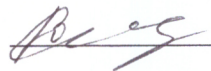


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

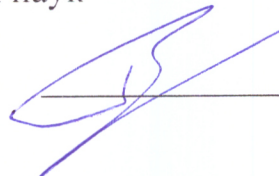
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту системи
відеоспостереження компанії»

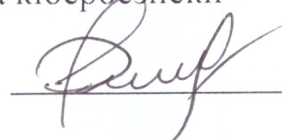
Виконав: студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Єгор ВЕГЕРІН

Керівник: доцент кафедри КІ та КБ, кандидат
технічних наук

 Олександр ПІРОГ

Рецензент: старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Єлизавета ТРОКОЗ

Житомир – 2024

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека»

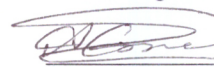
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

«05» 03 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Вегерін Єгор Юрійович

Тема роботи: **«Проект підсистеми захисту системи відеоспостереження компанії»**

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 10 червня 2024 р.

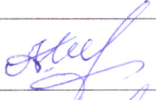
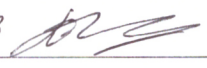
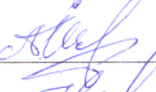
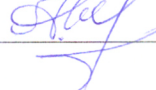
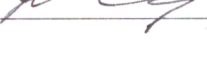
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Захист систем відеоспостереження
2. Протоколи WPA-2 та Radius

Обладнання та програмне забезпечення:

1. Cisco Packet Tracer
2. Операційна система Windows 10, Cisco IOS
3. Топологія мережі

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Шелуха О.О.	 02.03	02.03 
2	Шелуха О.О.	 19.03	19.03 
3	Шелуха О.О.	 01.05	01.05. 

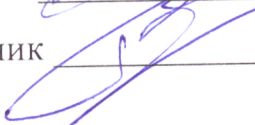
Студент  Єгор ВЕГЕРІН

Керівник  Олександр ПІРОГ

Календарний план

№з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 березня	
2	Розробка плану проекту	2 березня	
3	Вибір програмного забезпечення	4 березня	
4	Пошук теоретичної інформації	26 березня	
5	Розробка проекту	20 квітня	
6	Вибір обладнання	30 квітня	
7	Створення в програмному додатку проекту	15 травня	
8	Створення в програмному додатку схеми для тестування захисту	22 травня	
9	Тестування проекту	28 травня	
10	Оформлення пояснювальної записки	10 червня	

Студент  Єгор ВЕГЕРІН

Керівник  Олександр ПІРОГ

АНОТАЦІЯ

Метою кваліфікаційної роботи є розробка безпечної системи відеоспостереження.

В роботі досліджено основні теоретичних відомостей щодо побудови безпечних систем відеоспостереження, розглянуто типові вразливості систем відеоспостереження та розроблено систему відеоспостереження. Також надано рекомендації щодо підбору компонентів, безпечного налаштування та фізичної безпеки систем відеоспостереження.

Дипломна робота має обсяг 67 сторінок, містить 45 рисунків, 2 таблиці, 26 літературних джерел.

Ключові слова: відеоспостереження, безпека, IP-камери, відеореєстратори, уразливості, віддалений доступ, мережева безпека.

					ДУ «Житомирська Політехніка».22.125.19.000 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Організація захисту інформації в системі відеоспостереження	Літ.	Арк.	Аркушів	
Розроб.		Васерін Є. Ю.		18.06.24					
Керівник		Пірог О.		18.06.24			2	50	
Реценз.		Гракоз Є. М.		18.06.24		ФІКТ, Гр. КБ 20-2			
Н. контр.		Пірог О.		18.06.24					
Затверд.		Васерін Є. Ю.		18.06.24					

ANOTATION

Video surveillance is the foundation of modern security systems. It provides direct monitoring of the territory, helps to prevent intrusions of intruders, detect suspicious activity, identify emergencies and conduct investigations. Analysis of video recordings can help identify intruders, including attempts to connect to the local network in order to steal important information. Technological progress has made IP video surveillance one of the most widespread security solutions. Video surveillance is increasingly being viewed not only as a detection tool, but also as a means of obtaining valuable information about the activities of employees and customers. Video surveillance contains a lot of information, so it has become a source of great threat. The ability to use analytical methods to extract useful information from video data is becoming increasingly important when choosing video surveillance systems. On the one hand, video servers and video cameras are becoming increasingly intelligent due to the growth of processor power.

Nowadays it is very easy to buy video surveillance cameras and video recorders, because they are inexpensive and widely sold. Given this consumer demand, many manufacturers develop new IP cameras, web cameras and video recorders and do not care too much about the details of their protection and vulnerabilities. The most common practice is remote access to video surveillance cameras, since for its implementation it is not necessary to have special software, but you can get by with just a browser and simple manipulations that almost anyone can do. If a person knows how to find the IP addresses of cameras and their vulnerabilities, then he can open up thousands of cameras around the world. Video surveillance systems that are connected to the network allow building distributed systems with the possibility of remote access and wide opportunities for integration with other systems. However, they also have problems related to network security, which are the vulnerability of data and devices.

Keywords: video surveillance, security, IP cameras, video recorders, vulnerabilities, remote access, network security.

ЗМІСТ

АНОТАЦІЯ.....	2
ВСТУП.....	6
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВИКЛАДКИ ЩОДО СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ	8
1.1 Основні поняття та визначення системи відеоспостереження	8
1.2 Покоління систем відеоспостереження.....	10
1.3 Основні компоненти системи відеоспостереження.....	12
1.4 Аналогові системи відеоспостереження	12
1.5 Цифрові системи відеоспостереження	17
РОЗДІЛ 2 ОГЛЯД ВРАЗЛИВОСТЕЙ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ (ВСС)	27
2.1 Атаки на системи відеоспостереження	27
2.2 Атаки з використанням прихованих каналів (Covert Channel Attacks)	30
2.3 Атаки з використанням стеганографії (Steganography Attacks)	31
2.4 Відмова в обслуговуванні та атаки заглушення (Denial of Service and Jamming Attacks).....	34
2.5 Атака шкідливим програмним забезпеченням (Malware Attack).....	35
2.6 Атака з підвищенням привілеїв (Privilege Escalation Attack)	36
РОЗДІЛ 3 ТЕХНІЧНА РЕАЛІЗАЦІЯ ПРОЕКТУ	38
3.1 Вибір системи відіоспостереження	38
3.2 Заходи фізичної безпеки	54
3.3 Розробка фізичної моделі.....	54
3.4 Розробка симулятивної моделі системи відеоспостереження компанії захи-щенної протоколом WPA-2 використовуючи Cisco Packet Tracer	57
ВИСНОВКИ	65
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DVR (Digital Video Recorder)

P2P (Peer-to-peer)

DMZ (Demilitarized Zone)

TPM (Trusted Platform Module)

PKI (Public Key Infrastructure)

CCA (Covert Channel Attacks)

PTZ (Pan-Tilt-Zoom)

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ВСТУП

Актуальність теми. Відеоспостереження – основа сучасної системи безпеки. Воно забезпечує безпосередній моніторинг території, допомагає запобігти проникненням зловмисників, виявити підозрілу діяльність, визначити надзвичайні події та провести розслідування. Аналіз відеозаписів може допомогти виявити зловмисників, зокрема спроби підключення до локальної мережі з метою крадіжки важливої інформації. Технологічний прогрес зробив IP-відеоспостереження одним із найбільш розповсюджених рішень у сфері безпеки. Відеоспостереження все частіше розглядається не тільки як інструмент виявлення, а і як засіб отримання цінної інформації про діяльність співробітників та клієнтів. Відеоспостереження містить багато інформації, тому воно стало джерелом великої загрози. Можливість використання аналітичних методів для вилучення корисної інформації з відеоданих набуває все більшого значення під час вибору систем відеоспостереження. З одного боку, відео сервери та відеокамери стають усе більш інтелектуальними завдяки нарощуванню процесорних потужностей.

У наш час дуже легко придбати камери відеоспостереження і відеореєстратори, тому що вони мають низьку ціну та повсюдно продаються. Ураховуючи цей споживчий попит, багато виробників розробляють нові IP-камери, WEB-камери і відеореєстратори та не занадто піклуються про деталі їх захисту і вразливості. Найпоширенішою є практика віддаленого доступу до камер відеоспостереження, адже для реалізації цього не потрібно володіти спеціальним програмним забезпеченням, а можна обійтися просто браузером і простими маніпуляціями, які може провести майже кожна людина. Якщо особа вміє знаходити IP-адреси камер і їх вразливості, то вона може відкрити для себе тисячі камер у всьому світі. Системи відеоспостереження, які підключені до мережі, дозволяють будувати розподілені системи з можливістю віддаленого доступу та широкими можливостями з інтеграції з іншими системами. Проте їм властиві і проблеми, пов'язані із захищеністю мереж, якими є вразливість даних і пристроїв.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		5

Метою кваліфікаційної роботи є розробка підсистеми захисту системи відеоспостереження компанії.

Встановлена мета визначає наступні завдання:

- дослідження теоретичних відомостей про системи відеоспостереження;
- розгляд вразливостей систем відеоспостереження;
- вибір компонентів системи відеоспостереження;
- надання рекомендацій щодо фізичної безпеки;
- розробка безпечної системи відеоспостереження.

Об'єктом дослідження є процес функціонування системи відеоспостереження їх компоненти та забезпечення їх безпеки.

Предметом дослідження є методи та засоби розробка та забезпечення безпеки функціонування системи відеоспостереження.

Методологія роботи. Під час дослідження було використано загальнонаукові та емпіричні наукові методи, що ґрунтуються на системному підході, такі як абстрагування, аналіз, синтез, порівняння, узагальнення, систематизація та моделювання.

Практичне значення отриманих результатів. Результати роботи можуть бути використані під час розробки систем відеоспостереження.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних літературних джерел. Основний зміст роботи викладено на 66 сторінках друкованого тексту. Робота містить 1 таблицю та 40 рисунків. Список використаної літератури налічує 49 джерел, що викладені на 3 сторінках.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВИКЛАДКИ ЩОДО СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Основні поняття та визначення системи відеоспостереження

CCTV, або система відеоспостереження закритого контуру, – це телевізійна система, яка не транслює сигнали для загального доступу, а передає їх на обмежену кількість моніторів. Система відеоспостереження зазвичай використовує відеокамери CCD (для запису відео), кабельні або бездротові передавачі/приймачі або Інтернет (для передачі відео) та монітори (для перегляду відео).

Система відеоспостереження застосовується не тільки для цілей безпеки та спостереження, але й в інших сферах, таких як лабораторії в школах або приватних компаніях, а також на виробничих лініях на заводах. Зі зростанням застосування систем відеоспостереження, індустрія відеоспостереження розробила різноманітне обладнання, таке як віореєстратори з таймлапс-функцією, комбайнери, інфрачервоні освітлювачі тощо. Останнім часом розроблено веб-камерний сервер, який використовує Інтернет для дистанційного спостереження.



Рисунок 1.1 – Системи відеоспостереження

Насправді, найперше використання системи відеоспостереження (CCTV) припадає на 1942 рік, коли її вперше застосували військові в Німеччині. Вони використовували дистанційні камери з чорно-білими моніторами для спостереження за запуском ракет V2. У 1940-х роках військові США також використовували відеоспостереження під час розробки та випробувань атомної зброї, оскільки це дозволяло їм спостерігати за тестами з безпечної відстані.

З того часу відеоспостереження стало дуже поширеним не тільки на військових, а й на цивільних об'єктах. У 1970-х та 1980-х роках відеоспостереження широко використовувалося як додатковий захід безпеки в банках. Багато інших роздрібних торговців також почали використовувати ці системи у своїх магазинах як метод запобігання злочинам та їх фіксації. Відеокамери користуються особливою популярністю в магазинах біля дому та на автозаправках.

На автозаправках їх використовують для запису зображень водіїв, які залишають станцію, не сплативши за паливе. Немає чітких доказів того, що відеоспостереження знижує рівень злочинності, але воно є дуже ефективним засобом для затримання злочинців, яких було зафіксовано під час скоєння злочину. Системи відеоспостереження також стали дуже корисними для моніторингу дорожнього руху. Першою країною, яка почала використовувати їх для цієї мети, була Великобританія. Тисячі камер були встановлені по всьому місту для спостереження за дорожнім рухом та фіксації аварій.

З того часу їх почали розміщувати в транспортних засобах, таких як таксі, автобуси та потяги. Їх також встановлюють у приватних зонах, наприклад, на парковках, щоб зменшити кількість випадків вандалізму. У 1990-х роках деякі міста США та Канади використовували ці системи відеоспостереження для відстеження порушників правил дорожнього руху. Порушникам автоматично надходили штрафи після того, як їх зафіксували на камеру.

Сьогодні відеоспостереження дуже поширене в оселях. Багато будинків, обладнаних системами безпеки, мають камери відеоспостереження як додатковий

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

засіб захисту від злому або небажаних гостей. Їх також використовують у багатьох громадських місцях, включаючи школи та аеропорти, для запису підозрілої діяльності.

Ці камери також зазнали змін з роками. Колись вони були великими білими коробками, які не могли збільшувати або зменшувати зображення чи стежити за об'єктами. Сьогодні вони можуть бути маленькими та непомітними. Вони мають багато передових функцій, включаючи високу роздільну здатність та можливість виявляти та відстежувати рух у місцях, де його не повинно бути.

1.2 Покоління систем відеоспостереження

Системи відеоспостереження першого покоління (1GSSs) (1960-1980 рр.) використовують аналогові технології для моніторингу оточення. Відеодані з кількох камер передавалися до контрольної кімнати, де оператори-люди спостерігали за обстановкою за допомогою телеекранів. Недоліками цих систем є:

- Значна ймовірність пропуску важливих подій через обмежену увагу операторів.

- Складність аналогового відеозв'язку (високі вимоги до пропускної здатності, низька гнучкість розподілу та неефективне розподілення та зберігання зображень).

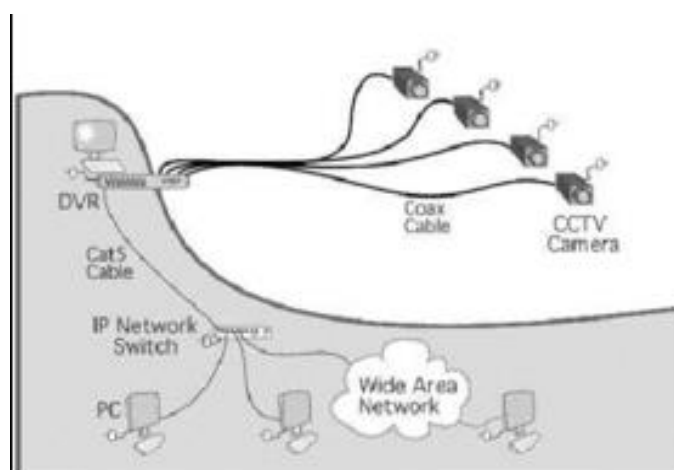


Рисунок 1.2 – Системи відеоспостереження 2 покоління

Системи відеоспостереження другого покоління (2GSSs) (1980-2000 рр.) мають переваги над системами 1GSSs, оскільки 2GSSs використовують технології раннього розвитку цифрових відеокомунікацій. «Більшість дослідницьких зусиль у період 2GSSs були спрямовані на розробку автоматизованих методів виявлення подій у режимі реального часу для відеоспостереження. Наявність автоматизованих методів значно полегшила б моніторинг великих об'єктів із кількома камерами, оскільки автоматичне виявлення подій дозволяє попередню фільтрацію та відображення основних подій.»

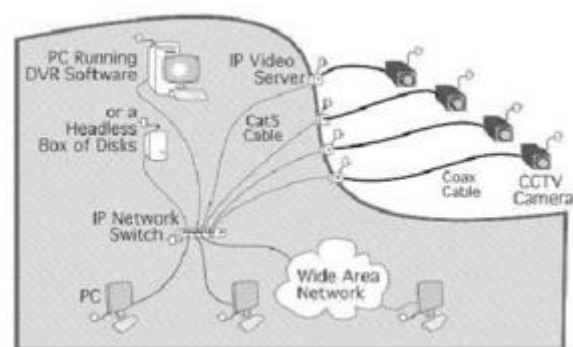


Рисунок 1.3– Системи відеоспостереження 3 покоління

Системи відеоспостереження третього покоління (3GSSs) (з 2000 року по теперішній час) – це сучасне покоління, яке використовує лише цифрові компоненти. Більше того, вони орієнтовані на роботу з великою кількістю камер для охоплення великих територій, розподіл обчислювальних потужностей та об'єднання різних типів датчиків (мікрофони, тепловізійні камери тощо). Головна мета – полегшити та зробити більш ефективним обмін даними, керування ними та виявлення подій у відео з великої кількості датчиків в режимі реального часу. «Основними сферами застосування 3GSSs є сфери громадського моніторингу. Це зумовлено швидким зростанням великих міст та зростаючою потребою у забезпеченні підвищеної безпеки для населення.»

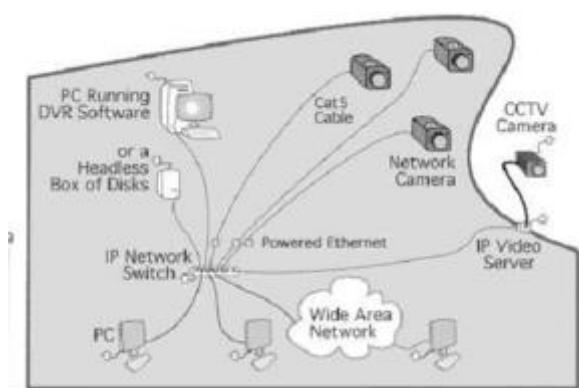


Рисунок 1.4 – Системи відеоспостереження 2 покоління

1.3 Основні компоненти системи відеоспостереження

Зовнішній вигляд повної системи відеоспостереження може сильно відрізнятися. Проте, існує ряд базових компонентів, які завжди повинні бути присутніми.

Перший і, ймовірно, найважливіший компонент - це камера. Без гарної камери вся система втрачає сенс. Неважливо, наскільки хороше інше обладнання системи, оскільки якщо камера забезпечує зображення низької якості, вся система марна.

Наступною дуже важливою частиною системи є відеомагнітофон (ВМ). ВМ повинен записувати зображення, що надходять з камери. Для збільшення тривалості запису на одній касеті багато відеомагнітофонів використовують технологію таймлапс (запис з прискореною швидкістю).

1.4 Аналогові системи відеоспостереження

Аналогові системи існують уже досить давно, і розробники досі намагаються вичавити з них максимум. Завжди є що покращити, і саме тому багато компаній все ще виробляють аналогові системи, оскільки чимало користувачів на ринку досі їх використовують.

Замість того, щоб інвестувати в абсолютно нову цифрову систему, вони дотримуються аналогової версії та час від часу оновлюють її, щоб підтримувати якість роботи. У цьому розділі буде представлено опис простої аналогової

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

системи. На малюнку 1.5 зображена базова аналогова система відеоспостереження.

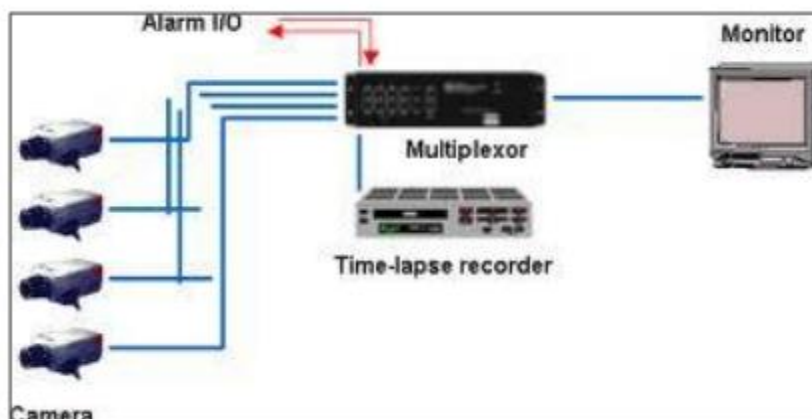


Рисунок 1.5 – Аналогові системи відеоспостереження

Камера, ймовірно, є найважливішою частиною системи відеоспостереження. Без гарної камери вся система транслюватиме зображення лише низької якості.

Обговорюючи аналогові камери, ми часто маємо на увазі камери з аналоговим виходом, проте всередині камери все ж таки часто присутні схеми цифрової обробки сигналу. Камера є лише частиною цілої системи, коли ми говоримо про неї, ми маємо на увазі камеру разом з об'єктивом.

Завдання об'єктива полягає в тому, щоб світло від джерела освітлення відбивалось від об'єкта зйомки. Об'єктив збирає світло зі сцени та формує її зображення на чутливому до світла сенсорі камери. Потім сенсор камери перетворює видиму сцену, сформовану об'єктивом, в електричний сигнал, придатний для передачі на віддалений монітор і відеомагнітофон.



Рисунок 1.6 – Камера Відеоспостереження

Відеомонітор або дисплей комп'ютера (ЕПТ, РК-дисплей або плазмовий) відображає зображення з камери, перетворюючи електричний відеосигнал назад у видиме зображення на екрані монітора. На малюнку 1.7 зображено ЕПТ-монітор із кнопками регулювання.

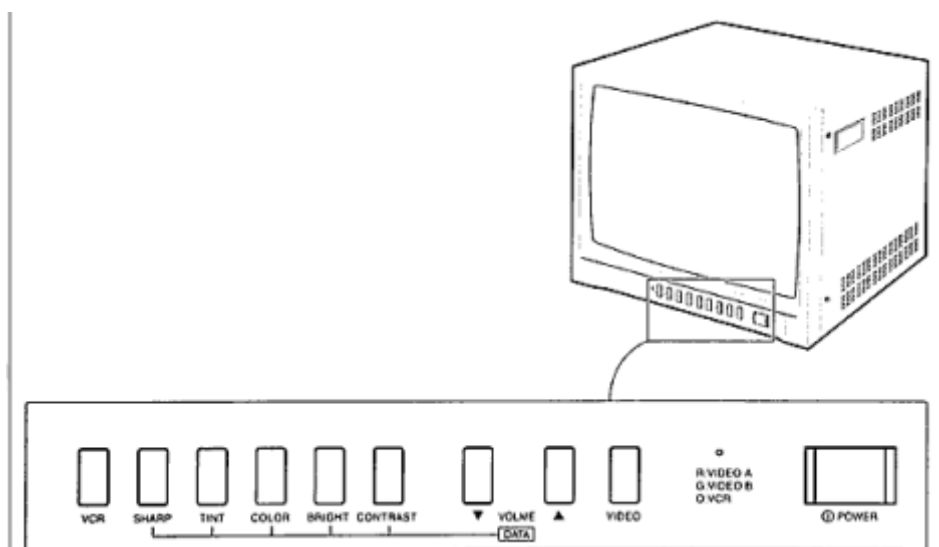


Рисунок 1.7 –Монітор відеоспостереження

Для збереження зображень, знятих камерою, система використовує відеомагнітофон (ВМ) із касетами. ВМ зберігає зображення на відеокасетах, які потім можна архівувати та використовувати для відтворення пізніше. Важливо, щоб ВМ був високої якості, щоб збережені зображення відповідали якості оригіналу, знятого камерою. Тому ВМ повинен мати можливість працювати з високою роздільною здатністю, що означає велику кількість телевізійних рядків. Відеомагнітофон також має бути дуже надійним, щоб не зупинятися раптово та не псувати відеокасети.

Іноді в системах відеоспостереження використовують два незалежні відеомагнітофони для резервного копіювання на випадок несправності. Використання двох ВМ також може бути способом уникнення зупинок під час заміни відеокасет. Великою проблемою відеомагнітофонів є те, що час від часу потрібно міняти касети.

Відеомагнітофони в системах відеоспостереження можуть бути дуже різними. Існують як ВМ, що використовують касети, аналогічні тим, які використовуються в домашніх відеомагнітофонах, так і більш просунуті моделі. Єдина причина, чому відеомагнітофони для відеоспостереження використовують інші типи касет, полягає в тому, щоб вони могли пропонувати більш тривалий час запису.



Рисунок 1.8 – Відеомагнітофон

Лінія передачі передає електричний відеосигнал від камери до віддаленого монітора. Ось варіанти дротового носія сигналу:

- (а) Коаксіальний кабель
- (б) Неекранована вита пара (UTP)
- (в) Волоконно-оптичний кабель
- (г) Локальна мережа (LAN)
- (д) Глобальна мережа (WAN)
- (е) Внутрішня мережа (інтранет)
- (ж) Мережа інтернет

Варіанти бездротової передачі:

- (а) Радіочастота (RF)
- (б) Мікрохвильовий зв'язок
- (в) Оптичний інфрачервоний (ІЧ) діапазон

Сигнали можуть бути аналоговими або цифровими

Для підвищення гнучкості системи існує безліч різних продуктів. Одним із продуктів, який часто використовується для доповнення існуючої системи та її

налаштування, є мультиплексор. Мультиплексор є обов'язковим елементом, якщо система повинна мати більше однієї камери.

Мультиплексор пропонує різноманітні функції, але найважливішою, ймовірно, є можливість підключати багато камер до одного відеомагнітофона та/або одного монітора. Мультиплексори мають різні конфігурації, але часто вони дозволяють підключати щонайменше чотири камери як вхідні канали. Однак існують мультиплексори, які можуть пропонувати до 32 або більше різних вхідних каналів.

Впровадження мультиплексорів у сферу відеоспостереження було справді важливим кроком. Раніше одна камера підключалася до одного відеомагнітофона, а потім з'єднувалася з монітором або навпаки. Мультиплексор часто має багато вхідних і вихідних можливостей. Існує безліч варіантів налаштування під час роботи з системою відеоспостереження. На малюнку 2.3 зображена типова аналогова система відеоспостереження, що показує всі компоненти з мультиплексором.

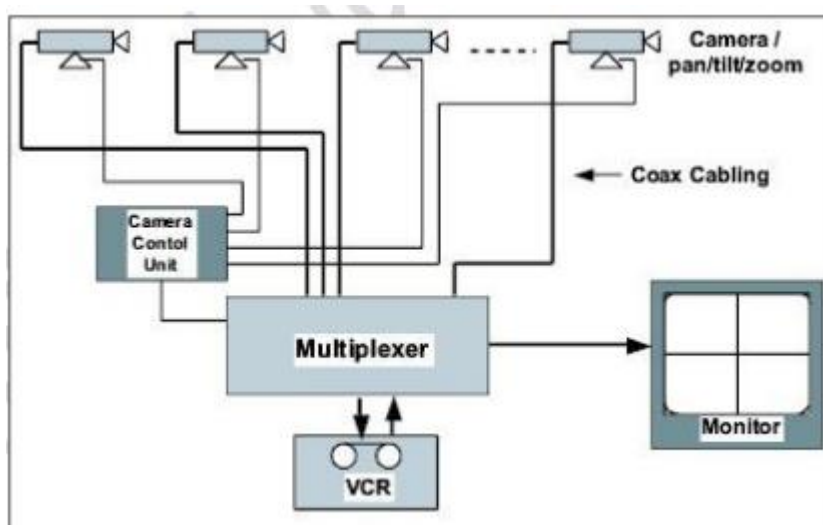


Рисунок 1.9 – Мультиплексор

1.5 Цифрові системи відеоспостереження

На відміну від аналогових систем, у цифрових системах відеоспостереження майже все обладнання використовує цифрову технологію замість аналогової. Але це твердження справедливе лише частково, оскільки в деяких елементах обладнання все ще використовується аналогова електроніка. Базова цифрова система відеоспостереження має ті ж самі основні компоненти, що й аналогова, але, звичайно, різні компоненти використовують цифрову технологію.

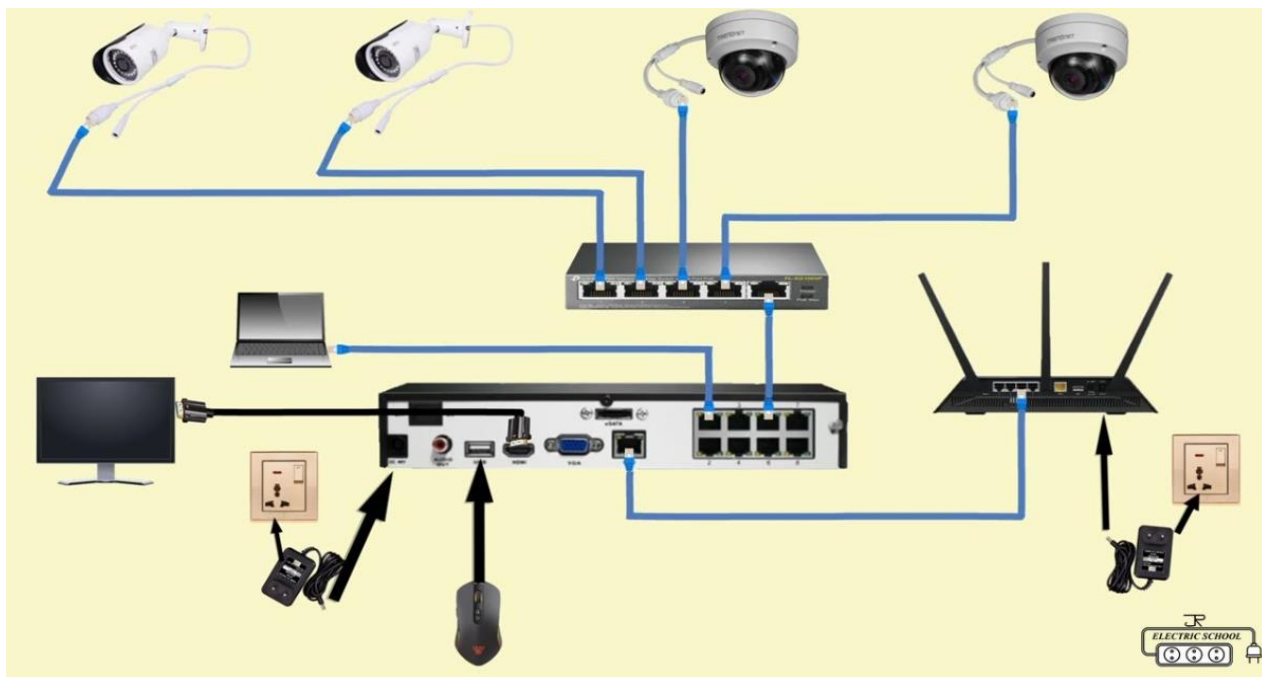


Рисунок 1.10 – Цифрові системи відеоспостереження

Цифрова камера значно відрізняється від аналогової. Але спільним для обох є використання об'єктивів. Часто об'єктив і корпус камери купуються окремо. Таким чином, легше налаштувати всю камеру відповідно до конкретних потреб. Цифрові камери в системах відеоспостереження використовують ту саму технологію, що й портативні цифрові камери, які сьогодні є майже у кожної людини. Але суттєва відмінність полягає в тому, що камери відеоспостереження часто є більш надійними, оскільки вони піддаються значно суворішим умовам експлуатації.

У цифровій камері світло проходить через об'єктив, як і в аналоговій. Але на цьому схожість з аналоговою камерою закінчується. Для перетворення світла на

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

цифрове зображення використовується елемент CCD (ПЗЗ - прилад із зарядовим зв'язком) або датчики CMOS (додаткова метал-оксид-напівпровідникова структура).

CCD-елемент схожий на маленький фотометр, який визначає інтенсивність світла та відображає її пропорційною аналоговою напругою. Для отримання цілого зображення багато CCD-елементів розміщуються разом у масиві. Один CCD-елемент відповідає одному пікселю. Таким чином, якщо масив CCD складається з масиву 1024*768 елементів, це також є найвищою роздільною здатністю (у пікселях), яку зрештою запропонує камера.

У 1998 році датчики CMOS почали використовуватись у цифрових камерах замість елементів CCD. Причиною стало те, що датчики CMOS дешевше виробляти, ніж CCD, а також те, що вони споживають менше енергії для належної роботи. Ще однією перевагою використання CMOS замість CCD була більша можливість налаштування параметрів зображення на ранній стадії.

Цей тип камери фактично є цифровою, але замість того, щоб мати цифровий (двійковий) сигнал на виході, сигнал перетворюється в аналоговий. Звісно, це означає, що сигнал буде більш зашумленим, але така камера в багатьох аспектах перевершує традиційну аналогову камеру.

Вона може використовувати всі переваги цифрової камери, такі як оброблення сигналу, і при цьому пропонувати аналоговий вихід. Такі камери часто використовують, коли компанії хочуть модернізувати свої аналогові системи відеоспостереження, але не хочуть замінювати все обладнання на дорогі цифрові пристрої.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.11 – Камера з цифровою технологією

В цифровій системі відеоспостереження всі зображення є цифровими, мають певну роздільну здатність та розмір. Для зберігання цих зображень більше не можна використовувати старий відеомагнітофон, натомість використовується цифровий відеореєстратор (DVR). DVR часто пропонує високі технології та багато функцій.

Найпоширеніший спосіб підключення камери до DVR - через мережевий кабель. Перевагою DVR є те, що зображення зберігаються на жорсткому диску, а не на відеокасеті. Таким чином, немає необхідності міняти носії запису. Коли жорсткий диск заповнюється, DVR повинен почати видаляти зображення або просто перезаписувати старі. Щоб зберігати якомога більше зображень, DVR повинен бути оснащений великими жорсткими дисками. Хоча зараз жорсткі диски стають дедалі дешевше, DVR часто постачаються з досить маленьким об'ємом пам'яті. Тому можна додатково придбати жорсткий диск, який можна встановити в DVR або підключити через інтерфейс, наприклад, SCSI-з'єднання, FireWire або USB 2.0.

Компанії, що продають DVR, часто намагаються заробити на них додаткові кошти, використовуючи власні розроблені інтерфейси. Таким чином, клієнтам доводиться купувати їхні продукти, коли вони хочуть збільшити кількість

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

жорстких дисків. Але в багатьох випадках стандартний жорсткий диск, такий самий, як у звичайному ПК, цілком підійде.

Під час розрахунку кількості зображень, які помістяться на жорсткий диск DVR, враховується не тільки його розмір. Також важливий розмір зображень та швидкість їх запису. Як уже згадувалося раніше, запис в реальному часі вважається записом із 30 кадрів/сек (fps) для NTSC та 25 кадрів/сек (fps) для PAL. Таким чином, існує велика різниця між записом в реальному часі та записом з 20 кадрами/сек.

Наприклад, припустимо, що в DVR встановлено жорсткий диск на 60 ГБ. Камера налаштована на захоплення 30 кадрів/сек, тоді кожне зображення має розмір 52 КБ (приклад із зображенням JPEG із роздільною здатністю 704x576 пікселів). Скільки часу тоді прослужить жорсткий диск?

Розрахунок тривалості запису (альтернативний спосіб):

1. Швидкість передачі даних відеопотоку:

- Швидкість передачі: $30 \text{ кадрів/сек} * 52 \text{ КБ/кадр} = 1560 \text{ Кбіт/сек}$
- Перетворення Кбіт/сек в МБ/сек для порівняння з розміром жорсткого диска: $1560 \text{ Кбіт/сек} / (1024 \text{ Кбіт/Мбіт}) = 1,56 \text{ Мбіт/сек}$

2. Тривалість запису на жорсткий диск 60 ГБ:

- Тривалість запису: $60 \text{ ГБ (ємність жорсткого диска)} / 1,56 \text{ Мбіт/сек (швидкість передачі)} = 38461 \text{ секунд}$

3. Перетворення секунд в години та хвилини:

- Тривалість запису: $38461 \text{ секунд} / 60 \text{ секунд/хвилина} = 641 \text{ хвилина}$
- Тривалість запису: $641 \text{ хвилина} / 60 \text{ хвилин/година} = 10,7 \text{ годин}$

Таким чином, жорсткий диск на 60 ГБ в цьому прикладі прослужить приблизно 10,7 годин запису в реальному часі (30 кадрів/сек). Збільшення швидкості запису або розміру зображення зменшить тривалість запису.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.12 – Цифровий відеореєстратор

Так само, як аналогову систему можна розширити, цифрові системи пропонують багато різних можливостей для створення складнішого рішення. І найкращий спосіб зберігати зображення, зняті камерою, – це використовувати сервер зображень на базі звичайного комп'ютера.

Сервер зображень – це пристрій із великими можливостями зберігання даних. Насправді, сервери – це просто звичайні комп'ютери. Єдина додаткова потреба – це програмне забезпечення для налаштування передачі зображень з різних камер та визначення того, що з ними робити після отримання. Комп'ютер повинен мати значний об'єм жорсткого диска, дуже гарну мережеву карту, швидкий процесор та багато оперативної пам'яті.

Це рішення значно дешевше як придбати, так і модернізувати. Якщо програмне забезпечення застаріває, його легко оновити, просто придбавши краще. Це набагато дешевше, ніж купувати нове обладнання, як у випадку із серверами зображень, не побудованими на стандартних комп'ютерах. Якщо раптом місця на

жорсткому диску стане замало, потрібно придбати нові, що на сьогоднішній день дуже дешево, оскільки комп'ютерна індустрія велика, а конкуренція жорстка.

Велика перевага сервера зображень на базі ПК полягає в тому, що немає секрету щодо того, що знаходиться всередині машини. Легко купувати нові деталі та модернізувати систему. Також недорого придбати новий комп'ютер, коли старий стане нездатним ефективно керувати системою.

Можливо, найкращий спосіб використання сервера зображень – це його спільне використання з DVR-ами. Один DVR можна розмістити локально біля кожної камери, а потім сервер зображень можна розмістити в більш централізованому місці. Всі DVR-и потім підключаються до інтернету, а також до сервера зображень.

Потім сервер зображень можна налаштувати на завантаження всіх зображень або лише певних зображень за заздалегідь визначеним графіком. Розумним рішенням є передавати зображення з DVR-ів на сервер зображень вночі, оскільки в цей час в інтернеті менше трафіку. Для передачі зображень DVR-и та сервер зображень використовують FTP-сервер. Таким чином, зображення передаються швидко, легко та безпечно.

Завдяки такій роботі системи її значно легше контролювати. Зображення завжди потрапляють на сервер зображень, і тоді відповідальні особи можуть переглянути матеріали, не відчуваючи тиску через те, що DVR переповнений зображеннями, і деякі з них потрібно буде стерти або зупинити DVR.



Рисунок 1.13 –Сервер зберігання зображень

Сьогодні точиться жвава дискусія щодо того, чи система відеоспостереження (CCTV) повинна бути цифровою чи аналоговою. Більшість експертів стверджують, що всі системи відеоспостереження стануть цифровими в майбутньому, але враховуючи стан ринку сьогодні, використання аналогових або цифрових систем залежить від того, де ця система буде встановлена.

Наприклад, має велике значення, чи система повинна мати камери зовні чи всередині будівель, і чи повинні камери використовуватися вдень чи вночі. Легко сказати, що слід використовувати цифрові системи, оскільки зараз усе переходить на цифровий формат, але й досі багато аналогових систем можуть забезпечити дуже добрий результат. На сьогоднішній день встановлення справді хороших цифрових систем коштує цілий статок. Тому багато компаній обирають використання дешевших цифрових систем або більш досконалих аналогових систем.

Але можливо, найкраща система складається як з аналогового, так і з цифрового обладнання, як своєрідний гібрид, зображений на малюнку

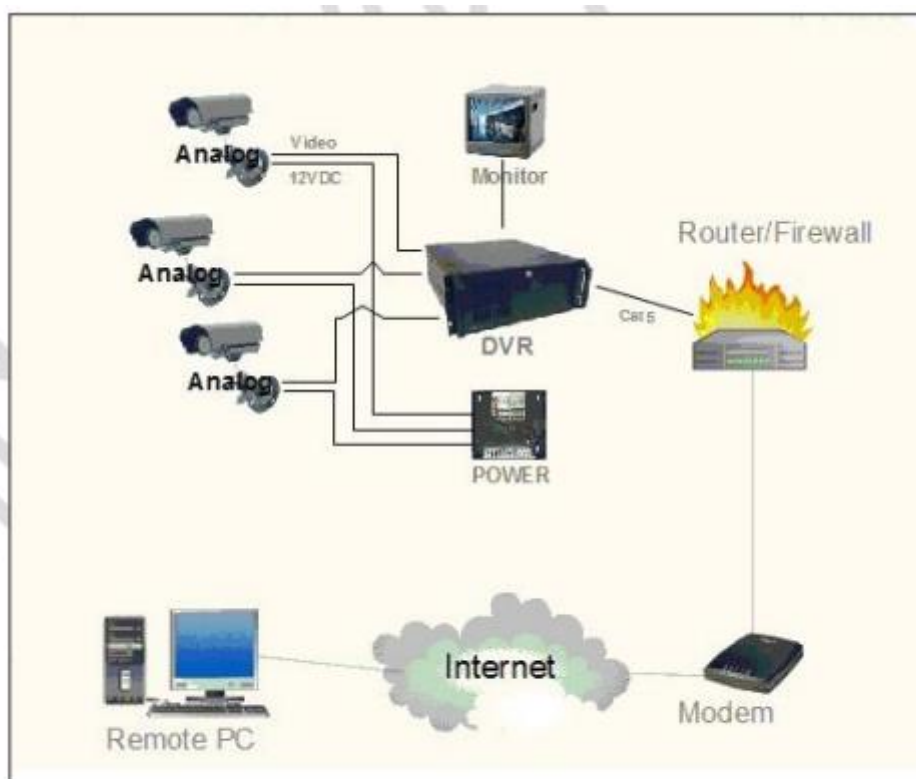


Рис 1.14 - Гібридні системи

Рисунок 1.14 – Гібридні системи

Для того, щоб система була легкою для розширення або модифікації в майбутньому, її основні компоненти повинні базуватися на цифрових технологіях. Єдина аналогова частина, яку досі дійсно цікаво використовувати, – це камера. Всі інші компоненти системи насправді повинні бути цифровими.

Причина використання аналогової камери полягає в тому, що вона забезпечує значно краще зображення за умов слабкого освітлення, ніж цифрова камера. Звісно, існують цифрові камери, які забезпечують дуже хороші зображення за дуже низьких значеннях освітленості, але вони все ще дуже дорогі.

Для перетворення аналогового сигналу в цифровий та для можливості використання аналогової камери використовується відеосервер. Відеосервер має можливість підключення до інтернету через веб-сервер. Часто відеосервер має принаймні чотири канали. Зображення можна потім переглядати безпосередньо, отримавши доступ до відеосервера.

Дискусія щодо гібридної аналогово-цифрової системи, описана вище, базується на тому, що система буде встановлюватися з нуля. Але часто компанії стикаються з абсолютно іншою проблемою. Вони вже мають встановлену аналогову систему відеоспостереження. Тоді вони хочуть розширити систему або якось підвищити її продуктивність. Питання полягає в тому, як це зробити.

Компанія хоче інвестувати гроші в систему, яка прослужить багато років, але вона відчуває велику проблему, оскільки базова система є аналоговою. Найкращий спосіб поступового розширення та зміни системи для її майбутньої надійності – це покрокове перетворення системи в цифрову.

Ймовірно, першим кроком буде заміна старого відеомагнітофона (VCR) на цифровий відеореєстратор (DVR). Встановлення DVR також означає, що частина системи буде базуватися на мережі. DVR можна підключити до інтернету, а це означає, що користувачі можуть увійти до DVR та переглядати відеопотік з камери або записаний матеріал, який зберігається на жорсткому диску DVR.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

Після встановлення DVR дуже легко підключити цифрові камери напряму або через комутатор до DVR. Оскільки DVR підключено до інтернету, тепер також можна встановити сервер зображень, на який можна передавати зображення з DVR. Також можна додати звичайні ПК, щоб спростити керування системою.

Наступний крок – позбутися мультиплексорів та встановити замість них відеосервер, щоб і надалі можна було використовувати аналогові камери. Останній крок, щоб повністю позбутися старого аналогового обладнання, – це встановлення цифрових камер.

Таблиця 1.1

Порівняння цифрових та аналогових систем

Аналогові камери		Цифрові камери
Камери	Перевірена та надійна, але обмежена роздільною здатністю PAL або NTSC з чересстрочною разверткою.	Доступні з широким спектром датчиків CCD та CMOS. Краща робота за слабкого освітлення. Великий вибір: від дешевих веб-камер з низькою роздільною здатністю до мегапіксельних камер з опціями бездротової передачі, живлення по Ethernet (POE), аналітики тощо.
Встановлення	Потрібен окремий коаксіальний або оптоволоконний кабель для кожного з'єднання, окремі кабелі для живлення та керування. Для більших відстаней потрібні підсилювачі.	Просто підключіть камеру до мережі та налаштуйте її мережеві параметри. Один мережевий кабель можна використовувати для відео, даних і живлення.
Розширення системи	Складне. Кожна аналогова камера потребує власного кабелю. Якість зображення знижується при використанні довгих кабелів.	Підключіть додаткові пристрої до мережі та додайте їх до програмного забезпечення NVR.
Запис відео	Відео зберігається на відеокасетах VHS, які потребують постійної заміни та великого місця для зберігання. Якість записаного відео з часом погіршується.	Оцифровані зображення записуються на масиви жорстких дисків, що забезпечує легке керування та пошук. Відео можна копіювати без втрати якості.
Експорт	Фізичні касети можна легко передати як докази поліції, а стандартний формат SVHS гарантує легке відтворення. Однак якість знижується при копіюванні касет.	Робоча копія є точною копією оригінального запису. Процес експорту може бути повільним і громіздким. Стандартного формату експорту немає, тому потрібна програма-програвач.
Стійкість до несправностей	Дуже обмежена.	Гнучкі можливості для різних рівнів стійкості до несправностей для зберігання, передачі даних по мережі та керування системою.
Стандарти	Добре встановлений стандарт відеосигналу, але в іншому випадку залежить від виробника.	Міжнародні IT-стандарти для стиснення та передачі відео. Стандарти, що розвиваються (ONVIF, PSIA) для взаємодії пристроїв.

Системна платформа	Фірмове обладнання, інфраструктура та операційна платформа, призначені спеціально для відеоспостереження.	Стандартне ІТ-обладнання, операційні системи, мережа та сховище.
Підключення	Спеціалізовані кабелі типу "точка-точка" з дуже обмеженими можливостями для віддаленого доступу або розподілених систем.	Можливість використання існуючої локальної мережі або виділеної мережі. Практично необмежена гнучкість підключення через локальну мережу, WAN або Інтернет.
Відеоаналітика / ANPR (автоматичне розпізнавання номерних знаків)	Окрема додаткова система з обмеженими можливостями інтеграції. Базова відеоаналітика може виконуватися цифровим сигнальним процесором (DSP) кодера.	Програмна платформа дозволяє інтегрувати інформацію про тривоги та метадані аналітики.

Висновки за 1 розділ : Під час роботи з цим розділом мною було розглянуто : що таке системі відеоспостереження , які покоління систем відеоспостереження існують, з яких компонентів будуються системи відеоспостереження та що таке аналогові та цифрові системи відеоспостереження та їх порівняння.

РОЗДІЛ 2 ОГЛЯД ВРАЗЛИВОСТЕЙ СИСТЕМ ВІДЕОПОСТЕРЕЖЕННЯ (ВСС)

2.1 Атаки на системи відеоспостереження

Таблиця 2.1 – Атаки на відеосистеми

Рік	Місце/Пристрій	Виробник	Опис
Вересень 2016	Французький веб-хостинг OVH	-	DDoS-атака Mirai [4] - найбільша DDoS-атака на той час, потужність понад 600 Гбіт/с, спрямована на пристрої Інтернету речей, включаючи маршрутизатори, IP-камери та цифрові відеореєстратори.
Січень 2017	США	-	Атака програм-вимагачів [5] уразила 123 з 187 мережних відеореєстраторів системи відеоспостереження громадських місць по всьому Вашингтону.
Травень 2018	Ячійо та Аґео, Японія	Canon	Хакери офіційно вивели з ладу понад 60 камер безпеки Canon.
Грудень 2018	IP-камери Bosch (версії прошивки: 6.32 та вище)	Bosch	Класифікується як вразливість переповнення буфера ("buffer overflow") у RCP та парсері веб-сервера. Це дозволяє зловмиснику повторно активувати вимкнені функції (наприклад, telnet) або обійти облікові дані доступу (логін/пароль).
Жовтень 2018	Yi Technology, відома китайська організація, тісно пов'язана з Xiaomi	Yi Home Camera	Проблема виникла через вразливість витоку даних, яка існувала в мобільному зв'язку з камерою Yi Home Camera.
Березень 2018	Південнокорейська фірма Hanwha Techwin	Kaspersky	Компанія Kaspersky виявила майже 2000 вразливих камер, до яких можна було отримати доступ через відкриті IP-адреси в Інтернеті.
Березень 2018	Hanwha SmartCam	-	Через помилку в конструкції зловмисник міг отримати доступ через хмару до всіх камер та керувати ними. Основною проблемою є те, що хмарна архітектура залежала від протоколу зв'язку XMPP.
Червень 2018	Камери безпеки Foscam	-	Зловмисник використовував вразливість переповнення буфера на основі стека, щоб обвалити процедуру webService та отримати адміністративний доступ.
Липень 2019	Делі, Індія	-	Віддалений злам та бекдор-доступ до камер відеоспостереження.
Березень 2021	США	-	Атака програм-вимагачів на запис 150 000 камер відеоспостереження в банках, тюрмах, школах, автомобілебудівній компанії Tesla та інших місцях з метою викриття "держави спостереження".

Причини вищезгаданих атак можуть бути пов'язані з використанням стандартних облікових даних для входу, відсутністю належних прав доступу та слабкими функціями безпеки та конфіденційності.

Мотивацією для зловмисника може бути шантаж, можливість спостерігати відеопотік у реальному часі, доступ до відеозаписів, доступ до мережі VSS, вимкнення відеопотоків, порушення конфіденційності, віддалене відключення з'єднання та виконання атак типу "відмова в обслуговуванні" тощо.

Оскільки VSS використовуються в важливих місцях, лише уповноважені особи повинні мати доступ до їх моніторингу та керування.

Конфіденційність та безпека є найголовнішими питаннями під час використання таких систем.

Зважаючи на все це, ця робота спочатку визначає можливі атаки на такі системи, а потім обговорює заходи, які можна вжити для запобігання атакам. Крім того, проводиться порівняння існуючих фреймворків VSS разом з їх перевагами та недоліками.

Після запуску атаки Mirai та її наслідків у 2016 році кількість досліджень, пов'язаних з атаками та вразливістю в сфері VSS, значно зросла. У статтях обговорювались лазівки та недоліки мереж Інтернету речей (IoT).

У цьому розділі ми розглянемо всі можливі типи активних атак на різних рівнях систем відеоспостереження. Основними проблемами є:

- (а) конфіденційність та безпека системи відеоспостереження,
- (b) невизначеність щодо того, що відбувається з вашими даними, коли вони зберігаються в хмарі, і
- (с) те, як пристрої моніторингу користувачів, такі як смартфони, також можуть стати причиною атаки в мережі відеоспостереження.

Типовий сценарій атаки складається з наступних кроків:

- (а) збір інформації,
- (b) оцінка вразливості,

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

- (с) запуск атаки та
(d) усунення наслідків.

Деякі інструменти, що використовуються зловмисниками на різних етапах, наведено на рисунку нижче.

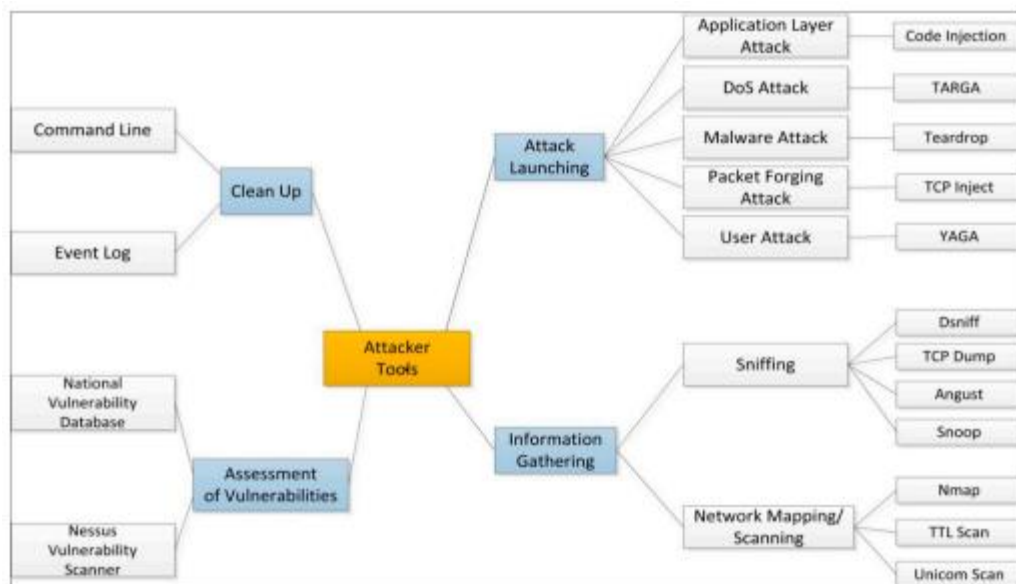


Рисунок 2.1 – Приклади інструментів для атаки

Системи відеоспостереження (ВСС) використовуються програмами для розпізнавання рис обличчя, автоматичного читання номерних знаків, сканування та зчитування QR-кодів, а також стиснення зображень.

ВСС має додатковий рівень абстракції – візуальний. Цей рівень вразливий до певного типу атак, оскільки вони стосуються семантики зображень та розпізнавання образів. Атаки поширюються/впроваджуються різними способами, наприклад, через попередньо встановлене шкідливе програмне забезпечення в системі, оновлення прошивки або вставку віддаленої команди.

Шкідливі зображення можуть бути вбудовані в зображення, зроблені відеокамерами/датчиками.

Однією з найпоширеніших атак на відеопотік у реальному часі з ВСС є атака з дублюванням кадрів. Зловмисник, отримавши доступ до системи ВСС, може вставити раніше записані "нормальні" кадри замість потокового відео, щоб уникнути виявлення підозрілої діяльності.

Для виявлення таких атак з дублюванням кадрів просторові та часові подібності між кадрами витягуються та аналізуються за допомогою різних методів кореляції. Для цього потрібна величезна база даних для зберігання великої кількості даних та значний час обчислень для виявлення та запобігання таким атакам у режимі реального часу.

2.2 Атаки з використанням прихованих каналів (Covert Channel Attacks)

В цьому типі атак об'єкти інформації можуть передаватися між процесами, які за політикою безпеки повинні бути заблоковані. Ці атаки відрізняються від законного використання каналів для зламування систем із середнім рівнем захисту, наприклад, за допомогою стеганографії, яка маскує заборонені об'єкти всередині легальних інформаційних об'єктів.

За допомогою такого типу атак зловмисники можуть спілкуватися із шкідливим програмним забезпеченням, вбудованим у систему.

Користуючись такими критеріями, як час/сховище, мережа/ОС/обладнання, значення/зміна, атаки з використанням прихованих каналів можна класифікувати на різні типи. Ось деякі приклади атак з використанням прихованих каналів:

- Маніпулювання ІЧ-світлодіодами камер відеоспостереження/ВСС: передача даних керування зловмиснику на камери ВСС за допомогою повідомлень через інфрачервоні світлодіоди;
- Новий тип оптичного прихованого каналу під назвою VisisSploit, який виточує дані через РК-дисплей комп'ютера;
- Мережеві приховані канали можна створювати для координації атак типу "відмова в обслуговуванні", обходячи брандмауер користувача. Наприклад, поле TTL заголовка IPv4 можна використовувати для передачі інформації в або з мережевого домену.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3 Атаки з використанням стеганографії (Steganography Attacks)

Стеганографія - це метод використання непотрібних або менш важливих інформаційних бітів у вмісті користувача (зображення, відео, мережевий трафік) для приховування даних. Існує два поширених типи атак з використанням стеганографії: приховування шкідливого коду в легальній програмі та використання каналу керування.

Поширений прийом багатьох троянських програм полягає в додаванні даних до кінця файлу або використанні невикористаних частин формату файлу. За будь-якого методу стеганографії важко виявити шкідливий код, який надходить через файли користувачів у мережі. Шкідливі корисні дані можуть бути вбудовані в набір файлів PNG. Потім файли PNG можна скомпілювати в легальну програму разом із функцією, яка витягне та скине шкідливе програмне забезпечення на систему.

В атаках на протоколи керування зловмисники можуть використовувати "систему доменних імен (DNS) та протокол передачі гіпертексту (HTTP)" для вбудовування шкідливого коду у відповідь на запит клієнта.

Наприклад, розглянемо Користувача А (власника будинку чи офісу), який підходить до IP-камери. Після успішного розпізнавання обличчя Користувача А вона зберігає зображення та робить інше зображення без обличчя (назване зображенням-обкладинкою). Тепер для надсилання "стегозображення" (комбінованого зображення, де фактичне зображення приховане в зображенні-обкладинці) використовується метод стеганографії. Це "стегозображення" зберігається на домашньому сервері, який потім буде оброблено за допомогою зворотної стеганографії для отримання оригінального зображення з обличчям.

Інший Користувач В (зловмисник) перехоплює передачу даних між IP-камерою та домашнім сервером і захоплює всі дані, що містять "стегозображення" разом з іншими захопленими зображеннями. На цьому етапі зловмисник може

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

виконати три категорії атак: атаку тільки на стегозображення, атаку з відомою обкладинкою та атаку з відомим повідомленням.

Будь-яке зображення можна представити значенням пікселя (набором одиниць і нулів). Зображення-обкладинка також матиме ряд бітів, але їхня послідовність бітів відрізнятиметься на стороні LSB або MSB порівняно з відповідним зображенням обличчя. Будь-яка зміна в бітах LSB зображення обличчя не суттєво його змінить, тоді як зміни в бітах MSB значно погіршать якість зображення обличчя. Зловмисник може використовувати статистичний аналіз для виявлення змін у бітах LSB або людське зорове сприйняття для виявлення змін у бітах MSB, щоб виявити зображення обличчя з зображення-обкладинки. Потім Користувач В може використовувати це розшифроване зображення обличчя для атаки на систему домашньої безпеки та отримання доступу до будинку чи офісу.

Атаки на камери з керуванням PTZ (поворотом, нахилом, масштабуванням)

PTZ (Pan-Tilt-Zoom) - це функціональна характеристика камери відеоспостереження, яка дозволяє збільшувати та зменшувати масштаб, а також змінювати поле зору камери по горизонталі (вправо, вліво) та вертикалі (вгору, вниз). Для реалізації цієї функції моделі камер використовують вбудовані крокові двигуни та протоколи передачі даних PTZ. Протоколи даних PTZ використовують канали RS-422 або RS-485, а також Ethernet та Wi-Fi. Камерами з підтримкою PTZ можна керувати за допомогою клавіатурних скорочень або спеціально розробленого джойстика за допомогою команд PTZ.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.2 – Камери з керуванням PTZ(Pan-Tilt-Zoom)

Скомпрометована камера PTZ може надсилати дані зовнішньому зловмиснику разом з координатами PTZ . Коли користувач використовує мобільний додаток для перегляду відеопотоку з камери через хмарний сервер, усі запити PTZ надсилаються через хмарні сервери до камери. Якщо таке спілкування відбувається через інтервал кожні кілька секунд, зловмисник, який перехоплює це спілкування, можливо, не зможе розшифрувати дані PTZ, але може точно визначити інтервал, через який відбувається спілкування. Тоді зловмисник може запустити атаку, яка відповідає інтервалу зв'язку, таким чином уникаючи виявлення.

2.4 Відмова в обслуговуванні та атаки заглушення (Denial of Service and Jamming Attacks)

Будь-яка дія або серія дій, що перешкоджають функціонуванню будь-якої частини інформаційної системи, називається відмовою в обслуговуванні (DoS) шляхом заглушення каналу зв'язку.

У багатьох системах відеоспостереження під час моніторингу важливої діяльності, такої як злочини в режимі реального часу, критично важливою є безперебійна робота системи. DoS-атаки та атаки заглушення з дуже короткою тривалістю (менше кількох хвилин) можуть призвести до того, що камера відеоспостереження (ВСС) пропустить швидкий злочин, наприклад, пограбування банку.

Відмова в обслуговуванні домашньої камери відеоспостереження не матиме такого значного впливу, порівняно з DoS-атаками на комерційні системи відеоспостереження, які можуть мати більші наслідки. Ці типи атак необхідно враховувати на ранніх етапах налаштування та тестування системи відеоспостереження.

Наприклад, "BrickerBot - це шкідливе програмне забезпечення, яке атакує пристрої Інтернету речей (IoT), що працюють під керуванням певної версії сервера DropBear SSH, а також атакує пристрої Linux під керуванням BusyBox (зазвичай IP-камери)".

Атаки DoS можна класифікувати на два типи: атаки переповненням та атаки на логіку. Атаки переповненням працюють шляхом перевантаження поточної мережі великим обсягом складних пакетів даних, щоб виснажити її ресурси, такі як пам'ять та пропускна здатність. Атаки на логіку використовують відомі вразливості системи для атаки на віддалені сервери. З цих двох типів атак, атаки переповненням є більш небезпечними, оскільки важко (витрачає багато ресурсів, часу та коштів) відрізнити реальні пакети даних від пакетів переповнення.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

2.5 Атака шкідливим програмним забезпеченням (Malware Attack)

Шкідливе програмне забезпечення (ШПЗ) буває різних форм і типів, таких як віруси, трояни, програми-вимагачі та шпигунське програмне забезпечення. На смартфонах користувачі завантажують мобільні додатки, а шкідливий код, вбудований у програму, може отримати доступ до особистої інформації, яку зловмисники потім можуть використовувати для фінансової вигоди.

Вірус-шкідник Mirai, що з'явився у 2016 році, використовує IP-адреси пристроїв, вразливих в Інтернеті речей (IoT), а потім перетворює ці пристрої на ботів, які можна використовувати як частину ботнетів для масштабних мережових атак.

Інше шкідливе програмне забезпечення, BrickerBot, подібно до Mirai, заражає свою ціль, отримує доступ до пристрою та знищує його – "замикає" його, тобто пристрій більше не працює. У мережі відеоспостереження ніхто не хоче прокидатися і розуміти, що його камера відеоспостереження більше не працює, тому що її навмисно знищив хтось, хто намагався її "захистити". Також ніхто не хоче, щоб фотографія або відео з його пристрою або сховища додатків стало вірусним у соціальних мережах через те, що його камеру (яка може бути камерою відеоспостереження або камерою смартфона) зламали.

Атака шкідливим програмним забезпеченням несе значні загрози безпеці, оскільки дозволяє зловмиснику виконувати будь-яку команду на цільовій машині або в межах цільового процесу. Завдяки цьому зловмисник може мати різні способи вторгнення, здійснюючи ін'єкцію шкідливого коду, витік даних, а також підвищення прав.

Вразливості контролю доступу були виявлені в IP-камерах, відеореєстраторах (DVR) та VPN-маршрутизаторах, які публічно перераховані на веб-сайті <https://cve.mitre.org>.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

2.6 Атака з підвищенням привілеїв (Privilege Escalation Attack)

В багатокористувацькій архітектурі будь-якої мережі додатків або пристроїв права доступу для користувачів обмежені. Користувачі різних рівнів мають різні дозволи. У користувацьких додатках Android або програмах відеоспостереження компоненти, такі як служба, постачальник вмісту, приймач трансляцій та активність, можуть використовувати підвищення привілеїв для отримання більших дозволів, ніж потрібно або бажано.

Існує два варіанти підвищення привілеїв: вертикальне підвищення привілеїв та горизонтальне підвищення привілеїв.

Вертикальне підвищення привілеїв: помилки та недоліки проєктування можна використовувати, щоб дозволити користувачеві смартфона виконувати програми або функції більш високого рівня. Навіть процес, наприклад, може використовувати помилку в ядрі системи та запускати функції з системними правами. Потрібно, щоб щонайменше один процес працював із системними правами, щоб дозволити іншому процесу нижчого рівня підвищити рівень.

Горизонтальне підвищення привілеїв: користувач та програми знаходяться на одному рівні дозволів. Підвищення привілеїв відбувається, якщо користувач або програма можуть отримати доступ до даних або функцій іншого користувача або програми.

Однією з вбудованих функцій безпеки Android є песочниця для програм Android. Це спосіб керування та ізоляції користувацьких програм від критичних системних ресурсів та програм. Атака з підвищенням привілеїв обходить обмеження песочниці шляхом виконання шкідливого коду під час виконання. Додаток, який є "непривілейованим", все одно може отримувати доступ до файлів "привілейованих" системних додатків, таких як геолокація, код доступу користувача, стан батареї, дозвіл камери тощо.

Аналогічно, в системі відеоспостереження зловмисник може скористатися інформацією за замовчуванням про порт прошивки та вхідні дані та отримати доступ до пристрою як користувач із правами адміністратора. У такому сценарії

компанії нічого не можуть зробити, окрім як рекомендувати своїм клієнтам застосовувати новішу прошивку та використовувати більш складні паролі.

Поширені атаки на різні частини інфраструктури VSS наведено на рисунку 5. Таблиця 2 містить інформацію про різні типи атак, їх опис та приклади того, як такі атаки здійснюються зловмисниками.

Висновки за 2 розділ: Під час роботи з цим розділом мною було розглянуто: види атак на системи відеоспостереження, а саме атаки з використанням прихованих каналів, стеганографії, шкідливого програмного забезпечення, з підвищенням привілеїв та відмова в обслуговуванні та атаки заглушення

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

3. ТЕХНІЧНА РЕАЛІЗАЦІЯ ПРОЕКТУ

3.1 Вибір системи відіоспостереження

Системи відеоспостереження поступово стають звичним атрибутом сучасної України. Електронні пристрої здійснюють відеофіксацію за тим, що відбувається на стадіонах, спортивних майданчиках, вулицях, парках, транспортних магістралях, в аеропортах та вокзалах. Інформаційні технології застосовують з метою охорони громадського порядку, контролю безпеки дорожнього руху, захисту власності тощо. Якщо раніше системи відеоконтролю переважно впроваджувалися у великих містах, то сьогодні такі технології набули популярності й у малих громадах. Камери встановлюють органи державної влади, місцевого самоврядування та приватні особи. За своїм функціональним призначенням і способом обробки інформації системи відеоспостереження поділяють на такі різновиди:



Рисунок 3.1 – Системи відеоспостереження

Така функціональна можливість є практично в усіх комплексах міських систем. З огляду на практику інших країн світу, можна припустити, що вона є доцільною лише за наявності достатньої кількості операторів, які постійно відстежуватимуть зображення на моніторах («відеостінах»), що транслюють отриману з відеокамер інформацію у реальному часі. Але з цього приводу є

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		37

дискусії. Деякі фахівці, зокрема представники органів місцевого самоврядування, вважають такий підхід нераціональним і малоефективним, оскільки люди можуть помилятися щодо правильного реагування на отримані відеодані. Оператор, через стомленість або неуважність, може просто не помітити значимої інформації або невірно проаналізувати її, і в результаті — прийняти помилкове рішення. Також серед аргументів є те, що цілодобове функціонування системи потребує витрат іншого роду — оплата праці кількох змін операторів та проведення комплексу робіт по створенню для них належних умов праці.



Рисунок 3.2 – Системи що забезпечують візуальний контроль у режимі реального часу

Вказані системи дозволяють не тільки спостерігати за подіями у певному місці, а й накопичувати та зберігати отримане відео протягом необхідного часу. Переваги цього методу роботи у тому, що відеофайлами можна управляти: переглядати, редагувати, збільшувати зображення, робити уривки відео тощо. У

таких функціональних можливостях, передусім, зацікавлені органи правопорядку, адже збережені відеозаписи можна використовувати під час здійснення оперативно-розшукової діяльності, досудового слідства або у якості доказів при притягненні правопорушників до відповідальності. Разом із тим, місцева влада часто використовує таку інформацію, наприклад, при вирішенні питань, пов'язаних із містобудуванням, розвитком інфраструктури, оптимізацією транспортних потоків, роботою комунальних служб тощо. Системи такого типу також застосовуються на підприємствах, установах та організаціях інших форм власності для охорони території та майна або контролю за дотримання режиму роботи, використанням робочого часу тощо.



Рисунок 3.3 – Системи з можливістю збереження отриманої з відеокамер інформації

Ці системи відеоспостереження здатні не лише записувати всі події у секторі спостереження, а й відокремлювати інформацію із загального відеопотоку, аналізувати та структурувати її за визначеними у програмі критеріями. Наприклад, такі системи використовуються для автоматичного розпізнавання транспортних засобів за державними номерними знаками. Разом із тим, при сучасному програмному та апаратному оснащенні, вони здатні вирішувати

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

завдання більш широкого діапазону — розпізнавати обличчя для подальшої безконтактної ідентифікації особи, встановлювати наявність у зоні контролю певних предметів та речей (наприклад, об'єктом пошуку і відеофіксації може бути особа з великогабаритною сумкою), реагувати на параметри руху чи щільність транспортного потоку, фіксувати перетин віртуальних ліній, здійснювати підрахунок людей та інше. Так, однією з функцій системи відеоспостереження може бути інформування про скупчення людей, якщо їх кількість у зоні контролю перевищує задане програмою порогове значення. Це дозволяє оперативно встановлювати місця спонтанного виникнення натовпу (масові заворушення чи бійки, стихійні зібрання, наслідки аварії тощо) та своєчасно реагувати на подію в залежності від ситуації. Або є система «Гарпун», яка за допомогою відеокамер збирає та обробляє інформацію про номерні знаки транспортних засобів, що розшукуються у рамках кримінальних чи виконавчих проваджень, зокрема, у справах про адміністративні правопорушення, а також за ухвалою суду.

У серпні 2017 року дослідники з компанії «Checkmarx» провели аналіз захищеності IP-камер Loftek та VStartcam, які найбільш поширені в побуті у всьому світі. Під час дослідження виявлена серія вразливостей, які дозволяють організувати атаки для отримання контролю за пристроями і їх використання для організації комп'ютерних мереж, заражених шкідливим програмним забезпеченням, або для проведення атак на комп'ютери в локальній мережі.

Усього під час дослідження камер виявлено 21 вразливість, які можна зарахувати до категорії безпечних, або помірних. Серед наявних проблем виокремлюються зумовлені параметри входу без повідомлення про необхідність зміни пароля за замовчуванням, відсутність підтримки HTTPS (Hyper Text Transfer Protocol Secure) [3], а також проблеми CSRF (Cross-site Request Forgery), які дозволяють використовувати iFrame (Inline Frame) для відправки команд на камери, що містяться у внутрішній мережі користувача, який зайшов на сторінку.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

Для приховування своєї присутності після успішного отримання контролю над пристроєм зломисник може завести нового користувача з ім'ям «%20» і порожнім паролем, який не буде помітний у списку користувачів в інтерфейсі адміністратора. Експерт компанії Positive Technologies Ілля Сміт виявив і допоміг усунути критичну вразливість у вбудованому програмному забезпеченні IP-камер компанії Dahua, які широко використовуються для відеоспостереження в банківському секторі, енергетиці, телекомунікації, транспорті, системах «розумний дім» та інших сферах. Ця вразливість отримала назву «CVE-2017-3223» та є пов'язаною з можливістю переповнення буфера у web-інтерфейсі Sonia, який призначений для дистанційного керування і налаштуваннями камер.

Неавторизований користувач може відправити спеціально сформований POST-запит на вразливий web-інтерфейс і віддалено отримати привілеї адміністратора, що надає необмежений контроль над IP-камерою. Незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності IP-камер, стрімкий розвиток систем комунікації та протоколів їх захисту зумовлює потребу подальших досліджень цієї тематики.



					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		41

Рисунок 3.4 – VLoftек камера



Рисунок 3.5 – VStartcam камера

Для застосування найбільш ефективних інструментів захисту необхідно виокремити види загроз та провести аналіз методів нападу на системи відеонагляду. Можна виокремити три основних типи загроз для систем відеоспостереження: – злам для отримання доступу до даних;

- злам для перехоплення керування або відключення системи;
- злам із метою несанкціонованого використання обчислювальних потужностей системи.

На стадії аналізу вразливостей системи необхідно врахувати, що системи відеспостереження можуть використовуватися, зокрема, для розв’язання технологічних завдань і організації бізнес-процесів підприємства.

Тому можливою ціллю зловмисників може бути інша система, а обладнання системи відеоспостереження може використовуватися як проміжний етап атаки. Крім того, система відеоспостереження, як правило, інтегрована з іншими підсистемами безпеки і системами автоматизації. Питання інформаційної захищеності системи відеоспостереження переходить у завдання захисту всіх систем, у які вона інтегрована або з якими обмінюється даними. В аналогових

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

системах відеоспостереження відеокамера відправляє відеосигнал на монітор безпосередньо без стиснення. Це прості в монтажі, надійні, але громіздкі системи з обмеженим функціоналом. Сьогодні такі рішення використовують лише в невеликих системах із декількома камерами, які розміщені близько одна до одної або у вузькоспеціалізованих галузях.

Аналогові системи мають обмежений функціонал і можуть тільки вести спостереження в режимі реального часу, а також записувати відеоінформацію на цифрові накопичувачі (**DVR – DigitalVideoRecorder**) [4]. Розширення функціоналу потребує витрат на додаткові пристрої і їх монтаж. Запис на DVR також має обмеження: декодування відео відбувається безпосередньо в DVR, а не на відеокамерах. Так, пристрій DVR необхідно фізично з'єднати з кожною камерою за допомогою кабелю.



Рисунок 3.6 – DVR – Digital Video Recorder

ІР-камера відеоспостереження знімає відео і транслює відеопотік у цифровому форматі з використанням мережевого протоколу, який забезпечує маршрутизацію пакетів. Тобто ІР-камера складається з матриці, об'єктива, центрального процесора, процесора обробки, процесора стиснення та мережевого інтерфейсу. ІР-камери відеоспостереження є самодостатнім окремим засобом

спостереження, керування якими здійснюється через WEB-інтерфейси, передаючи всі потоки мережі.

Майже всі сучасні цифрові IP-камери відеоспостереження побудовані на операційній системі Linux, яка дуже обмежена і має тільки найбільш необхідне для роботи. Сама по собі операційна система Linux безкоштовна, дуже надійна і стійка до зовнішніх впливів і зламів, тому виробники і будують на її базі відеореєстратори, відеосервери, камери відеоспостереження та інші пристрої. Наявність модуля Wi-Fi і мережевого інтерфейсу RJ-45 дозволяють проводити безпосереднє підключення до IP-камер.

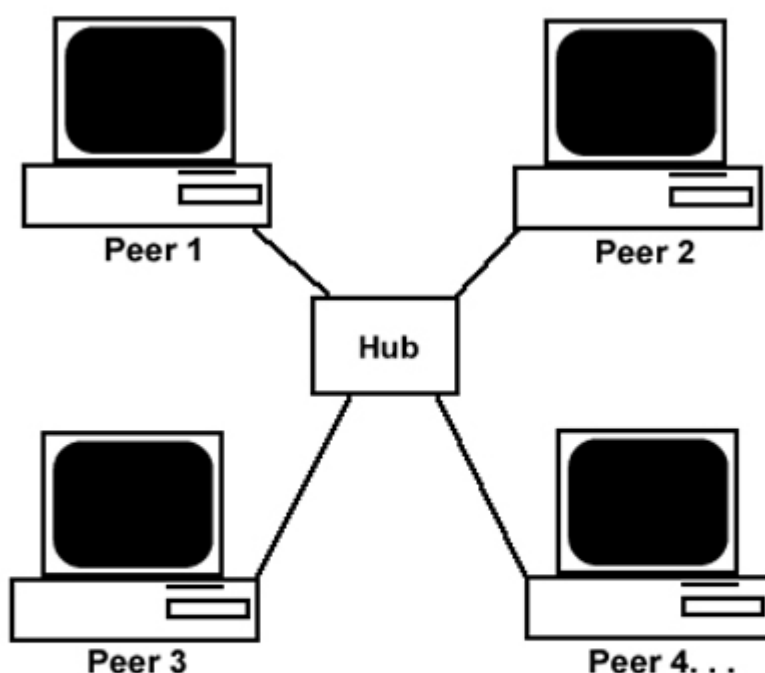
Раніше для цього використовувалися спеціальні додатки, але зараз все можна проводити через стандартний браузер із мобільного телефона або комп'ютера. Їх слабкість у тому, що вони завжди включені і мають віддалений доступ, чим активно і користуються зловмисники. Перевагою сучасних IP-камер є великий «інтелект», як-от система увімкнення запису зарозпізнаванням руху, автоматичне відстеження руху, виявлення залишених предметів, цифровий зум і фотофіксація особи, номери машини тощо. Крім того, IP-камери можуть стискати відео, відправляючи картинку з безлічі камер через один кабель.

За допомогою кодування можна стискати відеофайли, скорочуючи завантаженість лінії зв'язку до 80%. Це зменшує вимоги до обсягів мережевих накопичувачів (NVR – Network video recorder), які можуть зберігати відеозаписи з якістю 720p тривалістю до 50 днів на жорсткому диску обсягом 4 Тб. Зв'язок із NVR може здійснюватися через мережу Інтернет, тобто на основі IP-камер можна побудувати розподілену систему відеоспостереження, яка буде передавати дані відеозапису через мережу на віддалений накопичувач.

Таку систему можна контролювати віддалено, зокрема з мобільних пристроїв, а мережевий накопичувач фізично не є доступним для потенційних зловмисників, оскільки може перебувати за сотні кілометрів від контролюваного об'єкта. Проте будь-які проблеми з переданням інформації можуть призвести до повного або часткового порушення працездатності системи.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

Слід зазначити, що більшість IP-камер мають функцію **P2P (Peer-to-peer)** [5] і можуть працювати без статичної IP-адреси, поєднуючи камеру і монітор через інтернет-сервер виробника камери. Мережа з функцією P2P заснована на рівноправності учасників. Найчастіше в такій мережі відсутні виділені сервери, а кожен вузол є як клієнтом, так і виконує функції сервера. Така організація дозволяє зберігати працездатність мережі за будь-якої кількості і будь-якому поєднанні доступних вузлів. Ця функція дозволяє організувати відеоспостереження у тому разі, коли провайдер не надає статичні IP-адреси. Крім того, налаштування камер P2P дуже просте.



P2P Network

Рисунок 3.7 – P2P(Peer-to-peer)

Коли відбувається підключення камери з функцією P2P, їй присвоюється номер. За його допомогою відбувається визначення сервером можливості передання даних на сервері. Ідентифікатор звіряється і користувач отримує доступ до відеопотоку через персональний комп'ютер або пристрій під

керуванням Android чи iOS. Крім отримання інформації, можна здійснювати безпосереднє керування роботою камери. З одного боку, функція P2P в IP-камерах надає багато переваг, проте ця функція здатна змінити конфігурацію DMZ (Demilitarized Zone) на маршрутизаторі.

DMZ [6]– це спеціалізований локальний сегмент мережі, який містить загальнодоступні сервіси з повним відкритим доступом для внутрішньої та зовнішньої мережі. У налаштуваннях маршрутизатора не можна використовувати для системи відеоспостереження функцію DMZ, оскільки вона може надати зловмисникові необмежений доступ до відеокамери, яка перебуває в мережі. Для захисту лінії дротового зв'язку потрібно використовувати керовані комутатори. Необхідно здійснювати фільтрацію за MAC-адресою з підтримкою «білих» списків, роботу з VLAN, VPN, блокування портів, які не використовуються.

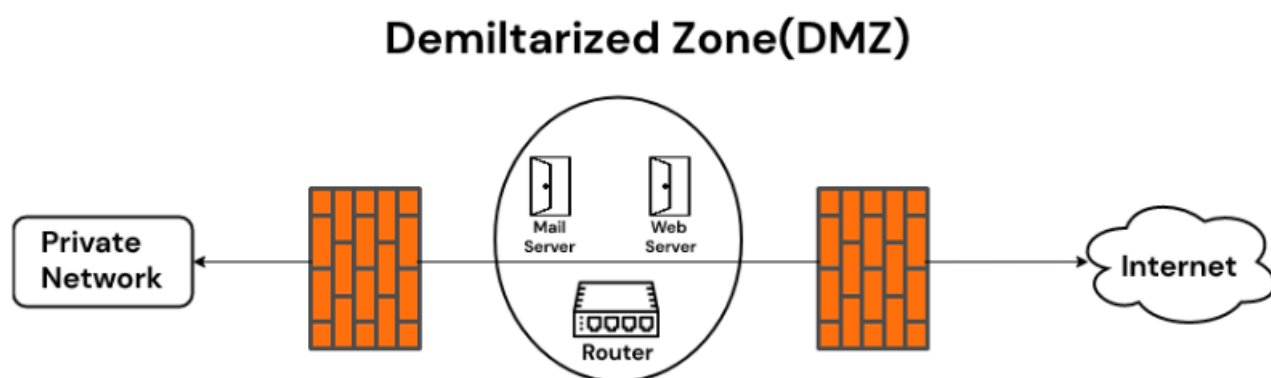


Рисунок 3.8 – DMZ

Деякі комутатори можуть самі шифрувати вхідні дані та передавати їх далі на пристрій, який буде розшифровувати вхідний потік. Також комутатори можуть відслідковувати спроби недозволеного доступу або будь-які зміни в локальній мережі і повідомляти про них адміністратора системи.

Бездротові Wi-Fi IP/P2P-камери [5] можуть заощадити значні засоби на встановленні відеоспостереження. Наразі пропускну здатності Wi-Fi мережі достатньо для передання відео високої роздільної здатності. Проте канал Wi-Fi може бути блокований DDoS-атаками, відправленими через радіоканал, які спрямовані на порушення якості функціонування мережі або на абсолютне

припинення доступу користувачів. У цьому разі перерветься потік відео, який іде від камери на мережевий відеореєстратор. При цьому відключення мережі не означає припинення відеоспостереження, адже сучасні відеокамери мають убудовані карти пам'яті, які дозволяють згодом «вручну» переглянути відеозапис.



Рисунок 3.9 – Бездротові Wi-Fi IP/P2P2-камери

Загрозою конфіденційності відеоспостереження через мережу Wi-Fi є радіосніферінг. Сніфери займаються перехопленням та аналізом мережевого трафіка. Для того, щоб підвищити стійкість Wi-Fi мережі відеоспостереження, провести захист периметра і виявити спроби підключення небажаних користувачів, застосовуються програмно-апаратні комплекси. Ці прилади безперервно сканують кожен канал Wi-Fi і автоматично виявляють різноманітні загрози, включаючи поширені атаки шляхом перебору паролів, уторгнення за допомогою утиліт Aircrwn, фазинг тощо.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

Програмне забезпечення сповіщає оператора про спробу вторгнення і дозволяє виявляти джерела перешкод, «глушилки» сигналу й іншу підозрілу активність у всьому діапазоні частот Wi-Fi, а також у мережах мобільного зв'язку 3G, 4GLTE і CDMA. Необхідно враховувати безпеку не тільки камер, а і всієї інфраструктури, оскільки зловмисникам досить одного слабкого місця, щоб отримати доступ до всієї системи.

Захищений зв'язок між камерами і мережевими компонентами забезпечується шляхом призначення кожному елементу ключа автентифікації. Це електронний підпис, необхідний для перевірки всіх компонентів (від камер до керівного програмного забезпечення). Для забезпечення безпеки всього процесу автентифікації пристрої повинні підтримувати автентифікацію на основі імені користувача і пароля (IEEE 802.1x).

Для захисту даних відеоспостереження першочергове значення має шифрування потоків даних і збереженої інформації. Ефективний варіант реалізації шифрування на апаратному рівні – це використання у всіх IP-камерах і записувальних пристроях довіреного модуля **TPM (Trusted Platform Module)** [7].

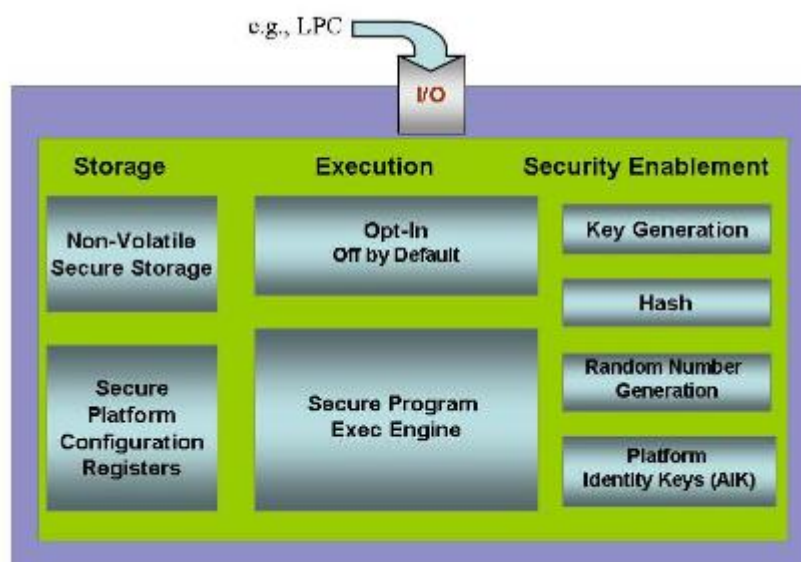


Рисунок 3.10 – TPM(Trusted Platform Module)

Цей модуль є надійним сховищем криптографічних ключів для захисту даних. У разі зламу пристрою зловмисники не зможуть скористатися витягнутою з нього інформацією. Коли дані потрапляють у керівне або клієнтське програмне забезпечення, криптографічний ключ допомагає розшифрувати дані, а також підтверджує, що камера – аутентифікований мережевий партнер. Ступінь конфіденційності даних відеоспостереження може варіюватися від несекретної до цілковито секретної. Але навіть мережі з надійними пристроями і безпечними каналами передавання даних можуть стати жертвами людської помилки, тому надійні відеосистеми пропонують варіанти керування особистими правами доступу користувачів і підтримують дійсні галузеві стандарти.

Рішення для інформаційного захисту систем відеоспостереження повинні відповідати провідним галузевим стандартам інфраструктури відкритих ключів **PKI (Public Key Infrastructure)** [8]. Можливі варіанти використання власних PKI-рішень виробника з власним сертифікаційним центром або підтримка сторонніх PKI-рішень.

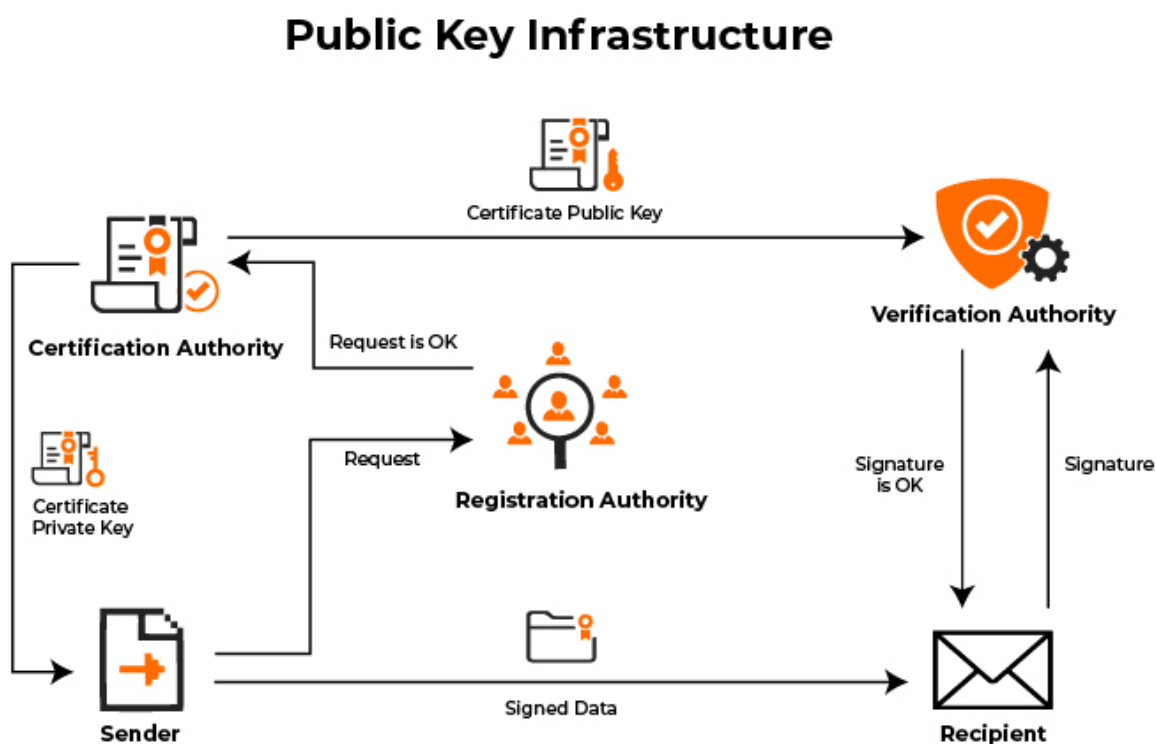


Рисунок 3.11 – PKI(Public Key Infrastrucure)

Зміна пароля за замовчуванням для цифрового відеореєстратора або IP-камери не гарантує абсолютного захисту пристрою від атак зловмисників. Технічні фахівці під час установлення IP-камери або цифрового відеореєстратора змінюють пароль, установлений за замовчуванням, на інший, який видається більш безпечним і гарантує, що зловмисник не зможе проникнути в систему. Ця процедура може допомогти, але не вирішує проблему захисту загалом. Камери відеоспостереження мають внутрішню операційну систему, а також інші програми, які можуть мати вразливості та дають можливість використовувати їх для отримання доступу до системи

3.2 Заходи фізичної безпеки

Безпека інформації у будь-якій інформаційній системі не в останню чергу залежить від оточення, в якому ця система функціонує, а тому комплексний захист персональних даних у системах відеоспостереження повинен передбачати заходи з фізичної безпеки, які спрямовуються на запобігання несанкціонованого доступу до службових приміщень, а також на збереження засобів обробки інформації. До заходів фізичної безпеки відносяться:

1. Нормативне врегулювання. В органі мають бути розроблені та затверджені внутрішні документи, які визначають режимні правила та процедури під час обробки персональних даних.

2. Режим доступу до приміщень. Вхід до приміщень, де обробляється інформація з відеосистем, дозволяється лише особам, які мають відповідний рівень доступу. Особа може увійти до приміщення лише після проходження нею процедури ідентифікації і перевірки наявних для цього повноважень. Списки осіб, які отримали той чи інший рівень доступу, затверджуються керівником органу та своєчасно оновлюються.

3. Моніторинг фізичного доступу до приміщень. Доступ до приміщень має відслідковуватися за допомогою пристроїв відеоспостереження та сигналізації.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

При цьому доцільно застосовувати автоматизовані засоби, що розпізнають і фіксують порушення доступу до приміщень та повідомляють про них.

4. Контроль за відвідувачами. Всі відвідувачі підлягають реєстрації у відповідних журналах чи електронному реєстрі, із збереженням даних про них не менше, ніж протягом одного року. Для проведення реєстрації у приміщенні має бути виділена окрема зона. Відвідувачі отримують доступ до приміщень лише у робочий час, увесь період їх перебування на об'єкті вони супроводжуються особою з числа персоналу, яка контролює їх дії.

5. Захист обладнання. Обладнання має бути захищене так, щоби мінімізувати ризики несанкціонованого доступу до нього. Наприклад, слід унеможливити фотографування або перегляд сторонніми особами зображення на моніторах, зняття відеоінформації з комп'ютерів на флеш-накопичувач та інше. Має бути заборонено виносити з приміщень носії інформації та засоби обробки персональних даних. Кожна така спроба повинна бути зареєстрована і стати підставою для службового розслідування.

Крім цього, захист інформації передбачає виконання заходів, не пов'язаних напряму з можливістю стороннього втручання — протипожежний захист, захист від екологічних та техногенних катастроф, захист від перебоїв у подачі електроенергії тощо.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.12 – Приклад заходу фізичної безпеки

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

3.3 Розробка фізичної моделі

Для дипломного проекту було вибрано офіс, чия структурна схема буде наведена нижче.

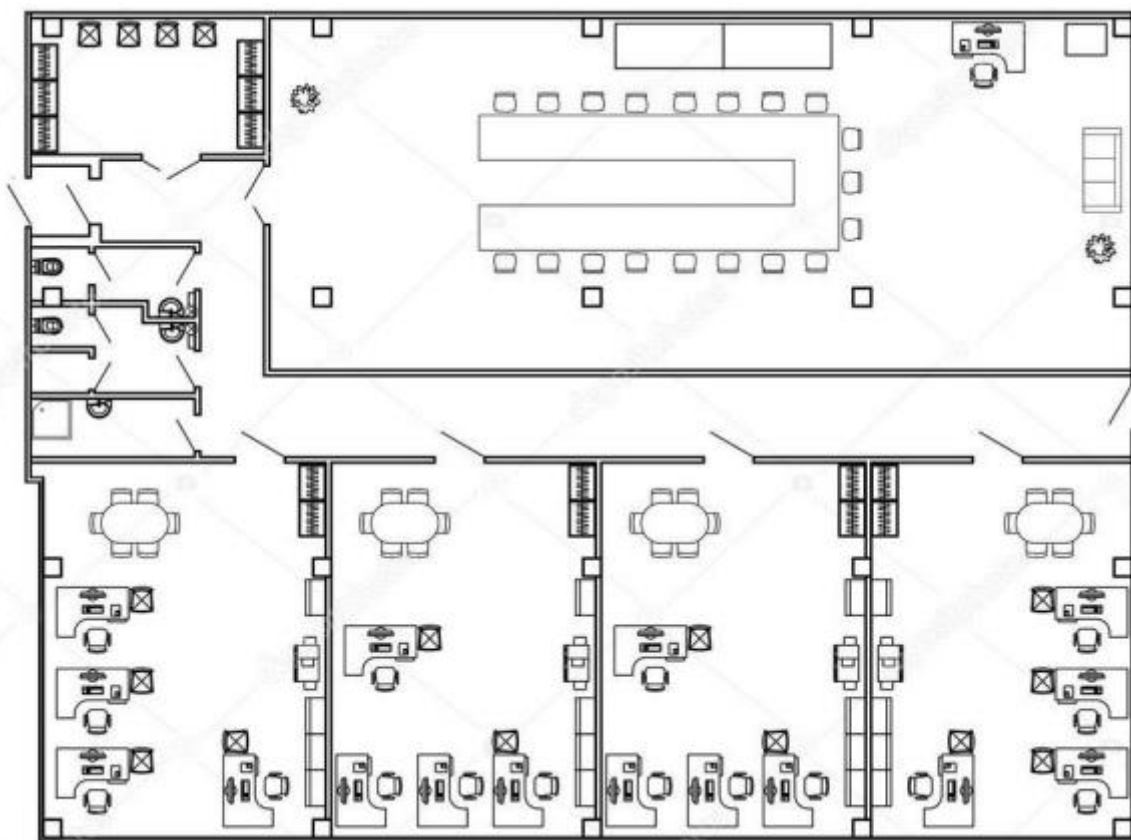


Рисунок 3.13 – Розробка фізичної моделі

У цьому дипломному проекті буде використано 8 камер бренду Hikvision моделі DS-2CV2Q01FD-IW. Основною характеристикою, що робить цю камеру такою, що підходить для цілей проекту, – є вбудований Wi-Fi модуль.

Камера також оснащена:

- Об'єктивом 2.8 мм з кутом огляду 92°.
- Функцією запису звуку.
- Можливістю налаштування насиченості, яскравості та контрастності відео за допомогою програмного забезпечення або веб-браузера.

- Максимальною роздільною здатністю 1280x720 пікселів при 25 кадрах в секунду.

- Підтримкою карт пам'яті micro SD (SD / SDHC / SDXC) об'ємом до 128 Гб (якщо Wi-Fi не використовується).

Вартість однієї камери становить 2 156 грн. Ці камери будуть встановлені в офісах та кабінетах для контролю за роботою персоналу. Зображення камери наведено на рисунку нижче.



Рисунок 3.14 – Камера Hikvision

Переваги використання цих камер:

- **Простота монтажу:** завдяки Wi-Fi модулю не потрібна прокладка кабелів.

- **Широкий кут огляду:** камера охоплює значну площу.

- **Якісне зображення:** висока роздільна здатність та чітка картинка.

- **Запис звуку:** можливість фіксувати не тільки візуальну інформацію, але й звук.

- **Можливість розширення пам'яті:** запис відео на карту пам'яті, якщо Wi-Fi недоступний.

- **Доступна ціна:** камера має оптимальне співвідношення ціни та якості.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

Завдяки своїм характеристикам та перевагам, камери Hikvision DS-2CV2Q01FD-IW стануть ефективним інструментом для контролю за роботою персоналу в офісах та кабінетах.

Камери HikvisionDS-2CV2Q01FD-IW будуть підключені до відеореєстратора за допомогою маршрутизатора XiaomiWiFiMiRouter 3.

Характеристики маршрутизатора:

- **Частоти Wi-Fi:** 2.4 ГГц, 5 ГГц.
- **Інтерфейси:**
 - 2 x 10/100 Ethernet LAN.
 - 1 x 10/100 BaseT WAN.
 - 1 x USB.
- **Швидкість:**
 - LAN портів: 100 Мбіт / с.
 - Wi-Fi: до 300 Мбіт / с.
- **Безпека:**
 - Кодування WPA-PSK / WPA2-PSK.
 - Контроль бездротового доступу.
 - Прихований SSID.
- **Бездротові можливості:** 802.11b, 802.11g, 802.11n, 802.11ac.
- **Ціна:** 999 грн.

Зображення маршрутизатора наведено на рисунку нижче.



					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		55

Рисунок 3.15 –Маршрутизатор Xiaomi WiFi MiRouter

Переваги використання маршрутизатора Xiaomi WiFi MiRouter 3:

- **Підтримка двох діапазонів Wi-Fi:** 2.4 ГГц та 5 ГГц, що забезпечує більш широке покриття та стабільне з'єднання.
- **Гігабітні LAN-порти:** дозволяють передавати дані на високій швидкості.
- **USB-порт:** дає можливість підключити зовнішній жорсткий диск або принтер.
- **Високий рівень безпеки:** маршрутизатор підтримує сучасні протоколи кодування та має функції контролю бездротового доступу.
- **Доступна ціна:** маршрутизатор має оптимальне співвідношення ціни та якості.

Також підтримує здатність запису до 6 мегапікселів, і до 1920x1080p для HDMI виходу. Камера підтримує такі кодеки: H.264 / MJPEG, ці кодеки зменшують відеопотік за розміром при цьому з мінімальними втратами в якості.

Завдяки своїм характеристикам та перевагам, маршрутизатор Xiaomi WiFi MiRouter 3 стане надійним рішенням для підключення камер Hikvision DS-2CV2Q01FD-IW до відеореєстратора.

3.4 Розробка симулятивної моделі системи відеоспостереження компанії захищеної протоколом WPA-2 використовуючи Cisco Packet Tracer

Перш ніж перейти розробки мережі, потрібно її спроектувати. Для цього було вибрано програму-симулятор “CISCO Packet Tracer 8.2”. На рисунку нижче, зображено побудову локальної мережі згідно логічної топології.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		56

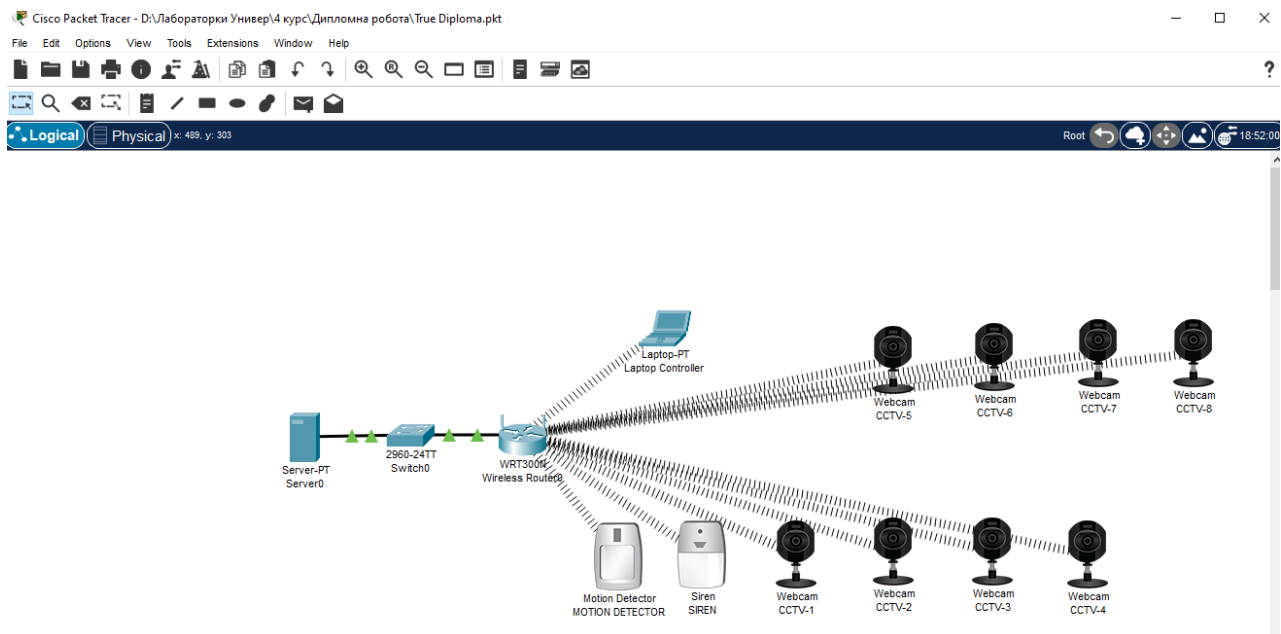


Рисунок 3.16 – Симулятивна модель локальної мережі

Як видно з рисунку 30 комп'ютерна мережа складається із одного сервера, одного світча, одного ноутбука, однієї сирени, одного датчика руху, восьми камер та однієї безпроводної точки доступу.

Наступним етапом після побудови локальної мережі є налаштування обладнання. Цей процес починається із налаштування серверу.

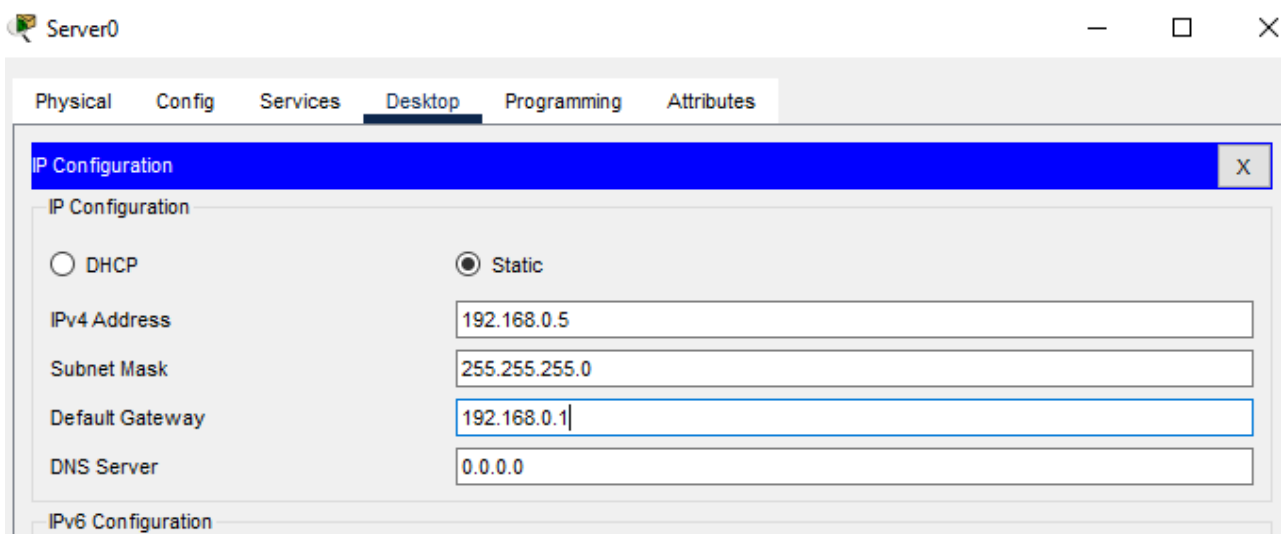


Рисунок 3.17 – Налаштування серверу

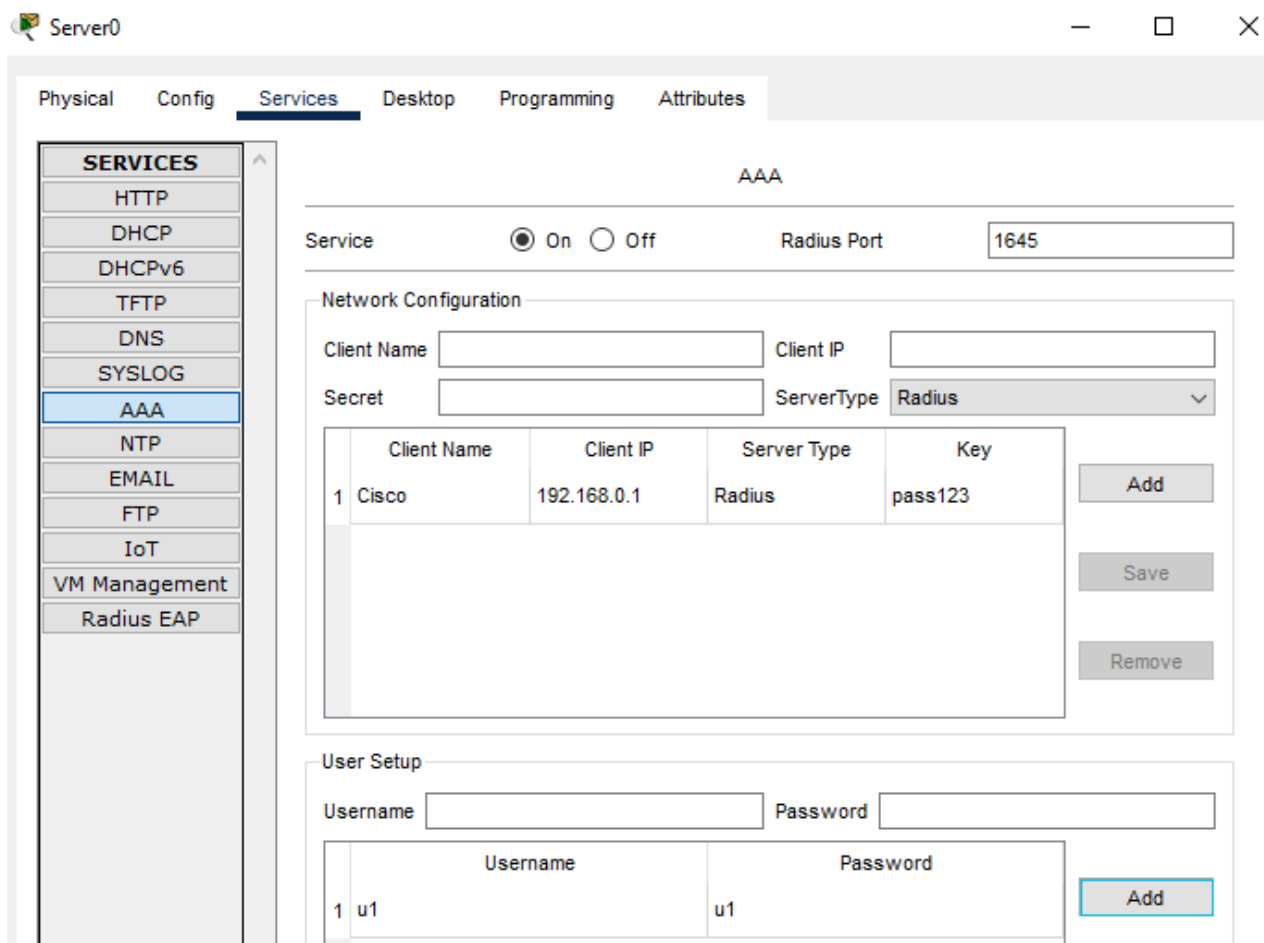


Рисунок 3.18 – Налаштування протоколу Radius

RADIUS (англ. Remote Authentication Dial-In User Service) — протокол передачі даних що використовується в комп'ютерних мережах для автентифікації, авторизації та обліку різноманітних сервісів (англ. authentication, authorization, accounting, AAA). RADIUS був розроблений Livingston Enterprises, Inc. в 1991 році, а потім був перенесений в стандарти IETF (англ. Internet Engineering Task Force).

RADIUS це клієнт-серверний протокол що працює на прикладному рівні, і може використовувати як транспорт як TCP так і UDP.

Наступним кроком є підключення протоколу WPA-2 у роутеру.

Протокол WPA2 з'явився 2004 року. Це оновлена версія WPA. WPA2 заснований на механізмі мережі високої безпеки (RSN) і працює у двох режимах:

Персональний режим або спільний ключ (WPA2-PSK) – використовує спільний пароль доступу та зазвичай застосовується в домашніх мережах.

Корпоративний режим (WPA2-EAP) – більше підходить для мереж організацій та комерційного використання.

В обох режимах використовується протокол CCMP, заснований на алгоритмі розширеного стандарту шифрування (AES), що забезпечує автентифікацію та цілісність повідомлення. Протокол CCMP є більш надійним, ніж вихідний протокол TKIP, що використовується в WPA, тому його використання ускладнює атаки зломисників.

Однак протокол WPA2 також має недоліки. Наприклад, він вразливий для атак із переустановкою ключа (KRACK). Атаки з переустановкою ключа використовують вразливість WPA2, що дозволяє імітувати реальну мережу та змушувати користувачів підключатися до шкідливої мережі замість цієї. Це дозволяє зломисникам розшифровувати невеликі фрагменти даних, об'єднання яких дозволить зламати ключ шифрування. Однак не всі пристрої можуть бути виправлені, тому WPA2 вважається більш надійним, ніж WEP і WPA.

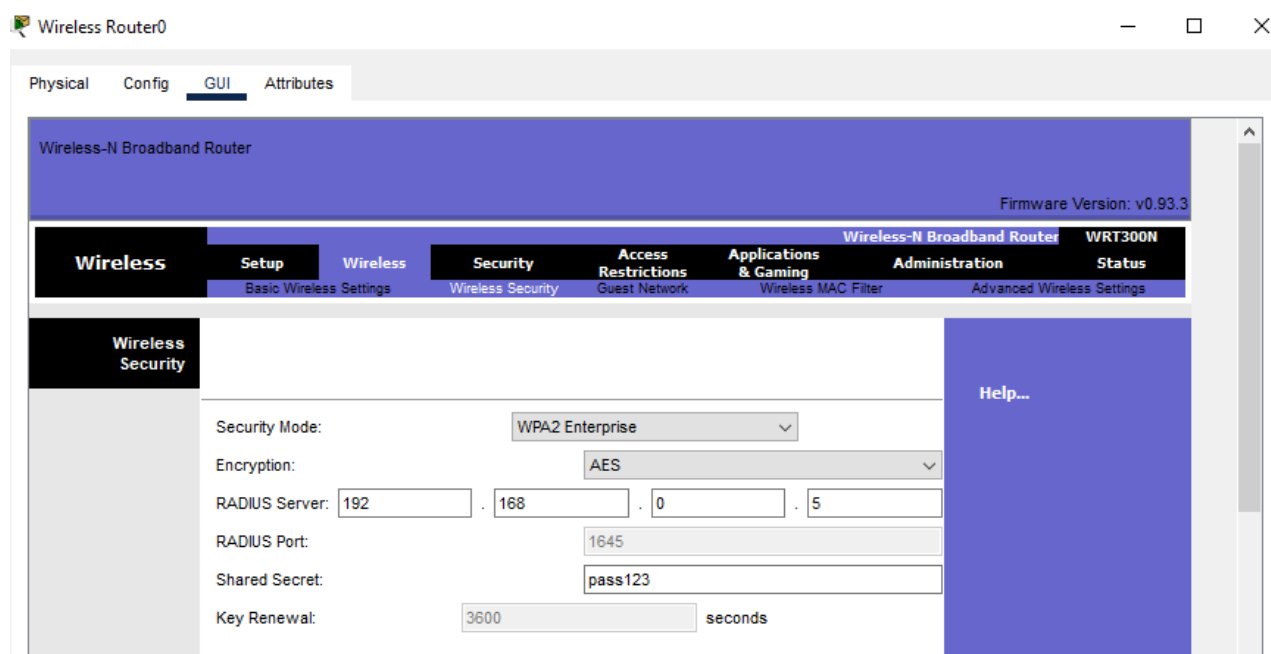


Рисунок 3.19 – Налаштування протоколу Radius

Після підключення та налаштування протоколу WPA2, можна почати налаштування ноутбуку що буде також виступати в якості контроллера.

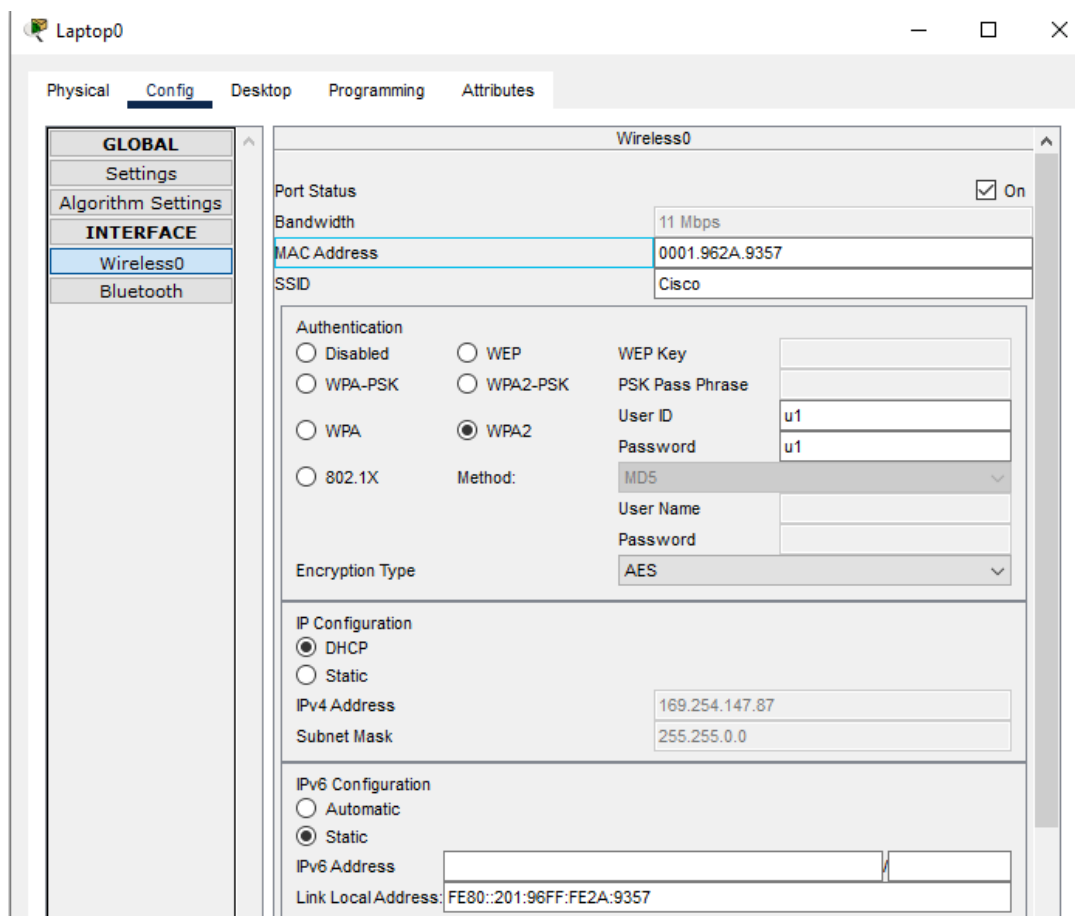


Рисунок 3.20 – Налаштування ноутбуку

Тепер ,ми можемо розпочати налаштування наступних пристроїв, а саме: однієї сирени, одного датчика руху та восьми камер.

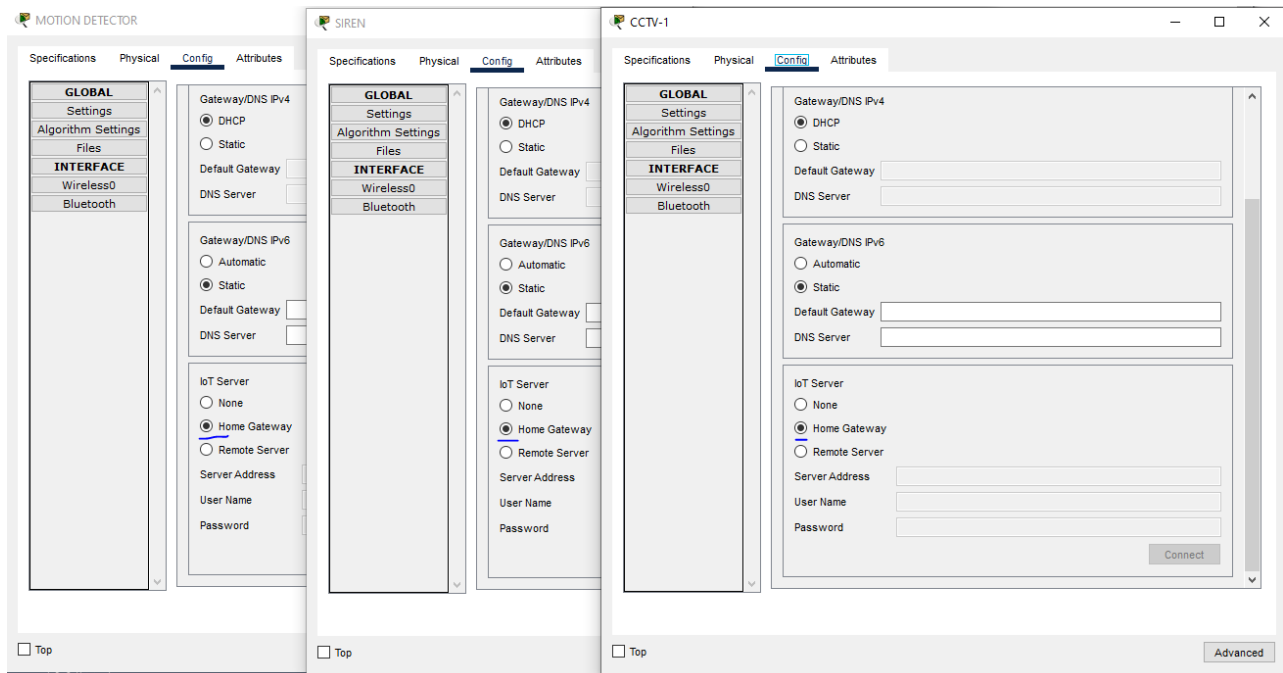


Рисунок 3.21 – Налаштування пристроїв

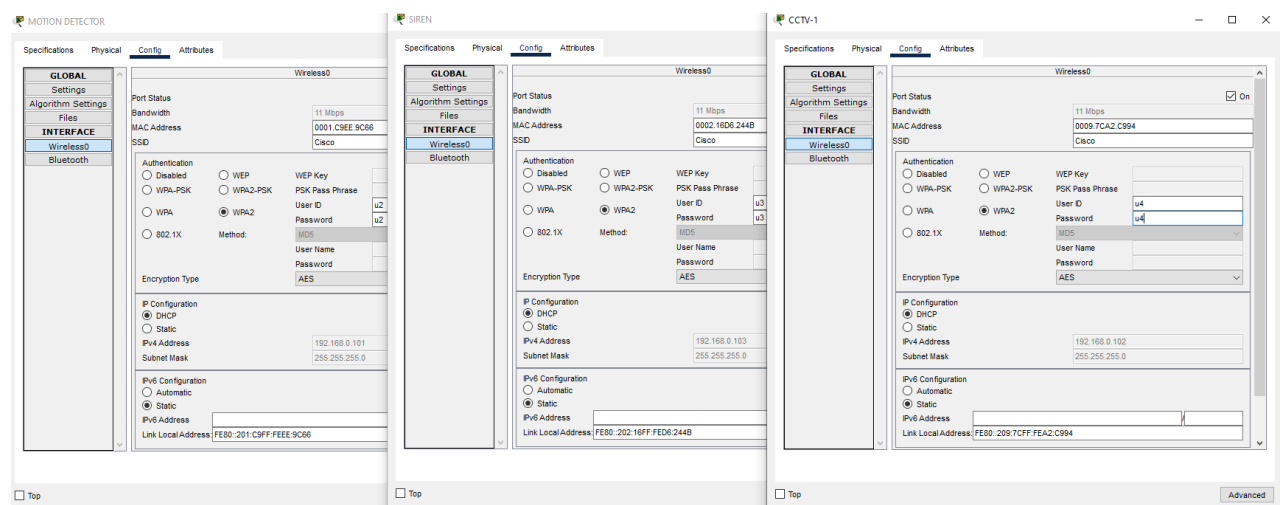


Рисунок 3.22 – Налаштування пристроїв

Після налаштування пристроїв, можна перейти до завершення налаштування контролеру. Ідея є у тому, що у разі спрацювання детектора руху, камери вийдуть із стану очікування а також увімкнеться тривога. Подібна система зможе допомогти із збереження місця на сервері.

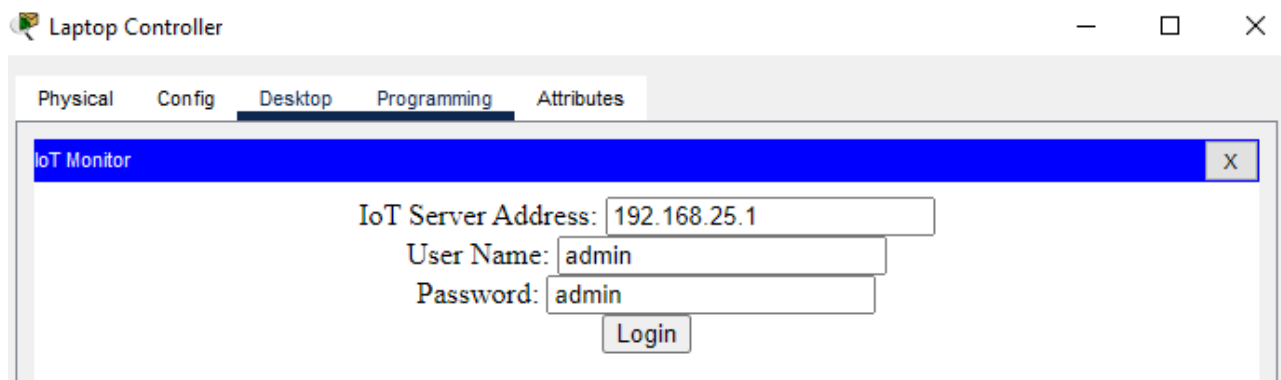


Рисунок 3.23 – Налаштування контроллера

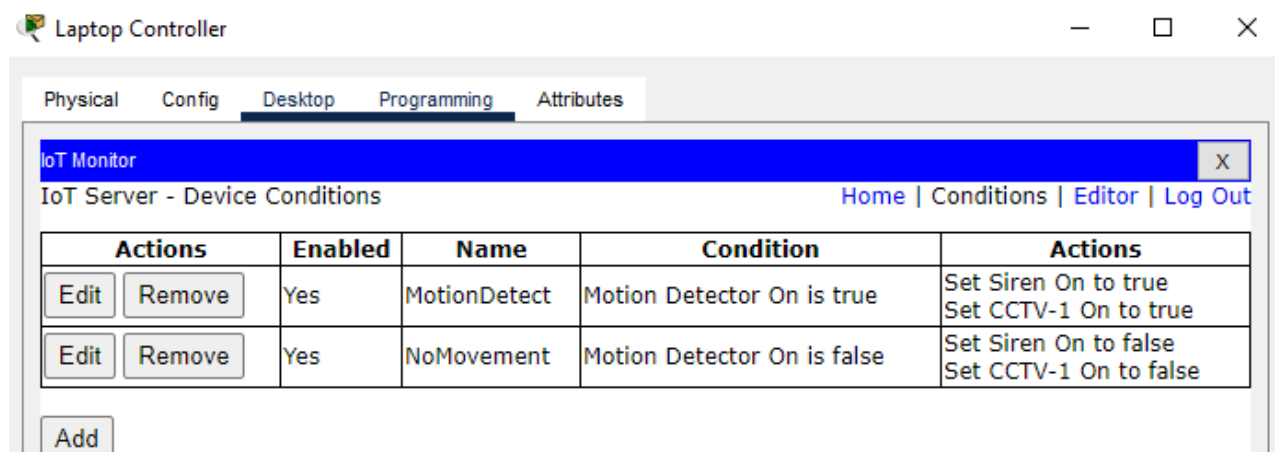


Рисунок 3.24 – Налаштування контроллера

Так має виглядати працююча система відеоспостереження.

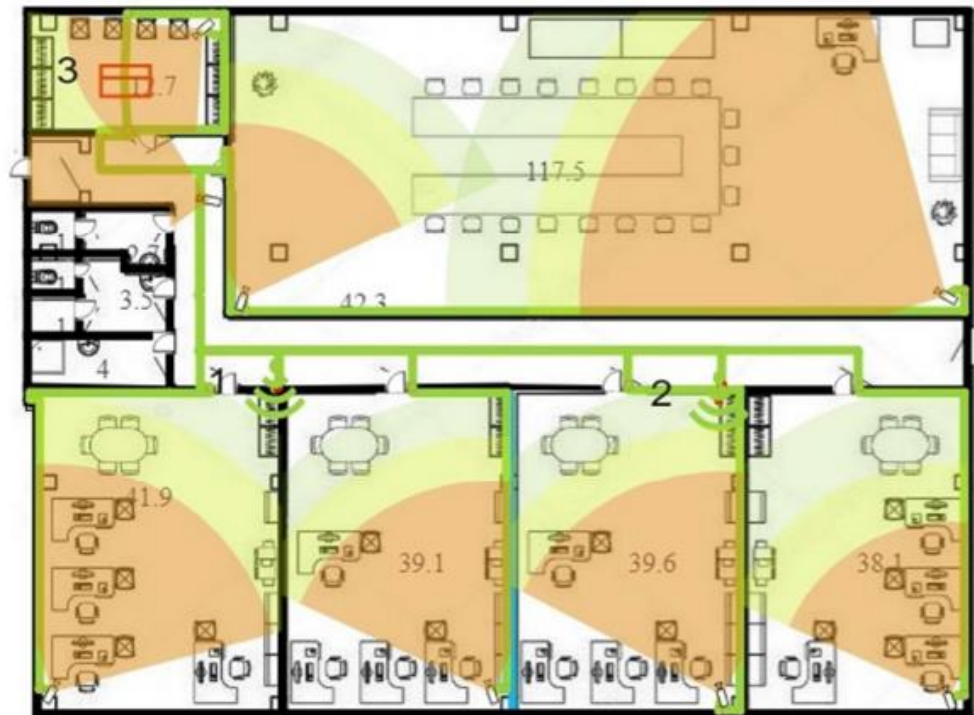


Рисунок 3.25 – Працююча система відеоспостереження

ВИСНОВКИ

У дипломній роботі було досліджено що таке системи відеоспостереження, їх історія, покоління та компоненти. Після більш глибокого розуміння самих систем відеоспостереження, можна було перейти до огляду вразливостей систем відеоспостереження.

Були розглянуті такі види атак :

- Атаки з використанням прихованих каналів (Covert Channel Attacks)
- Атаки з використанням стеганографії (Steganography Attacks)
- Відмова в обслуговуванні та атаки заглушення
- Атака шкідливим програмним забезпеченням (Malware Attack)
- Атака з підвищенням привілеїв (Privilege Escalation Attack)

Після розгляду систем відеоспостереження та їх вразливостей можна було перейти до технічної реалізації проекту, що складається з розробки фізичної моделі і подальшої розробки симулятивної моделі системи відеоспостереження компанії захищеної протоколом WPA-2 використовуючи Cisco Packet Tracer.

Таким чином, можна виокремити основні рекомендації із гарантування безпеки бездротових Wi-Fi мереж: Швидкий розвиток IP-відеоспостереження й інших мережевих систем безпеки вимагає безперервної співпраці між інтеграторами та виробниками для створення і реалізації передових методів, необхідних для забезпечення кібербезпеки.

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз систем відеоспостереження: веб-сайт. URL: <https://ukrbukva.net/page,2,73985-Analiz-sistem-videonablyudeniya.html> (дата звернення: 26.05.2024).
2. Відеоспостереження в офісі: веб-сайт. URL: <https://hikvision.org.ua/ua/articles/videosposterezhennya-v-ofisi> (дата звернення: 04.02.2019). 10. Partizan: веб-сайт. URL: <http://partizan.ua/index.php> (дата звернення: 06.02.2019).
3. Захист даних в WiFi мережах: веб-сайт. URL: <http://isearch.kiev.ua/ru/searchpracticeru/-internetsecurity-ru/828-security-wifi> (дата звернення: 12.05.2024).
4. Захист інформації в мережі WiFi: веб-сайт. URL: http://library.udpu.org.ua/library_files/6365_01.pdf (дата звернення: 16. .05.2024).
5. Комп'ютерні мережі Лекція 6. Модель OSI: веб-сайт. URL: <https://e-tk.lntu.edu.ua/mod/page/view.php?id=3544> (дата звернення: 27.05.2024).
6. Мережевий і транспортний рівень: веб-сайт. URL: <https://studfiles.net/preview/3792007/page:8/> (дата звернення: 09.05.2024).
7. Проектирование локальной сети: веб-сайт. URL: <http://vuz24.ru/nex/vuz-53115.php> (дата звернення: 21.05.2024).
8. Сетевые камеры: веб-сайт. URL: https://drive.google.com/file/d/1AJHnyusj2F72aWWF3ias_gQIv0Wyk9N0/view (дата звернення: 26. 05.2024).
9. Топологія комп'ютерної мережі: веб-сайт. URL: https://studopedia.su/10_122746_topologiya-kompyuternoi-merezhi.html (дата звернення: 20. 05.2024).
10. A review of video surveillance systems: веб-сайт. URL: https://www.academia.edu/99092199/A_review_of_video_surveillance_systems?email_work_card=title (дата звернення: 25.05.2024).

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

11. Apple Remote Desktop: веб-сайт. URL: <https://www.apple.com/remotedesktop/> (дата звернення: 25.04.2024).

12. Attacks and Preventive Measures on Video Surveillance Systems: A Review: https://www.academia.edu/70979100/Attacks_and_Preventive_Measures_on_Video_Surveillance_Systems_A_Review?email_work_card=title (дата звернення: 15.05.2024).

13. CCTV Surveillance System, attacks and design goals: веб-сайт. URL: https://www.academia.edu/43674905/CCTV_Surveillance_System_attacks_and_design_goals?email_work_card=title (дата звернення: 05.05.2024).

14. CCTV Surveillance System, attacks and design goals: веб-сайт. URL: https://www.academia.edu/43674905/CCTV_Surveillance_System_attacks_and_design_goals?email_work_card=title (дата звернення: 25.05.2024).

15. Configuration, Interfacing and Networking of Wireless IP-Based Camera for Real-Time Security Surveillance Systems Design: веб-сайт. URL: https://www.academia.edu/77121582/Configuration_Interfacing_and_Networking_of_Wireless_IP_Based_Camera_for_Real_Time_Security_Surveillance_Systems_Design?email_work_card=title (дата звернення: 26.05.2024).

16. Cybersecurity and Ransomware: веб-сайт. URL: https://www.academia.edu/71677344/Cybersecurity_and_Ransomware?email_work_card=title (дата звернення: 11.05.2024).

17. Design and Implementation of An Improved Digital Video Surveillance System: веб-сайт. URL: https://www.academia.edu/106038946/Design_and_Implementation_of_An_Improved_Digital_Video_Surveillance_System?email_work_card=title (дата звернення: 28.05.2024)

18. Hikvision Digital Technology Co., Ltd.: веб-сайт. URL: <https://www.hikvision.com/brands/hikvision/> (дата звернення: 12.05.2024).

19. IP camera a tool for effective surveillance system. URL: https://www.academia.edu/45675768/IP_CAMERA_A_TOOL_FOR_EFFECTIVE_SURVEILLANCE_SYSTEM?email_work_card=title (дата звернення: 18.04.2024).

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

20. IP camera a tool for effective surveillance system: веб-сайт. URL: https://www.academia.edu/45675768/IP_CAMERA_A_TOOL_FOR_EFFECTIVE_SURVEILLANCE_SYSTEM?email_work_card=title (дата звернення: 27.05.2024).

21. New Functionality, Security and Protection of CCTV Systems: Technological Progress and Digital Society Development: веб-сайт. URL: https://www.academia.edu/113168284/New_Functionality_Security_and_Protection_of_CCTV_Systems_Technological_Progress_and_Digital_Society_Development?email_work_card=title (дата звернення: 20.04.2024).

22. New Functionality, Security and Protection of CCTV Systems: Technological Progress and Digital Society Development: веб-сайт. URL: https://www.academia.edu/113168284/New_Functionality_Security_and_Protection_of_CCTV_Systems_Technological_Progress_and_Digital_Society_Development?email_work_card=title (дата звернення: 27.05.2024).

23. Remote Office Manager: веб-сайт. URL: <https://www.ixbt.com/soft/remote-office-manager.shtml> (дата звернення: 29.04.2024).

24. Technologies for multimedia and video surveillance convergence: веб-сайт. URL: https://www.academia.edu/8536003/Technologies_for_multimedia_and_video_surveillance_convergence?email_work_card=title (дата звернення: 13.05.2024).

25. Video surveillance system: веб-сайт. URL: https://www.academia.edu/36678353/VIDEO_SURVEILLANCE_SYSTEM?email_work_card=title (дата звернення: 29.05.2024)

26. Visual-centric surveillance networks and services Guest Editorial: веб-сайт. URL: https://www.academia.edu/15727189/Visual_centric_surveillance_networks_and_services_Guest_Editorial?email_work_card=title (дата звернення: 22.05.2024).

					ДУ «Житомирська Політехніка».22.125.19.000 –ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		