроблено з урахуванням найвищих стандартів безпеки та ефективності, спрямований на глибоке забезпечення бездоганної роботи системи відеоспостереження та забезпечення не лише функціональності, але й впевненості у її надійності.

План післяпродажного обслуговування для системи відеоспостереження включає наступні ключові етапи:

1. Відповідність завданням системи:

- Вибір обладнання, враховуючи конкретні завдання системи відеоспостереження.
- Формулювання чітких вимоги до кількості та функціональності камер і мережевого обладнання.

2. Масштабованість:

- Планування системи з можливістю розширення.
- Забезпечення можливості масштабування апаратного комплексу без значних втрат ефективності.

3. Стандарти безпеки та стійкість до пошкоджень:

- Вибір обладнання відповідно сучасним стандартам безпеки.

- Стійкість до непередбачених умов для надійної роботи системи.

4. Системи резервного живлення:

- Вибір обладнання з системами резервного живлення.
- Створення умов для безперебійної роботи обладнання та збереження цілісності інформації при відмові основного живлення.

5. Сумісність та інтеграція програмного забезпечення:

- Вибір програмного забезпечення, яке гармонійно співпрацює з обладнанням.
- Забезпечення сумісності та безперешкодну інтеграцію з іншими системами безпеки.

6. Функціональність програмного забезпечення:

- Врахування функціональних можливості програмного забезпечення, які відповідають поточним вимогам.

7. Аналітика та звіти:

- Забезпечення ефективного використання системи відеоспостереження за допомогою аналітики та інструментів для аналізу зібраних даних.
- Вибір програмного забезпечення з розширеними можливостями для вивчення патернів та використання зібраної інформації.

8. Централізоване управління:

- Забезпечення централізованого управління системою відеоспостереження.
- Вибір програмного забезпечення з зручним інтерфейсом для конфігурації та моніторингу всієї системи в одному місці.

9. Безпека та шифрування:

- Використання ПО , яке відповідає стандартам безпеки та виконання патчингу.
- Використання протоколів шифрування та аудит доступу до системи.

Підсумовуючи, власники систем відеоспостереження повинні ретельно обирати технічні рішення, враховуючи не лише конкретні завдання, а й

індивідуальні особливості свого бізнесу. Варто пам'ятати про важливість гнучкості та масштабованості системи. Усі аспекти, від стандартів безпеки до ефективного аналізу даних, повинні бути контрольовані для забезпечення успішного та надійного функціонування системи відеоспостереження.

3.2. Рекомендації для фахівців з кібербезпеки та захисту інформації

Однією з рекомендацій фахівцю з інформаційної безпеки є створення стратегій та планів безпеки. Стратегія безпеки комп'ютерних систем включно з відеоспостереженням є важливим документом, який визначає підходи та завдання використання відеоспостереження для забезпечення безпеки об'єкта. В умовах швидкозмінюючогося середовища, де загрози розвиваються, стратегія повинна бути гнучкою та адаптованою до конкретних потреб та ситуацій об'єкта. Розробка стратегії включає важливі етапи, починаючи з аналізу потреб і загроз. Визначення цілей і завдань системи відеоспостереження вимагає конкретності та вимірюваності, щоб забезпечити їх досяжність та актуальність [16]. Вибір підходів, таких як моніторинг периметра чи контроль доступу, визначається на основі цілей та завдань. Наступний кроком необхідно визначити вимоги до системи, включаючи технічні, функціональні та безпекові аспекти. Розробка плану реалізації допомагає визначити терміни, бюджет та відповідальних за впровадження.

Важливо зауважити, що стратегія безпеки систем - це документ, який повинен регулярно оновлюватися відповідно до змін у потребах та загрозах об'єкта. Розробка стратегії має значні переваги, такі як покращення ефективності системи, зменшення витрат та підвищення загального рівня безпеки об'єкта.

Розробка стратегії безпеки відеоспостереження включає в себе наступні етапи:

1. Аналіз потреб і загроз

На першому етапі необхідно провести аналіз потреб і загроз об'єкта. Це допоможе визначити, які цілі та завдання необхідно досягти за допомогою системи відеоспостереження.

При аналізі потреб необхідно враховувати такі фактори:

- Вид діяльності, що здійснюється на об'єкті;
- Тип об'єкта;

- Розмір об'єкта;
- Кількість людей, що перебувають на об'єкті;
- Типи загроз, які можуть виникнути на об'єкті.
- При аналізі загроз необхідно враховувати такі фактори:
- Фізичні загрози, такі як крадіжки, вандалізм, тероризм;
- Інформаційні загрози, такі як несанкціонований доступ до інформації, розкрадання даних;
- Технічні загрози, такі як збої в роботі обладнання, порушення цілісності даних.

2. Визначення цілей і завдань

На основі результатів аналізу потреб і загроз необхідно визначити цілі і завдання системи відеоспостереження.

Цілі системи відеоспостереження повинні бути конкретними, вимірюваними, досяжними, актуальними та обмеженими в часі.

Завдання системи відеоспостереження повинні визначати, як будуть досягнуті цілі.

3. Вибір підходів

На основі цілей і завдань необхідно вибрати підходи до використання відеоспостереження для забезпечення безпеки об'єкта.

До таких підходів можуть відноситися:

- Моніторинг периметра;
- Моніторинг внутрішніх приміщень;
- Моніторинг доступу;
- Моніторинг виробничих процесів;
- Моніторинг персоналу.

4. Визначення вимог до системи

На основі цілей, завдань та підходів необхідно визначити вимоги до системи відеоспостереження.

Вимоги до системи повинні включати в себе такі характеристики:

- Технічні характеристики обладнання;
- Функціональні можливості системи;
- Операційні вимоги;
- Вимоги до безпеки.

5. Розробка плану реалізації

На основі вимог до системи необхідно розробити план реалізації.

План реалізації повинен визначати:

- Терміни реалізації;
- Бюджет реалізації;
- Відповідальних осіб за реалізацію.

Стратегія безпеки відеоспостереження повинна регулярно переглядатися та актуалізуватися з урахуванням змін потреб і загроз об'єкта.

Розробка стратегії безпеки відеоспостереження має ряд переваг, зокрема:

- Покращує ефективність системи відеоспостереження;
- Зменшує витрати на реалізацію і експлуатацію системи;
- Збільшує безпеку об'єкта.

Стратегія безпеки відеоспостереження є важливим документом, який допомагає забезпечити ефективне використання системи відеоспостереження для забезпечення безпеки об'єкта.

Стратегія безпеки відеоспостереження, як визначено вище, становить фундаментальний компонент для забезпечення безпеки об'єкта. Однак, навіть з найбільш вдосконаленою стратегією, не можна виключити можливість виникнення інцидентів чи загроз, що вимагають негайного втручання. У таких випадках важливо мати чіткі та ефективні рекомендації для виявлення та реагування на інциденти. В цьому контексті, надійна стратегія виявлення та реагування є важливою складовою в цілісній системі безпеки.

Рекомендації для виявлення та реагування на інциденти мають вирішувати ряд завдань, включаючи швидке виявлення аномалій, аналіз інцидентів та негайне прийняття відповідних заходів. Детально розглянуті та ретельно впроваджені

рекомендації допомагають зменшити час реакції на інциденти та максимізувати ефективність введених контрзаходів. Врахування цих аспектів сприяє створенню інтегрованої системи безпеки, яка працює відповідно до стратегічно розробленого плану виявлення та реагування на потенційні загрози.

Виявлення інцидентів у системах відеоспостереження є важливим завданням, оскільки воно дозволяє швидко реагувати на загрози та мінімізувати їх вплив. Огляди безпеки є одним із методів, які використовуються для періодичної перевірки стану обладнання та налаштувань безпеки системи відеоспостереження. Цей підхід спрямований на виявлення ознак інцидентів та забезпечення ефективності системи.

Моніторинг систем може бути налаштований для спостереження за певними подіями, що можуть свідчити про інцидент. Серед таких подій можуть бути зникнення або пошкодження обладнання, зміни в конфігурації обладнання або програмного забезпечення, або зміни в записах відео. Цей метод дозволяє вчасно реагувати на події та пришвидшує виявлення інцидентів.

Аналіз даних з відеопотоку виступає як ефективний інструмент для виявлення інцидентів. Наприклад, використання аналізу відео для виявлення аномалій у поведінці людей чи об'єктів може бути корисним при розкритті потенційних загроз [24].

При виявленні інциденту у системі відеоспостереження важливо негайно вжити заходів реагування. Серед них ізоляція системи, що передбачає відключення від мережі та інших систем для запобігання поширенню інциденту. Збереження даних, пов'язаних з інцидентом, стає важливим етапом для подальшого розслідування та визначення причин та масштабів інциденту.

Розслідування інциденту є необхідним для визначення причин та обставин інциденту. Цей етап допомагає у вдосконаленні системи відеоспостереження та попередженні подібних інцидентів у майбутньому. Після усунення інциденту важливо відновити систему відеоспостереження, забезпечивши нормальне функціонування. План реагування на інциденти є важливим документом, який визначає послідовність дій при виявленні інциденту. Опис інцидентів, ролі відповідальних осіб та послідовність дій у плані допомагають узгоджено та

ефективно реагувати на події. Регулярне оновлення плану гарантує його відповідність до змін у системі відеоспостереження та середовищі безпеки.

Для створення такого плану рекомендовано використовувати таку матрицю (табл. 3.2), яка допоможе внести розуміння до серйозності інциденту. Це допоможе швидко й правильно визначати пріоритети.

Таблиця 3.2 - Матриця визначення серйозності можливих інцидентів

		Наслідок				
		Несуттєвий	Незначний	Помірний	Важливий	Серйозний
Ймовірність	Найбільш ймовірний	Середній	Високий	Дуже високий	Дуже високий	Дуже високий
	Ймовірний	Середній	Високий	Високий	Дуже високий	Дуже високий
	Можливий	Низький	Середній	Високий	Високий	Дуже високий
	Малоймовірний	Низький	Низький	Середній	Середній	Високий
	Винятковий	Низький	Низький	Низький	Низький	Середній

Після чіткого визначення серйозності можливих інцидентів слід розробити чіткий план реагування. Загалом можна виділити основні пункти такого плану:

- Підготовка.
- Виявлення
- Обмеження
- Усунення
- Відновлення
- Аналіз

В реалізації ефективного реагування на інциденти в системах відеоспостереження ключовою є правильна підготовка. Цей етап передбачає

розробку та оновлення планів невідкладних заходів, тренування персоналу та перевірку технічних засобів, готових до використання в разі потреби.

Важливим аспектом є етап виявлення, який визначає процес ідентифікації самого інциденту. Виявлення може включати в себе реакцію на аномалії у системі відеоспостереження, спеціальні події або сигнали, які можуть свідчити про можливі загрози чи порушення безпеки.

На етапі обмеження приймаються заходи для зупинення поширення інциденту та мінімізації його впливу. Це може включати відключення певних частин системи відеоспостереження, ізоляцію вражених областей чи переадресацію трафіку.

Усунення інциденту передбачає кроки для повного вирішення проблеми та відновлення нормальної роботи системи відеоспостереження. Це може включати відновлення пошкоджених частин системи, виправлення програмних чи апаратних вад, а також виключення можливості повторення подібних інцидентів.

Відновлення описує процес повного відновлення функціонування системи після усунення інциденту, включаючи повернення системи в робочий режим та перевірку її продуктивності.

На завершальному етапі аналізу проводиться оцінка інциденту для отримання важливих висновків. Це включає в себе оцінку ефективності плану реагування, виявлення причин інциденту та розробку заходів для попередження подібних ситуацій у майбутньому. Отримані вивчення можуть бути використані для вдосконалення стратегії безпеки відеоспостереження та забезпечення більш ефективного реагування на інциденти.



Рисунок 3.1 – Кроки створення плану реагування на інциденти

Окрім створення планів та стратегій фахівцю з кібербезпеки завжди необхідно постійно навчатися та вдосконалювати свої навички, щоб залишатися в курсі останніх тенденцій і мати можливість ефективно захищати свої організації. Розуміння останніх трендів у сфері кібербезпеки є необхідною умовою для фахівців.

Оскільки кіберзлочинці постійно вдосконалюють свої методи та тактики, фахівцям слід активно слідкувати за оновленнями та новими загрозами. Це вимагає регулярного вивчення нових технологій та методів атак, а також глибокого розуміння попередніх інцидентів. Практичні навички грають ключову роль у компетентності фахівців з кібербезпеки.

Участь у симуляціях та тренувальних вправах дозволяє випробувати свої навички в реальних атакоподібних умовах. Це сприяє не лише збереженню остроти реакції на інциденти, але і розвитку стратегічного мислення та спроможності швидко адаптуватися до нових ситуацій.

Розширення спектру кваліфікацій фахівців охоплює не лише кібербезпеку вузькому розумінні, але й суміжні галузі. Активне вивчення аналізу даних, криптографії, інженерії безпеки та програмування робить їх більш універсальними та готовими вирішувати складні завдання в області захисту інформації.

Організація спільної роботи та обмін досвідом через участь у конференціях, тренінгах та спільних проектах підвищує ефективність команди з кібербезпеки. Відкритий обмін інформацією допомагає виявляти нові підходи до вирішення проблем та підвищує рівень захисту в цілому.

Професійні сертифікації, такі як Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) чи Offensive Security Certified Professional (OSCP), надають визнання та додаткові можливості для розвитку. Участь у хакатонах, де фахівці можуть застосовувати свої навички на практиці, підвищує креативність та ефективність в умовах реальних завдань [22].

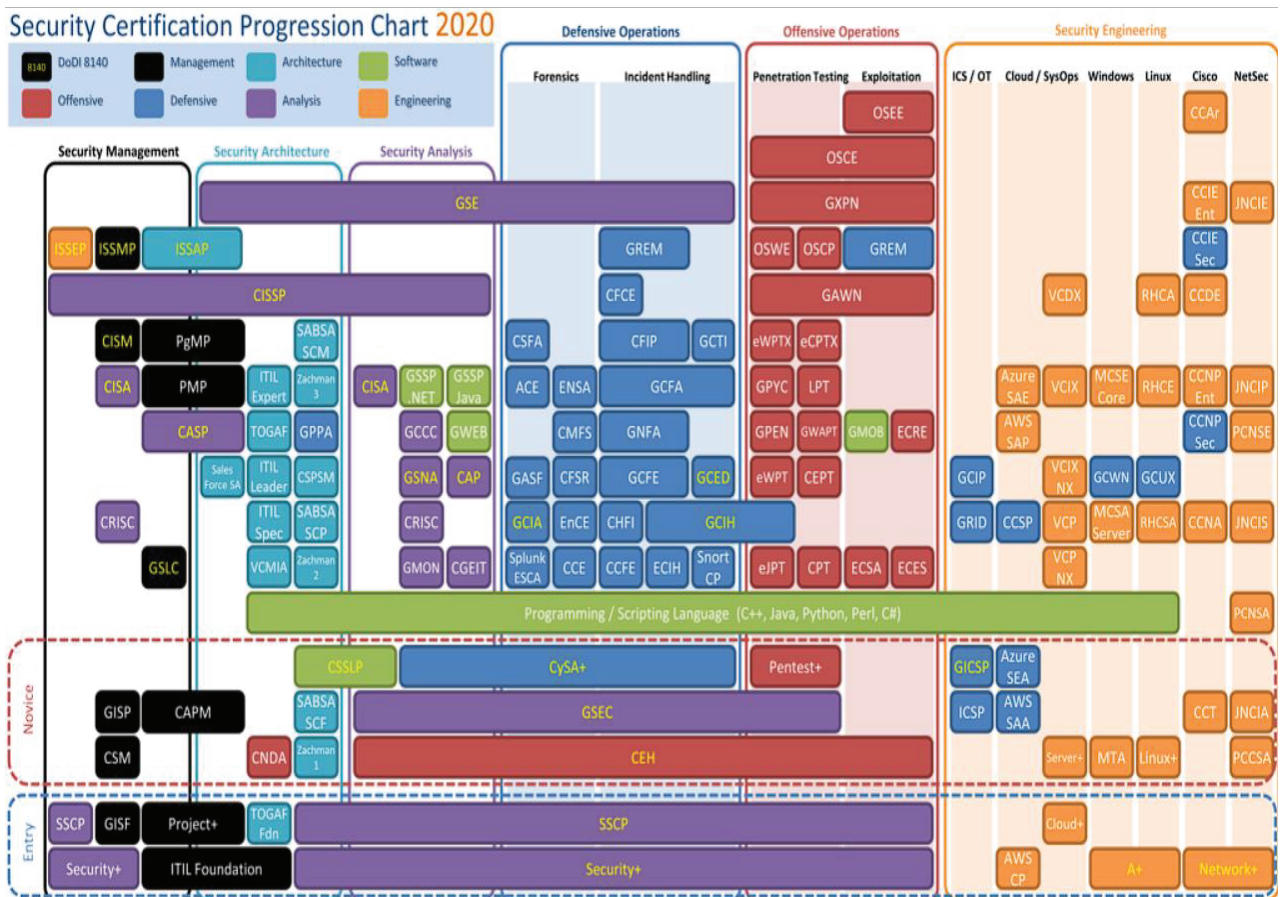


Рисунок 3.2 – Діаграма професійних сертифікацій для фахівців з кібербезпеки та інформаційної безпеки

Курси та конференції, такі як Black Hat і DEFCON, надають можливість зустрічі з провідними експертами галузі, обміну досвідом та ознайомлення з останніми технологічними та стратегічними розробками у сфері кібербезпеки.

Важливо також підкреслити значення самоосвіти, що стає визначальним елементом успішної кар'єри в кібербезпеці. Самостійне вивчення нових технологій, аналіз інцидентів та удосконалення власних навичок завершують образ сучасного фахівця з кібербезпеки, який не тільки пристосовується до змін, але й визначає їх [21].

3.3. Перспективні питання застосування штучного інтелекту та машинного навчання при забезпеченні кібербезпеки та роль глобального співробітництва в системах відеоспостереження

У 2023 році ШІ стає світовим трендом. Він продовжує набирати обертів і ставати все більш поширеним. Організації всіх розмірів і галузей впроваджують ШІ, щоб підвищити свою конкурентоспроможність, ефективність і безпеку. Не оминув ШІ і комп'ютеризовані системи відеоспостереження розкриваючи потенціал для автоматизації завдань та оптимізації використання людських ресурсів.

Однією з конкретних переваг є автоматизація моніторингу, де ШІ використовується для систематичного аналізу відеозаписів. Це дозволяє вчасно виявляти потенційні інциденти безпеки, які можуть бути пропущені людським оператором.

Ще однією важливою можливістю є виявлення і запобігання інцидентам. ШІ застосовується для виявлення аномалій у поведінці об'єктів чи осіб, що допомагає попереджати можливі загрози, такі як крадіжки, вторгнення чи кібератаки. Однією із популярних систем виявлення крадіжок є VaakEye. Система VaakEye, яка вже розгорнута в понад 50 магазинах по всій Японії, постійно відстежує записи з камер безпеки, виявляє підозрілу активність і сповіщає персонал, який може миттєво переглянути відео та вжити заходів [23].

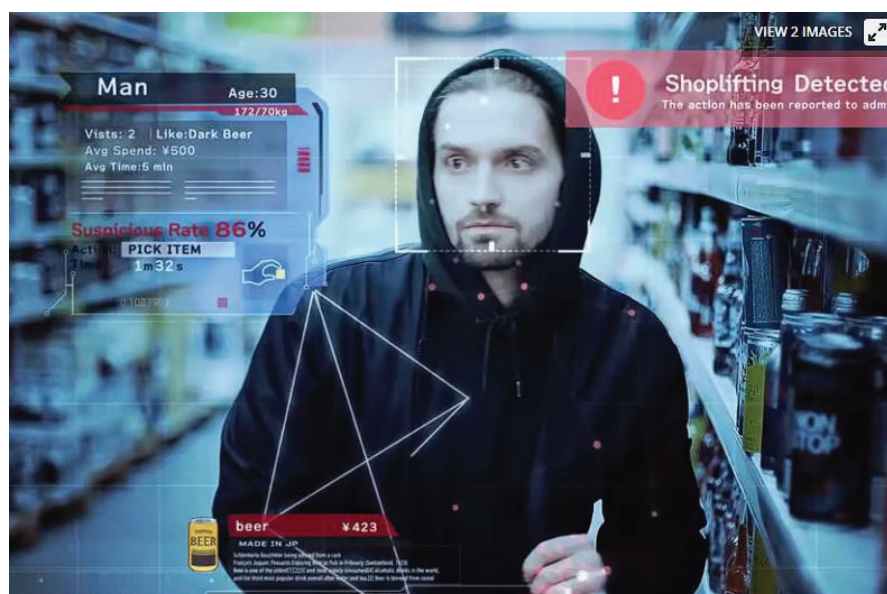


Рисунок 3.3 – Ілюстрації роботи системи VaakEye

Аналітичні здібності ШІ дозволяють проводити глибокий аналіз даних, щоб отримати додаткову інформацію про потенційні загрози. Наприклад, можливість виявлення зв'язків між різними інцидентами дозволяє забезпечити комплексний підхід до забезпечення безпеки.

Досягнення розуміння контексту є ще однією перевагою. ШІ допомагає операторам краще розуміти ситуацію, відображену на відеозаписах, що сприяє більш обґрунтованим рішенням під час виявлення інцидентів.



Рисунок 3.4 – Використання ШІ в аналізі відеопотоку поліцією КНР

Необхідно враховувати, що ШІ, хоч і є потужним інструментом, не є універсальним рішенням. Зловмисники можуть також використовувати ШІ для розробки більш вдосконалених атак. [24] Тому важливо комбінувати використання ШІ з іншими методами безпеки, такими як фізична безпека та участь людських операторів.

У висновку, можна стверджувати, що ШІ має значний потенціал революціонізувати безпеку систем відеоспостереження. Проте важливо бути свідомими потенційних ризиків та вживати заходів для захисту від них, особливо при взаємодії із застосуванням цієї технології. Опираючись на ці факти слід зазначити важливість глобального співробітництва для захисту систем відеоспостереження.

Оскільки системи експлуатуються в різних країнах та регіонах, глобальне співробітництво є ключовим для розробки та впровадження стандартів і законодавства в сфері безпеки систем відеоспостереження. Це досить важливо, так

як більшість систем можуть бути не стандартизовані та не відповідати законодавству різних країн. Так наприкінці 2022 року Велика Британія заборонила використовувати камери (в державних установах та закладах освіти) створені в КНР тому що вважає, що вони містять зловмисний програмний код та бекдори. Також США заборонили використання та продаж відеосистем Hikvision та Dahua на території країни.

Використання систем відеоспостереження може потенційно порушити права людини. Зафіксовані відеокамерами об'єкти можуть стати свідками непередбачених обставин, в результаті чого може виникнути конфлікт із захистом особистих прав та свобод. Глобальне співробітництво в цьому контексті набуває суттєвого значення, оскільки воно сприяє розробці та впровадженню стандартів і законодавства, спрямованих на забезпечення етичного та відповідального використання систем відеоспостереження.

Таке співробітництво має на меті розробку чітких норм, що регулюють обсяг та область застосування відеоспостереження, зокрема враховуючи вимоги до збереження приватності громадян. Глобальні стандарти можуть визначати, як системи відеоспостереження повинні збирати, обробляти та зберігати дані, а також як забезпечувати доступ до них. Це сприятиме уникненню недорозуміння та конфліктів у сфері захисту особистих даних та приватності.

Глобальне співробітництво є ключовим фактором у визначенні балансу між безпекою та захистом особистих прав. Лише шляхом спільних зусиль країн та міжнародних організацій можна створити ефективне правове та етичне рішення, яке гарантує інноваційний розвиток систем відеоспостереження згідно до прав та свобод людини.

3.4. Практична реалізація рекомендацій з усунення вразливостей

Проаналізувавши теоретичну інформацію з попередніх розділів можна змодельовати декілька прикладів можливих атак та навести конкретні рекомендації з усунення можливих вразливостей.

Таблиця 3.3 Сценарій атаки за допомогою використання вразливих паролів

	Опис
Приклад	Адміністратор системи встановлює простий пароль "12345", для доступу до керування системою відеоспостереження.
Сценарій атаки	Зловмисники можуть використовувати перебір паролів або здійснювати атаки "брутфорс" для отримання доступу до системи.
Наслідки	Несанкціоновані особи отримують контроль над системою відеоспостереження, можуть видаляти або змінювати відеозаписи та отримувати доступ до приватних зображень і відео.
Рекомендації з усунення вразливості	Адміністратору слід встановлювати складні паролі не менше 12 символів з яких мінімум одна велика буква, наявні цифри та спеціальні символи. Це значно збільшить час перебору паролю. Також слід створити список доступу до сторінки входу до керування системою відеоспостереження. Ці рішення максимально унеможливають несанкціонований доступ до системи.

Таблиця 3.4 Сценарій атаки MITM

	Опис
Приклад	Зловмисник використовує атаку типу MITM.
Сценарій атаки	Зловмисник отримав доступ до частини мережі в якій знаходиться система(и) відеоспостереження. Можливі сценарії атаки: 1 – зловмисник перехоплює нешифрований трафік в мережі; 2 – зловмисник перехоплює трафік та виконує підміну даних, або ж пасивне прослуховування;
Наслідки	Зловмисник отримавши доступ до мережі, може переглядати, модифікувати конфігурацію обладнання, створювати 1 – отримання доступу до нешифрованого відеопотоку, конфіденційних даних, або ж отримання логіну та паролю до доступу до системи відеоспостереження, вході чого зловмисник отримує доступ до перегляду відео даних та при можливому перехваті логіну та пароля адміністратора системи, зможе вносити зміни в конфігурацію, тощо.; 2 – підміна даних може використовуватись у різних цілях, таких як заміна дійсного відеозапису на інший (вразі фізичного вторгнення на об'єкт, легітимні відеоданні будуть змінені, або ж видалені і не зможуть бути використані, як доказова база), перенаправлення користувача на фішингову сторінку входу до системи контролю системи відеоспостереження, що внаслідку скомпрометує логін та пароль користувача.

Рекомендації з усунення вразливості	1 – слід використовувати належне шифрування даних в мережі; 2 – на кінцевих вузлах слід налаштувати перевірку сертифікатів при вході до важливих систем, блокувати сайти, які використовують http протоколи, додати декілька способів автентифікації.
--	---

Таблиця 3.4 Сценарій атаки через застаріле програмне забезпечення

	Опис
Приклад	Об'єкт використовує системи відеоспостереження Hikvision зі застарілим програмним забезпеченням.
Сценарій атаки	Зловмисник аналізує версію ПО системи та знаходить що данна версія має вразливість CVE-2021-36260 (HSRC-202109-01).
Наслідки	Вразливість дозволяє зловмиснику отримати повний контроль над пристроєм з необмеженою кореневою оболонкою, яка має набагато більший доступ, ніж навіть власник пристрою, оскільки вони обмежені обмеженою "захищеною оболонкою" (psh), яка фільтрує введення до певного набору. обмежених, переважно інформаційних команд.
Рекомендації з усунення вразливості	Своєчасне оновлення програмного забезпечення систем відеоспостереження. Постійний моніторинг CVE всього ПО об'єкту.

Таблиця 3.5 Сценарій атаки через застаріле програмне забезпечення

	Опис
Приклад	Зловмисник отримує фізичний доступ до мережі через підключення до комутатора.
Сценарій атаки	Зловмисник може використати атаки: – DHCP starvation; – VLAN hopping; – Rogue DHCP Server; – CAM-table overflow
Наслідки	При застосуванні атаки DHCP starvation: відмова в обслуговуванні. IP-адреси в просторі закінчилися і нові клієнти не можуть отримати їх. Таким чином користувачі не зможуть взаємодіяти з мережею; VLAN hopping – дозволяє отримувати доступ до інших підмереж (можлива при використанні транкових інтерфейсів в мережі жертви); – підміна DHCP – сервера. Дана атака чудово комбінується з атакою Rogue DHCP Server. Так як на основному DHCP – сервері не залишилось вільних IP – адрес , наступні клієнти отримають їх зі серверу зловмисника; атака CAM-table overflow – або ж переповнення локальної таблиці MAC –адрес [30], реалізується коли таблиця комутації заповнюється і після цього комутатор працює в режимі хабу, тобто після успішної атаки зловмисник перехватує весь трафік в межах широкомовного домену, якому належить цей порт

Рекомендації з усунення вразливості	Для запобігання вразливостям слід вжити наступних заходів: 1 – унеможливити фізичний доступ до мережевого обладнання стороннім особам; 2 – налаштовувати функції безпеки на обладнанні, такі як port-security та dhcp snooping, що не дасть зловмиснику, вичерпати ліміти IP адрес, безкарно змінювати MAC – адреси та дасть змогу обмежувати кількість пакетів на порт та унеможливить зміну DHCP серверу.
--	--

У висновку дослідження було встановлено, що системи відеоспостереження піддаються ряду атак, які можна реалізувати за допомогою різних методів. Щоб захистити системи від атак, необхідно усунути вразливості, які роблять ці атаки можливими. Для цього можна використовувати рекомендації, такі як використання надійних паролів, двофакторна аутентифікація, отримання оновлень програмного забезпечення, встановлення брандмауера та використання антивірусного програмного забезпечення.

ВИСНОВКИ

В даній кваліфікаційній роботі було досліджено можливі вразливості і методи неавторизованого доступу до систем відеоспостереження та надано практичні рекомендації та створення та підтримки конфіденційності, доступності та цілісності інформації у таких системах.

У першому розділі роботи докладно розглянуто основи систем відеоспостереження, надаючи опис їх структури та функцій. Було виокремлено вразливості, які можуть стати об'єктом кібератак, та представлено ретельні методи захисту, спрямовані на підвищення безпеки цих систем.

У другому розділі дослідження було проведено аналіз сучасних прикладів вразливостей в системах відеоспостереження, звертаючи увагу на конкретні випадки та їхні наслідки. Детально розглянуто методи дослідження та виявлення вразливостей, спрямовані на виявлення потенційних загроз. Насамкінець, представлено конкретні заходи, які можуть бути прийняті для запобігання та виправлення виявлених вразливостей в системах відеоспостереження.

У третьому розділі дослідження надано конкретні практичні рекомендації для забезпечення безпеки систем відеонагляду. У першому підрозділі детально розглянуто рекомендації для впровадження систем відеоспостереження, звертаючись до кращих практик та важливих аспектів впровадження. У другому підрозділі, підвищено увагу на рекомендаціях для спеціалістів з інформаційної безпеки, надаючи їм інструменти та стратегії для забезпечення ефективного захисту систем відеонагляду. У третьому підрозділі, розглянуто майбутні напрями та завдання у сфері безпеки систем відеоспостереження, щоб бути в світлі останніх тенденцій та готувати системи до майбутніх викликів. Завершуючи розділ було наведено декілька сценаріїв атак на системи відеоспостереження та практичні рекомендації щодо їх усунення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Поради (рекомендації) щодо створення КСЗІ в ІКС [Електронний ресурс] – Режим доступу до ресурсу: <https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorenniya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet>. Політика інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: <https://atestor.ua/uk/poleznyye-stati/politika-informacii-noyi-bezpeki/>.
2. Hikvision CCTV Camera Types, Specifications [Електронний ресурс] – Режим доступу до ресурсу: <https://www.moglix.com/articles/hikvision-cctv-camera-types-specifications-and-price-list>.
3. Hikvision.org. Hikvision [Електронний ресурс] / Hikvision.org – Режим доступу до ресурсу: <http://hikvision.org.ua/>
4. Video Surveillance [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sciencedirect.com/topics/computer-science/video-surveillance>.
5. What are the cybersecurity issues in video surveillance? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.axis.com/blog/secure-insights/what-are-the-cybersecurity-issues-in-video-surveillance/>.
6. Лабораторія безпеки. securitylab [Електронний ресурс] / Лабораторія безпеки – Режим доступу до ресурсу: <https://securitylab.com.ua/ua/>.
7. Як захистити IP-камери від несанкціонованого перегляду? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.forter.com.ua/yak-zahistiti-ip-kameri-vid-nesankcionovanogo-pereglyadu/>.
8. ПРАВИЛА забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kmu.gov.ua/npas/32791826>.
9. The Village. Ajax Systems [Електронний ресурс] / The Village – Режим доступу до ресурсу: <https://www.the-village.com.ua/village/business/businessmen/279425-business-owners-ajax-systemssecurity-kyiv-kurenivka>.

10. Application Security Testing [Електронний ресурс] – Режим доступу до ресурсу: <https://snyk.io/learn/application-security/static-application-security-testing/>.
11. What Is Security Information and Event Management (SIEM)? Definition, Architecture, Operational Process, and Best Practices [Електронний ресурс] – Режим доступу до ресурсу: <https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/>.
12. Dynamic Application Security Testing (DAST) [Електронний ресурс] – Режим доступу до ресурсу: <https://snyk.io/learn/application-security/dast-dynamic-application-security-testing/>.
13. Principle of Least Privilege [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cyberark.com/what-is/least-privilege/#:~:text=The%20principle%20of%20least%20privilege,perform%20his%20Fher%20job%20functions.>
14. СЛАБКІ МІСЦЯ КОНТРОЛЮ ДОСТУПУ [Електронний ресурс] – Режим доступу до ресурсу: <https://cqr.company/ua/web-vulnerabilities/access-control-weaknesses/>.
15. What are the OWASP top 10 vulnerabilities? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.strongboxit.com/owasp-top-10-vulnerabilities/>.
16. 6 Risks of Running Outdated Systems [Електронний ресурс] – Режим доступу до ресурсу: <https://www.comms-unite.co.uk/news/6-risks-of-running-outdated-systems/>.
17. Metasploit Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.metasploit.com/docs/pentesting/>.
18. Nmap for Pentester: Host Discovery [Електронний ресурс] – Режим доступу до ресурсу: <https://www.hackingarticles.in/nmap-for-pentester-host-discovery/>.
19. Thorough Introduction to OWASP ZAP [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/@pmorr087/thorough-introduction-to-owasp-zap-2e0> What is an Incident Response Plan and How to Create One [Електронний ресурс] – Режим доступу до ресурсу: <https://www.varonis.com/blog/incident-response-plan>.

20. Фахівців з кібербезпеки готуватимуть по-новому [Електронний ресурс] – Режим доступу до ресурсу: <http://www.golos.com.ua/article/339279>.
21. <https://styan.com/cybersecurity-professional-certificates/> [Електронний ресурс] – Режим доступу до ресурсу: Про сертифікати з кібербезпеки.
22. Vaak's AI theft-detection system is already 81% accurate [Електронний ресурс] – Режим доступу до ресурсу: <https://newatlas.com/vaak-vaakeye-ai-theft-detection/59263/>.
23. China's new data privacy law 'will state how facial recognition can be used' [Електронний ресурс] – Режим доступу до ресурсу: <https://www.scmp.com/news/china/politics/article/3114829/chinas-new-data-privacy-law-will-state-how-facial-recognition>.
24. What is a CVE? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.redhat.com/en/topics/security/what-is-cve>.
25. Vulnerabilities [Електронний ресурс] – Режим доступу до ресурсу: <https://owasp.org/www.community/vulnerabilities/#:~:text=A%20vulnerability%20is%20a%20hole,that%20rely%20on%20the%20application..>
26. CVSS (Common Vulnerability Scoring System) [Електронний ресурс] – Режим доступу до ресурсу: <https://encyclopedia.kaspersky.ua/glossary/cvss-common-vulnerability-scoring-system/>.
27. Security Update Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://msrc.microsoft.com/update-guide/vulnerability>.
28. Search Engine for the Internet of Everything [Електронний ресурс] – Режим доступу до ресурсу: <https://www.shodan.io/>.
29. Vakaliuk T., Talchenko D., Osadchyi V., Bailiuk Ye., Pokotylo O. Vulnerabilities and Methods of Unauthorized Gaining Access to Video Surveillance Systems. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, February 28, 2023. Edited by Volodymyr Sokolov, Tamara Radivilova, Vasyl Ustimenko, Mariya Nazarkevych. CEUR Workshop Proceedings, ISSN

1613-0073. Vol-3421, 2023. Pp. 174-181. – Access mode: <https://ceur-ws.org/Vol-3421/short2.pdf>

30. Байлюк Є.М., Покотило О.А. Побудова моделі загроз для атак MAC-Flooding та MAC-spoofing з використанням OWASP Threat-Dragon. Тези доповідей V Всеукраїнської науково-технічної конференції "Комп'ютерні технології: інновації, проблеми, рішення". 01-02 грудня 2022 року. Житомир: «Житомирська політехніка», 2022. С.67-68.