

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(назва освітнього ступеня)

на тему: Розроблення автоматизованої системи управління відеоспостереженням в
медичному закладі

Виконав: студент IV курсу, групи КТ-41
спеціальності 151 – Автоматизація та комп'ютерно-
інтегровані технології

(шифр і назва спеціальності)

Керівник

(підпис)

(прізвище та ініціали)

Нормоконтроль

(підпис)

(прізвище та ініціали)

Завідувач кафедри

(підпис)

(прізвище та ініціали)

Рецензент

(підпис)

(прізвище та ініціали)

Тернопіль 2025

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Сенчишин Віктор Степанович, к.т.н. заступник зав. кафедри МТ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

[illegible]

Студент

(підпис)

(прізвище та ініціали)

Керівник роботи

(підпис)

(прізвище та ініціали)

Зміст

ВСТУП	6
1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ.....	8
1.1 Огляд сучасних систем відеоспостереження у медичній сфері.....	8
1.2 Аналіз аналогових і цифрових (IP) систем відеоспостереження та критерії оптимального вибору	10
1.3 Аналіз норм безпеки та конфіденційності в охороні здоров'я.....	12
1.3.1 Міжнародні стандарти конфіденційності	12
1.3.2 Національні вимоги (приклад України).....	13
1.3.3 Рекомендації щодо встановлення	13
1.4 Програмні засоби відеоаналітики	14
1.4.1 Огляд відеоаналітики.....	14
1.4.2 Основні функції відеоаналітики в охороні здоров'я.....	15
1.4.3 Приклади програмних платформ.....	16
1.4.4 Міркування щодо інтеграції.....	18
1.4.5 Обмеження та етичні проблеми.....	19
1.5 Порівняння аналогових і цифрових (IP) систем відеоспостереження та визначення оптимального вибору	20
1.5.1 Короткий огляд аналогових систем відеоспостереження.....	20
1.5.2 Огляд IP (цифрових) систем відеоспостереження.....	21
1.5.3 Визначення оптимального вибору для медичних закладів.....	22
2 ТЕОРЕТИЧНА ЧАСТИНА	24
2.1 Вибір обладнання (камери, сервери, комутатори тощо)	24
2.1.1 Камери	24
2.1.2 Мережевий відеореєстратор (NVR)	26
2.1.3 Зберігання даних	26
2.1.4 Мережева інфраструктура.....	27
2.1.5 Монітори, підключені до NVR	27

2.2 Розробка схеми розміщення камер у медичному закладі.....	30
2.2.1 Загальні принципи.....	30
2.2.2 Рекомендоване розміщення за зонами	30
2.2.3 Інтеграція зразка плану поверху.....	32
2.3 Мережева інфраструктура та методи передачі даних.....	32
2.3.1 Живлення через Ethernet (PoE)	33
3. ПРАКТИЧНА ЧАСТИНА	34
3.1 Вибір програмних рішень та середовища розгортання	34
3.1.1 Обґрунтування вибору готового рішення.....	34
3.1.2 Середовище розгортання.....	35
3.1.3 Сумісність програмного забезпечення.....	35
3.2 Інтеграція та налаштування готового інтерфейсу панелі керування (NVR/VMS).....	36
3.2.1 Початкове налаштування та конфігурація.....	36
3.2.2 Інтеграція камер	38
3.2.3 Налаштування віддаленого доступу через маршрутизатор MikroTik	40
4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ	43
4.1. Вплив шуму на організм людини та розробка заходів по зниженню його рівня.....	43
4.2. Заходи по захисту від ураження електричним струмом при роботі на автоматизованій лінії.....	45
4.3. Порядок виконання основних заходів з реагування на загрозу та виникнення надзвичайної ситуації	51
Висновки	55
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	56

ВСТУП

У сучасному світі, безпека в медичних закладах є особливо важливою. Медичні установи повинні мати високі вимоги до охорони, оскільки вони містять в собі дороге обладнання, медикаменти, особисті дані пацієнтів та повинні забезпечити постійне та безперебійне лікування. Реальними загрозами можуть бути крадіжки, неналежна поведінка відвідувачів, щоб уникнути цього потрібні ефективні технічні засоби для швидкого реагування.

Звісно у таких закладах є фізична охорона або реєстраційна, але на жаль це не гарантує повної обізнаності про ситуацію в режимі реального часу. Автоматизована система управління відеоспостереження стане важливим інструментом для підвищення рівня безпеки.

Для цього нам знадобляться:

- безперебійний відеомоніторинг важливих зон (входи, лабораторії, палати, склади);
- запис відео для розслідування та аналізу інцидентів;
- поєднання з іншими засобами безпеки (контроль доступу, сигналізація);
- віддалений доступ до відеокамер через мережу.

Більше того, впровадження таких систем забезпечує контроль за виконанням персоналом внутрішніх правил, допомагає уникнути конфліктів між пацієнтами та медичним персоналом, а також швидко і оперативно реагувати у разі виникнення екстрених ситуацій.

Ця тема набирає додаткової актуальності з урахуванням сучасних викликів, пов'язаних з кібербезпекою, забезпеченням безпеки відеоданих та необхідністю зберігати цифрову інформацію згідно з законодавчими вимогами. Тож розробка ефективної, захищеної та надійної автоматизованої системи відеоспостереження для медичного об'єкту є важливим технічним

завданням, що об'єднує в собі проектування обладнання, та безпечне управління зберіганням даних.

Крім того, пандемія COVID-19 висвітлила потребу в безконтактних, віддалених і автоматизованих рішеннях для моніторингу, особливо для карантинних зон і зон інфекційного контролю. Системи спостереження забезпечують можливість безконтактного спостереження за станом пацієнтів, поведінкою відвідувачів та дотриманням персоналом протоколів.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Огляд сучасних систем відеоспостереження у медичній сфері

Системи відеонагляду стають невід'ємною частиною сучасної інфраструктури медичних закладів, забезпечуючи як і фізичну, так і інформаційну безпеку. Їх застосування дозволяє не тільки підвищити рівень захисту пацієнтів і персоналу, а й автоматизувати всі процеси моніторингу, дотримання санітарно-гігієнічних норм і контролю за збереженням медичного обладнання.

У звіті Об'єднаної комісії (США), яка займається акредитацією медичних закладів, йдеться про те, що кількість інцидентів, пов'язаних з агресією щодо персоналу в лікарнях, постійно зростає. У зв'язку з цим необхідною умовою зниження ризиків вважається впровадження відеоспостереження в приймальних відділеннях, зонах очікування та інших ключових точках лікарень. [1]

У закладах охорони здоров'я використовуються різні типи камер спостереження: IP-камери з високою роздільною здатністю, PTZ-камери з функціями обертання і наближення, тепловізори для вимірювання температури тіла (особливо актуально під час епідемій, таких як COVID-19), а також відеодомофони для контролю доступу в зони підвищеної небезпеки. Наприклад, у клініці Клівленда (США) відеоспостереження інтегроване з системою електронного контролю доступу, що дозволяє в режимі реального часу контролювати пересування та фіксувати несанкціоновані дії [2].

У сучасних системах також широко застосовуються елементи відеоаналітики. Завдяки вбудованим алгоритмам штучного інтелекту (ШІ) можна виконувати:

- виявлення руху;
- розпізнавання обличь;

- виявлення покинутих предметів;
- виявлення випадків падіння пацієнта;
- контроль за носінням засобів індивідуального захисту (ЗІЗ).

Такі функції стануть у нагоді у відділенні інтенсивної терапії, геріатрії та психіатрії. За результатами дослідження, опублікованого в BMJ Innovations (2020), запровадження відеоспостереження у відділеннях для хворих на деменцію знизило частоту падінь на 23%, а також знизило навантаження на молодший медперсонал завдяки більш швидкому реагуванню на виклики [3].

Також за допомогою відеоспостереження контролюють дотримання санітарно-гігієнічних норм. У 2021 році Національна служба охорони здоров'я Великої Британії (NHS) запустила систему, яка фіксує обробку рук медперсоналу перед входом у зону високої стерильності. У результаті експерименту рівень дотримання гігієнічних норм підвищився на 15% [4].

Слід зазначити, що застосування відеоспостереження в медичній сфері має ґрунтуватися на дотриманні етичних і юридичних норм, зокрема, законів про захист персональних даних (GDPR в ЄС, HIPAA в США). Надмірне або неналежне використання відеокамер, особливо в місцях, де пацієнти сподіваються на приватність (палати, гардеробні, ванні кімнати), може спричинити за собою юридичні проблеми. Тому системи повинні бути технічно захищеними, з обмеженим доступом до архіву записів, логів дій користувачів та відеошифруванням.

Тож сучасні засоби відеоспостереження в медичних закладах - це не просто камери, а повноцінні інтегровані системи, які поєднують в собі обладнання, програмне забезпечення, аналіз та кібербезпеку. Вони допомагають не тільки захистити, але й підвищити якість надання медичної допомоги. [5].

1.2 Аналіз аналогових і цифрових (IP) систем відеоспостереження та критерії оптимального вибору

Відеоспостереження в медичних установах може бути реалізовано на базі аналогових або цифрових (IP) систем. Хоча аналогові камери все ще застосовуються в деяких установах, проте більшість сучасних проектів переходять на IP-технології завдяки їх більшій функціональності, можливості масштабування та адаптації.

Аналогові камери надсилають відеосигнал по коаксіальному кабелю на відеореєстратор (DVR), який веде запис, іноді з обмеженими можливостями його перегляду через мережу. Основні характеристики аналогових систем:

- невисока роздільна здатність (зазвичай до 960Н або 720р);
- низька вартість обладнання, але вища вартість кабельної мережі у великих масштабах;
- обмежені можливості взаємодії з сучасними ІТ-системами та аналітичними платформами;

У звіті IHS Markit (2019) стверджується, що до 2020 року понад 80% нових інсталяцій у секторі охорони здоров'я США вже базувалися на IP-рішеннях через технічну застарілість аналогових систем [6].

IP-камери передають дані в цифровому вигляді через комп'ютерні мережі. Вони мають вбудовані процесори, які дають змогу обробляти зображення, зберігати і передавати дані напряму на мережеві відеореєстратори (NVR), сервери або хмарні платформи. Основні переваги:

- висока роздільна здатність (від Full HD до 4K і вище);
- інтелектуальні функції (виявлення руху, розпізнавання облич, поведінкова аналітика
- гнучка масштабованість - нові камери можна без особливих зусиль додати без реконструкції кабельної мережі;

- можливість віддаленого доступу, в цьому числі через мобільні пристрої та веб-інтерфейси;
- інтеграція з лікарняними інформаційними системами і системами контролю доступу.

Крім того, сучасні IP-системи часто використовують технологію PoE (Power over Ethernet), яка забезпечує передачу живлення і даних по одному кабелю, що значно полегшує монтаж. Побачити порівняння ми можемо у таб.1.

Таблиця 1. Порівняння аналогових та IP-систем відеоспостереження

Характеристика	Аналогова система	IP-система
Якість зображення	Низька (до 720p)	Висока (Full HD, 4K, 8K)
Передача даних	Коаксіальний кабель	Ethernet, Wi-Fi, оптика
Масштабованість	Обмежена	Гнучка
Інтелектуальні функції	Немає	Вбудовані (AI, відеоаналітика)
Вартість обладнання	Низька	Вища
Вартість встановлення	Висока через кабельну базу	Нижча завдяки PoE
Можливість інтеграції	Обмежена	Висока
Доступ через Інтернет	Складний або відсутній	Стандартна функція
Захист та шифрування	Мінімальний	Високий рівень безпеки

З урахуванням специфіки сучасних медичних закладів, де важливими є питання конфіденційності, швидкого доступу до відеозаписів, аналітики поведінки пацієнтів та контролю за стерильними зонами, вибір, очевидно, падає на IP-системи. Їх адаптивність, можливості масштабування та інтеграції з медичними інформаційними системами (наприклад, PACS, HIS, EMR) роблять їх оптимальним рішенням для лікарень.

Allied Market Research (2021) прогнозує, що ринок IP-відеоспостереження в медичній сфері буде рости більш ніж на 12% щорічно до 2030 року [7], що є підтвердженням загальносвітової тенденції відходу від аналогових систем.

Аналіз показав, що IP-мережа відеоспостереження значно перевершує аналогові системи з огляду на їх функціональність, захищеність,

масштабованість та довгострокову ефективність. Попри дещо вищу початкову ціну, цифрові технології демонструють більшу надійність, автоматизацію та відповідність сучасним потребам охорони здоров'я.

1.3 Аналіз норм безпеки та конфіденційності в охороні здоров'я

Системи відеонагляду, що використовуються в секторі охорони здоров'я, потребують виконання не лише технічних, але й правових та етичних стандартів. Оскільки такі системи здатні обробляти персональні дані пацієнта та медичного персоналу, слід приділяти окрему увагу дотриманню стандартів конфіденційності, захисту даних та доступу до них.

1.3.1 Міжнародні стандарти конфіденційності

Одним із ключових нормативних актів, що регламентує обробку медичних та приватних даних, є HIPAA (Health Insurance Portability and Accountability Act), який є чинним у Сполучених Штатах Америки. Відповідно до HIPAA, будь-які системи, які можуть отримувати або зберігати інформацію про стан здоров'я пацієнтів, мають:

- надавати доступ лише вповноваженим особам;
- застосовувати шифрування відеопотоків під час передачі та зберігання;
- зберігати логи доступу до відеоархівів;
- забезпечувати фізичну та інформаційну безпеку серверів та сховищ даних.

У Європейському Союзі діє Загальний регламент про захист даних (GDPR), який потребує інформованої згоди на відеоспостереження в місцях, де воно може зачіпати особисті права людини, в тому числі і пацієнтів. Відповідно до статей 5 і 6 GDPR:

- збір персональних даних (у тому числі відеозаписів облич) мусить бути виправданим і мати обмежену мету;
- повинні бути визначені терміни зберігання даних, після чого дані підлягають видаленню;
- особи мають мати право на доступ до своїх даних, а також можливість подати скаргу на незаконне стеження.

1.3.2 Національні вимоги (приклад України)

В Україні захист персональних даних регулюється Законом України «Про захист персональних даних», а також відповідними галузевими розпорядженнями Міністерства охорони здоров'я. Системи відеоспостереження зобов'язані відповідати наступним умовам:

- не порушувати лікарську таємницю;
- розміщувати камери в межах приміщень, де надаються інтимні послуги (наприклад, гінекологічні кабінети, відділення довготривалої реабілітації);
- забезпечувати обмежений доступ до відеозаписів для не уповноважених на це осіб.

Також, важливо виконувати державні будівельні норми (ДБН) стосовно розміщення технічних пристроїв безпеки та захисту даних, якщо система зберігає дані на локальних серверах. Збір персональних даних (у тому числі відеозаписів облич) має бути обґрунтованим та обмеженим метою; мають бути встановлені терміни зберігання даних, після чого інформація підлягає знищенню; особи мають право на доступ до своїх даних, а також можливість подати скаргу на незаконне стеження.

1.3.3 Рекомендації щодо встановлення

При встановленні системи відеоспостереження в медичному закладі варто дотримуватися наступних рекомендацій:

- монтувати камери тільки в тих місцях, де це обґрунтовано з точки зору безпеки, і не вести спостереження за пацієнтами в палатах без їхньої на те згоди;
- реалізувати шифрування на рівні відеопотоку і при його архівуванні (наприклад, за стандартом AES-256);
- використовувати аутентифікацію і кількарівневий контроль доступу для працівників, які мають право на перегляд відео;
- забезпечити протоколювання дій системних адміністраторів.

Безпека та конфіденційність є ключовими компонентами при реалізації систем відеоспостереження в закладах охорони здоров'я. Застосування міжнародних стандартів (HIPAA, GDPR) і правил Privacy by Design дозволяє розробити систему, яка не тільки задовольняє технічні вимоги, але й не суперечить правам пацієнтів. Дотримання правових норм зводить до мінімуму ризик витоку персональних даних і дає змогу використовувати відеоспостереження як безпечний засіб для підтримки якості медичних послуг

1.4 Програмні засоби відеоаналітики

Сучасні системи відеоспостереження в медичних установах не зупиняються на пасивному записі та моніторингу. Замість цього вони все активніше інтегрують інтелектуальне програмне забезпечення для відеоаналітики, яке дає змогу приймати рішення в режимі реального часу, підвищує рівень обізнаності про ситуацію та автоматизує виявлення подій. У даному розділі розглядаються сучасні технології та інструменти відеоаналітики з акцентом на їх застосуванні в медичному середовищі.

1.4.1 Огляд відеоаналітики

Відеоаналітика – це застосування алгоритмів, часто заснованих на штучному інтелекті і машинному навчанні, для автоматичного аналізу

відеоконтенту. Ці програми можуть виявляти закономірності, виявляти певні події та формувати сповіщення без втручання людини.

У сфері охорони здоров'я застосування відео аналітика допомагає підвищити безпеку пацієнтів, покращити ефективність роботи та захистити чутливі зони, такі як палати інтенсивної терапії, відділення невідкладної допомоги та сховища лікарських препаратів.

1.4.2 Основні функції відеоаналітики в охороні здоров'я

Ключові функції відеоаналітики, що мають значення для медичних установ, включають в себе наступні:

- виявлення руху - виявлення сторонніх рухів у зонах з обмеженнями доступу.
- розпізнавання облич - керування контролем доступу та відстеження присутності персоналу з урахуванням правил конфіденційності, таких як GDPR і HIPAA.
- виявлення бездіяльності - розпізнавання людей, які довго затримуються в критичних місцях, наприклад, біля аптечок або серверів з даними.
- підрахунок людей - контроль заповнюваності зон очікування або підрахунок кількості персоналу в операційних.
- виявлення падінь - сповіщення персоналу в режимі реального часу про падіння пацієнта, особливо в геріатричних або реабілітаційних відділеннях.
- виявлення носіння персоналом засобів індивідуального захисту - забезпечення носіння персоналом засобів індивідуального захисту , зокрема під час спалахів інфекційних захворювань або в місцях зі стерильною зоною.

Ці можливості зменшують потребу в постійному візуальному контролі та забезпечують вищий рівень догляду за пацієнтами та безпеки в лікарні.

1.4.3 Приклади програмних платформ

Кілька комерційних платформ відеоаналітики з відкритим програмним кодом широко використовуються в галузі охорони здоров'я та інших сферах. Основні приклади включають:

- Milestone XProtect з XProtect Smart Client: Масштабоване програмне забезпечення для управління відео (VMS) з підтримкою плагінів для розумної аналітики. Пропонує інтеграцію з модулями штучного інтелекту для розпізнавання облич, стеження за рухом і розпізнавання номерних знаків [8].
- Avigilon Control Center (Motorola Solutions): Включає вбудовані аналітичні функції на основі штучного інтелекту, такі як виявлення незвичайного руху (UMD), пошук за зовнішністю (Appearance Search) і пошук ідентифікаційних даних,
 - призначені для використання в критично важливих умовах, наприклад, в лікарнях [9].
- Axis Camera Station + AXIS Object Analytics: Розроблений компанією Axis Communications, він пропонує виявлення
 - об'єктів, людей і поведінки з урахуванням конфіденційності та шифрування [10].
- OpenCV та TensorFlow (з відкритим вихідним кодом): Часто використовуються для розробки відео аналітики в дослідженнях і створенні нових прототипів. Ці бібліотеки надають підтримку моделям поглибленого навчання для виявлення об'єктів у реальному часі, оцінки пози та розпізнавання активності [11].
- BriefCam: Відома своїми функціями відеосинопсису та судово-медичного пошуку, що дозволяє дослідникам переглядати багатогодинні відеозаписи за лічені хвилини, підсумовуючи відповідні дії або події [12].

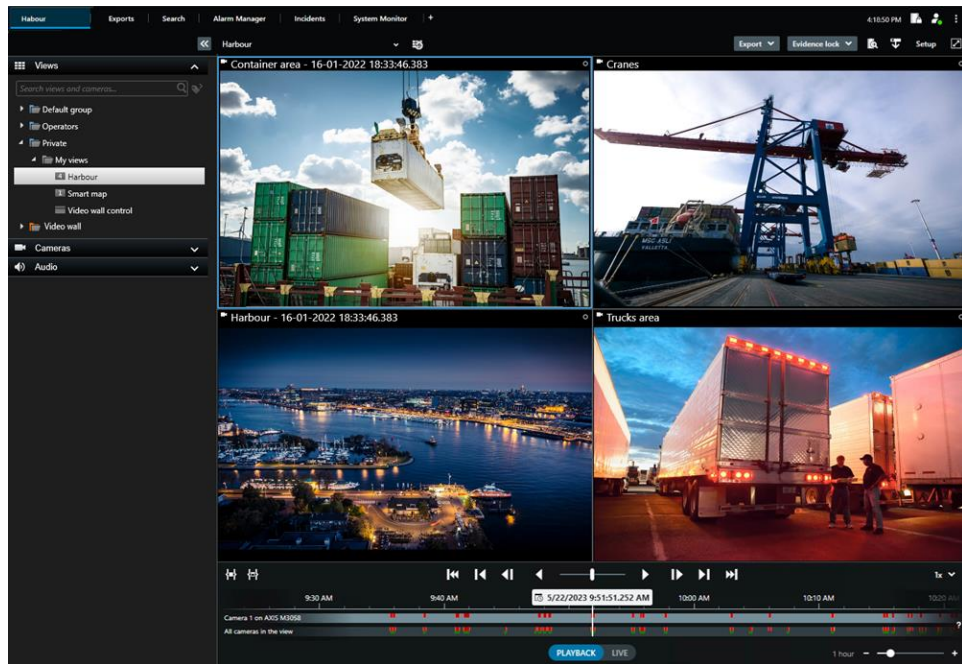


Рисунок 1.1 - Интерфейс Milestone XProtect



Рисунок 1.2 - Интерфейс Avigilon Control Center

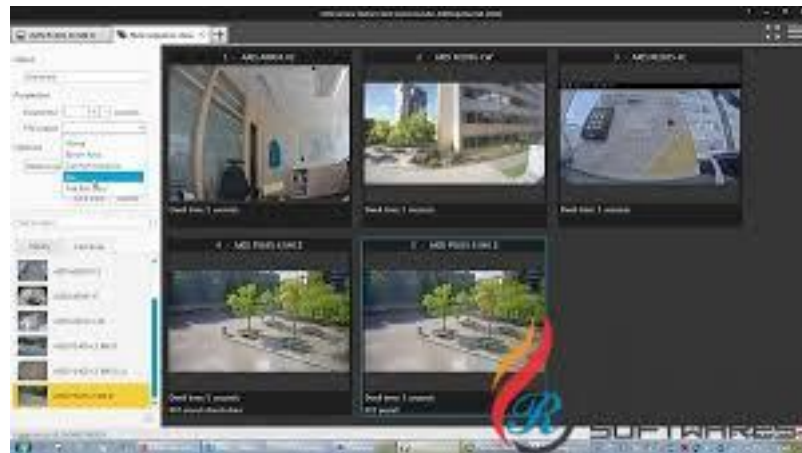


Рисунок 1.3 - Інтерфейс Axis Camera Station

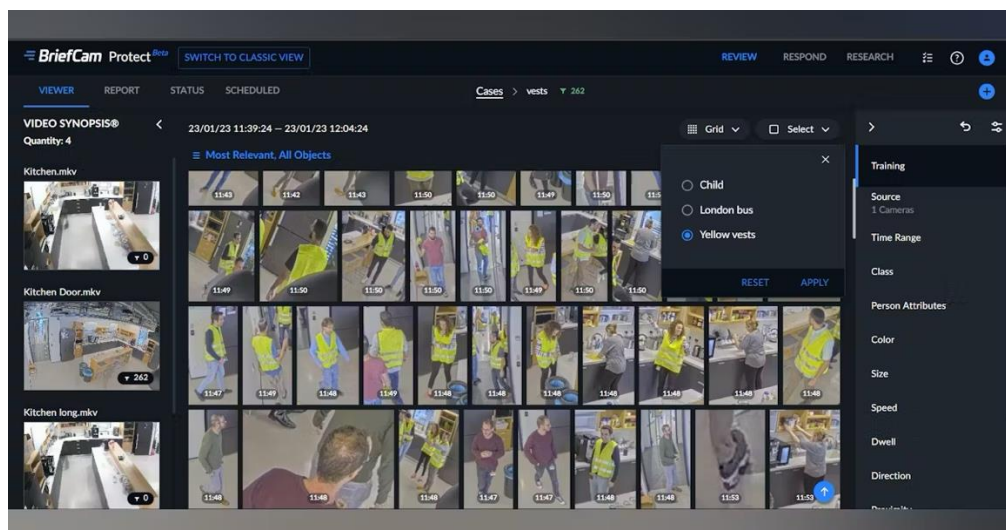


Рисунок 1.4 - Інтерфейс BriefCam

1.4.4 Міркування щодо інтеграції

При виборі інструменту відеоаналітики для медичного закладу необхідно врахувати кілька важливих аспектів інтеграції:

- сумісність з наявною мережею камер (IP або аналоговими системами через енкодери);
- час затримки та обчислювальна потужність, необхідна для аналітики в реальному часі;
- політика щодо зберігання даних, особливо для відеопотоків високої якості;

- безпека та дотримання норм конфіденційності - підтримка шифрування, анонімності та обмеження доступу;
- масштабованість - здатність до розширення системи в різних відділах або на різних об'єктах.

1.4.5 Обмеження та етичні проблеми

Попри свої переваги, системи відеоаналітики також несуть у собі певні ризики:

- точність і помилкові спрацьовування - алгоритми можуть невірно сприймати події, що призводить до зайвих сповіщень або пропуску інцидентів;
- упередженість моделей ШІ - недостатньо навчені моделі можуть працювати неефективно на різних групах населення;
- ризики для приватності - без належних заходів безпеки ШІ може неумисно розкрити конфіденційну інформацію про поведінку або особистість пацієнта.

Щоб вирішити ці проблеми, системи повинні розгортатися прозоро, із залученням зацікавлених сторін і дотриманням міжнародних етичних норм.

Програмне забезпечення для відеоаналізу виконує важливу роль у сучасних системах відеоспостереження в охороні здоров'я. Завдяки автоматизації, швидкому виявленню інцидентів та аналізу оперативної інформації, засоби відеоаналітики сприяють підвищенню безпеки та якості надання медичної допомоги. Однак впровадження таких технологій має здійснюватись на основі надійних механізмів захисту конфіденційності та з урахуванням етичних міркувань, гарантуючи, що технічні інновації відповідають правам і повазі до людської гідності пацієнтів і медичного персоналу.

1.5 Порівняння аналогових і цифрових (IP) систем відеоспостереження та визначення оптимального вибору

З розвитком технологій відеоспостереження відбувся суттєвий перехід від традиційних аналогових систем до сучасних цифрових систем на основі Інтернет-протоколу (IP). В сфері охорони здоров'я, де безпека, якість даних і можливість реагування в режимі реального часу є вкрай важливими, вибір правильної архітектури системи відеоспостереження має велике значення. У цьому розділі наведено порівняльний аналіз аналогових і IP-систем відеоспостереження та обґрунтовано вибір найбільш відповідного рішення для медичних установ.

1.5.1 Короткий огляд аналогових систем відеоспостереження

Аналогові системи відеоспостереження (Closed-Circuit Television, CCTV) використовувалися протягом десятиліть і досі працюють у багатьох застарілих інфраструктурах. Ці системи передають відеосигнали коаксіальними кабелями (рис.1.5) на цифрові відеореєстратори (DVR), де зберігаються і переглядаються відзняті матеріали.

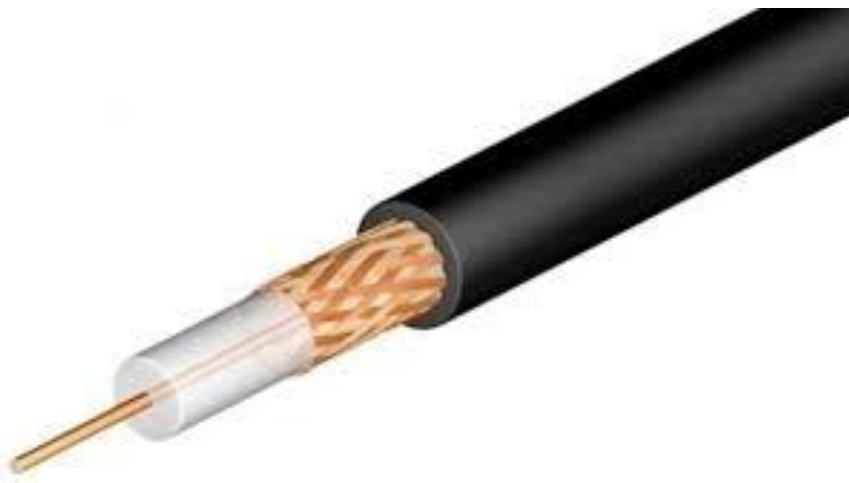


Рисунок 1.5 - Коаксіальний кабель

Переваги аналогових систем:

- менша початкова вартість - обладнання (камери, кабелі), як правило, дешевші, ніж IP-альтернативи;
- простота - простота встановлення та налаштування в невеликих приміщеннях;
- низькі вимоги до пропускну здатності - так як дані не передаються через IP-мережі, навантаження на IT-інфраструктуру лікарні мінімальне.

Недоліки:

- низька якість зображення - обмежена стандартною роздільною здатністю, хоча деякі системи зараз пропонують аналогове зображення високої чіткості (наприклад, HD-CVI, HD-TVI);
- проблеми з масштабуванням - можливість розширення обмежена і часто потребує значного перемонтажу кабелів;
- відсутність інтелектуальної аналітики - аналогові системи переважно не підтримують відеоаналітику, дистанційний доступ або інтеграцію з іншими цифровими системами;
- обмежена інтеграція - аналогові камери не підтримують зв'язок з сучасними лікарняними IT-системами, такими як системи контролю доступу або платформи оповіщення.

1.5.2 Огляд IP (цифрових) систем відеоспостереження

IP-системи відеоспостереження використовують підключені до мережі камери, які передають цифрові дані через Ethernet або Wi-Fi. Ці системи зберігають відзнятий матеріал на мережевих відеореєстраторах (NVR) або в хмарних сховищах і підтримують функції централізованого управління, автоматизації та розширеної аналітики.

Переваги IP-систем:

- відео високої роздільної здатності - від HD до 4K+, що є критично важливим для ідентифікації подій або окремих осіб у медичних установах;

- масштабованість і гнучкість - легко розширюється у відділеннях або на поверхах без значних змін у мережі;
- розширені функції - включають виявлення руху, розпізнавання облич, підрахунок людей, виявлення проникнень і навіть виявлення випадків падіння на основі штучного інтелекту;
- віддалений доступ - дозволяє уповноваженому персоналу переглядати відеозаписи в реальному часі з будь-якого місця, що підвищує швидкість реагування;
- інтеграція - можливість безперешкодного підключення до лікарняних інформаційних систем, контролю доступу, сигналізації та механізмів реагування на надзвичайні ситуації.

Недоліки:

- вища вартість на початковому етапі - потребує витрат на мережеву інфраструктуру, камери, сховища та програмне забезпечення;
- вимоги до пропускну здатності - може потребувати модернізації мережі для обробки потокового відео високої роздільної здатності та зберігання даних;
- проблеми з кібербезпекою - IP-системи необхідно належним чином захистити, щоб запобігти витоку даних або несанкціонованому доступу до них.

1.5.3 Визначення оптимального вибору для медичних закладів

Враховуючи особливості медичного середовища, включаючи безпеку пацієнтів, цілодобове відеоспостереження, дотримання вимог нормативних актів та охоплення великої території, системи на основі IP є найбільш оптимальним вибором для сучасних медичних закладів.

Хоча аналогові системи все ще корисні в невеликих клініках або клініках з невеликим бюджетом, переваги IP-систем значно перевищують їхню початкову вартість. Вони забезпечують не тільки вищу якість відео та

універсальність, але й відкривають можливості автоматизації, аналітики та віддаленого управління - функції, необхідні для управління безпекою в лікарні.

Крім того, ІР-системи більш тісно пов'язані з майбутнім «розумних» лікарень, де дані відеоспостереження будуть інтегровані з Інтернетом речей, електронними медичними картами і автоматизованими системами реагування на надзвичайні ситуації.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Вибір обладнання (камери, сервери, комутатори тощо)

Успішне впровадження системи відеоспостереження в медичному закладі залежить від правильного вибору комплектуючих. Ці комплектуючі повинні відповідати вимогам до продуктивності, надійності та масштабованості, а також урахуванням специфічних потреб медичних закладів, включаючи цілодобовий моніторинг, конфіденційність пацієнтів та інтеграцію з існуючою ІТ-інфраструктурою.

У цьому розділі описано критерії вибору та обґрунтування основних комплектуючих, що використовуються в пропонованій системі.

2.1.1 Камери

Вибраний тип: IP-камери (Hikvision)

Приклади моделей:

- Hikvision DS-2CD2087G2-L(U) (фіксований об'єктив, 8 МП, рис. 2.1)
- Hikvision DS-2DE4A425IW-DE (PTZ, 25-кратний оптичний зум, рис. 2.2)



Рисунок 2.1 – Hikvision DS-2CD2087G2-L(U)



Рисунок 2.2 – Hikvision DS-2DE4A425IW-DE

Критерії вибору:

- Роздільна здатність: мінімум Full HD (1080p), з покриттям ключових зон (входи, реанімація) 4K.
- Працювання в умовах низької освітленості: необхідне для нічного спостереження без постійного освітлення. Перевага надається моделям з технологією IR або ColorVu.
- Погодостійкість: камери для зовнішнього використання повинні мати захист IP66/IP67.
- Непомітний форм-фактор: для приміщень, де перебувають пацієнти, вибираються купольні камери, щоб уникнути дискомфорту.
- Підтримка інтелектуального аналізу: виявлення руху, зони вторгнення, перетин лінії та підрахунок людей.
- Стратегія розміщення:
 - Коридори та палати: фіксовані купольні камери.
 - Входи, вестибюлі: камери типу «купольна».
 - Периметр: камери PTZ для зовнішнього використання.
 - Критичні зони (відділення інтенсивної терапії, аптека): камери з високою роздільною здатністю та обмеженим доступом.

2.1.2 Мережевий відеореєстратор (NVR)

Обраний пристрій: Hikvision NVR DS-7732NXI-I4/16P/S (рис.2.3)

Основні характеристики:

- Підтримує до 32 IP-каналів.
- Вбудовані порти PoE для прямого підключення камер.
- Вбудовані аналітичні функції: розпізнавання облич, пошук руху.
- Подвійні відеопотоки для перегляду в реальному часі та оптимізації запису.
- Підтримка RAID для резервування жорстких дисків.

Обраний NVR здатний задовольнити як поточні потреби, так і майбутні вимоги. Він забезпечує віддалений доступ через Hik-Connect і легко інтегрується в мережу лікарні для централізованого управління.



Рисунок 2.3 – Hikvision NVR DS-7732NXI-I4/16P/S

2.1.3 Зберігання даних

- Жорсткі диски: Жорсткі диски для систем відеоспостереження (наприклад, Western Digital Purple або Seagate SkyHawk)
- Ємність: мінімум 6–12 ТБ залежно від якості запису та політики зберігання (зазвичай 30 днів).
-

2.1.4 Мережева інфраструктура

Комутатори PoE

– Комутатори PoE(наприклад, Ubiquiti, TP-Link JetStream або Hikvision DS-3E).

- Повинні підтримувати:
- Стандарти PoE IEEE 802.3af/at.
- Гігабітні канали зв'язку.

Кабелі

– Кабелі Cat 6 UTP (рис 2.4) для підключення камер, що забезпечують достатню пропускну здатність і подачу живлення PoE.

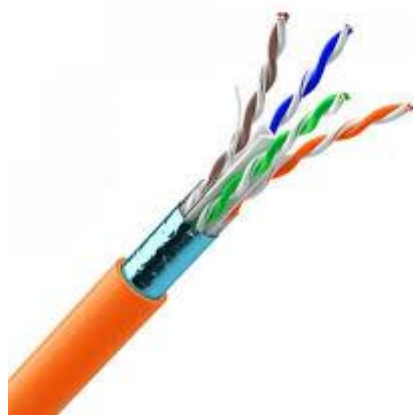


Рисунок 2.4 – Кабель Cat 6 UTP

Джерело безперебійного живлення

– Джерела безперебійного живлення (UPS) для NVR і комутаторів для забезпечення безперебійної роботи під час відключень електроенергії.

2.1.5 Монітори, підключені до NVR

У багатьох системах спостереження в лікарнях основний відеопотік відтворюється на одному або декількох моніторах, безпосередньо підключених до NVR (мережевого відеореєстратора). Така конфігурація забезпечує просте, стабільне та економічне рішення для безперервного

спостереження в режимі реального часу без необхідності використання окремого комп'ютера.

Монітори, підключені до NVR, використовуються для:

- перегляду в реальному часі потоків з камер у місцях з інтенсивним рухом або в критичних зонах (наприклад, головний вхід, приймальне відділення, реанімація);
- відтворення записаних відеозаписів через вбудований інтерфейс NVR;
- налаштування та керування системними параметрами за допомогою підключеної миші або інфрачервоного пульта дистанційного керування.

Більшість NVR, включаючи пристрої Hikvision, підтримують:

- HDMI (основний вихід для дисплеїв з високою роздільною здатністю, наприклад 1080p або 4K)
- VGA (додатковий вихід для моніторів зі старою технологією та нижчою роздільною здатністю)
- Порт HDMI, як правило, використовується для основного монітора завдяки кращій якості зображення.

Приклади моделей моніторів:

- Dell P2422H – 24” Full HD, IPS, HDMI + DisplayPort (рис. 2.5)
- Samsung UJ59 (LU28R550UQNXZA) – 28” 4K UHD, підходить для перегляду з декількох камер (рис. 2.6)



Рисунок 2.5 – Монітор Dell P2422H



Рисунок 2.6 – Монітор Samsung UJ59

Практичні міркування:

- Розмістіть монітор у безпечному місці з обмеженим доступом, щоб запобігти незаконному втручанню.
- Підключіть USB-мишу до мережевого відеореєстратора для зручної навігації.
- Налаштуйте параметри дисплея в меню мережевого відеореєстратора: макет (наприклад, 4×4, 3×3), поворот камери, екранні мітки.

2.2 Розробка схеми розміщення камер у медичному закладі

Правильне розміщення камер має ключове значення для дотримання основних цілей системи відеоспостереження в лікарні — забезпечення безпеки, захисту майна, моніторингу важливих зон та дотримання законів про конфіденційність. У цьому розділі йдеться про стратегію розробки ефективної та етичної схеми розміщення камер у різних зон медичного закладу.

2.2.1 Загальні принципи

При розробці схеми розташування камер для медичного закладу необхідно дотримуватися таких принципів:

- Зонування: розділіть будівлю на зони за рівнем ризику, функціональним призначенням та рівнем доступу.
- Конфіденційність: уникайте встановлення камер у зонах, де важлива конфіденційність пацієнтів (наприклад, у палатах, туалетах).
- Дублювання: якщо це можливо, переконайтеся, що критично важливі зони охоплюються більш ніж однією камерою.
- Контроль входу/виходу: Постійно стежте за входами та виходами, щоб відстежувати доступ та можливі вторгнення.
- Умови освітлення: Обирайте моделі камер, які відповідають освітленню кожної зони (моделі з інфрачервоним випромінюванням або для слабого освітлення в темних зонах).
- Висота монтажу: Камери слід встановлювати на висоті 2,5–3 метри в приміщенні та 3–4 метри на вулиці, щоб уникнути пошкодження та забезпечити чітке поле огляду.

2.2.2 Рекомендоване розміщення за зонами

У межах медичного закладу відеокамери повинні бути розміщені відповідно до функціонального призначення зон та потреб у безпеці. Одними

з ключових місць для встановлення камер є головні входи та аварійні виходи. В цих зонах рекомендується використовувати фіксовані кульові або поворотні камери з ширококутним об'єктивом та високою роздільною здатністю (не менше 4 МП), які дозволяють ефективно фіксувати всіх осіб, що входять або залишають приміщення. Необхідно передбачити функцію ведення журналу з позначками часу, а також нічне бачення — наприклад, за допомогою ІЧ-підсвічування або технології ColorVu.

У коридорах та загальних зонах доцільно встановлювати купольні камери з варіфокальними об'єктивами на стелі. Вони забезпечують ефективне відстеження руху персоналу, пацієнтів та відвідувачів. Для таких камер бажано реалізувати функції виявлення руху, використання режиму "коридор" (що дозволяє краще охопити вузькі простори) та сигналізацію при спробі втручання.

Кімнати очікування та приймальні вимагають нагляду за взаємодією пацієнтів з персоналом та можливістю виявлення незвичайної поведінки або агресії. У таких приміщеннях слід застосовувати вандалостійкі купольні камери, а за наявності правових підстав — активувати функцію аудіозапису. Для кращої якості зображення у зонах з нерівномірним освітленням бажано обрати моделі з підтримкою HDR (високого динамічного діапазону).

У відділеннях інтенсивної терапії та біля операційних рекомендується встановлювати камери виключно ззовні, біля дверей, щоб не порушувати конфіденційність пацієнтів. Для цього підходять купольні або міні-кульові камери. Вони повинні мати можливість реагувати на події доступу та надсилати сповіщення у разі виявлення руху.

Кімнати для зберігання медикаментів та аптеки мають потребу у суворому контролі. Тут встановлюються фіксовані камери з високою роздільною здатністю, орієнтовані на зони зберігання або двері. Доцільно налаштувати розумні сповіщення про відкриття дверей та інтегрувати відеонагляд із системами контролю доступу.

У ліфтах та на сходових клітках для контролю вертикального переміщення й аварійної евакуації використовуються міні-купольні камери з ширококутними об'єктивами. Вони мають підтримувати запис, що активується рухом, а також мати функцію цифрового 3D-шумозаглушення для покращення якості зображення.

Зовнішні та периметральні зони медичного закладу є ключовими для виявлення порушень периметра. У цих місцях слід встановлювати PTZ або кульові камери з великим радіусом дії, здатні виконувати автоматичне відстеження об'єктів, виявлення перетину віртуальної лінії та вторгнень на охоронювану територію.

2.2.3 Інтеграція зразка плану поверху

- Добре структурований план поверху повинен містити:
- Пронумеровані позиції камер
- Прокладка кабелів живлення та передачі даних (бажано через PoE)
- Ключові зони з рекомендованою роздільною здатністю та типами камер

Завдяки оптимізованій схемі розміщення камер лікарня дотримується балансу між безпекою, оперативним наглядом та етичною відповідальністю. Кожна камера розташована в оптимальному місці для виконання конкретного завдання, мінімізації сліпих зон та забезпечення майбутньої розширюваності системи.

2.3 Мережева інфраструктура та методи передачі даних

Надійна та безпечна мережа є основною складовою будь-якої системи IP-відеоспостереження. У медичних установах, де критично важливим є безперебійність роботи, захист даних та доступ до відео в режимі реального

часу, проектування мережевої інфраструктури має відповідати найсучаснішим вимогам щодо швидкості, сегментації та резервування.

У цьому розділі описано архітектурні принципи та методи передачі даних, обрані для системи відеоспостереження.

2.3.1 Живлення через Ethernet (PoE)

PoE полегшує встановлення, зменшуючи кількість необхідних окремих джерел живлення.

- Стандарт: IEEE 802.3af (15,4 Вт), 802.3at (PoE+, 30 Вт)
- Випадок використання: Більшість сучасних IP-камер, включаючи інфрачервоні та моторизовані, повністю підтримуються PoE+.
- Комутатори: Рекомендується використовувати керовані комутатори PoE (наприклад, серія Hikvision DS-3E як на рис 2.7).



Рисунок 2.7 – PoE комутатор Hikvision DS-3E

Слід переконатися, що комутатори PoE мають достатню потужність для всіх підключених пристроїв.

3. ПРАКТИЧНА ЧАСТИНА

3.1 Вибір програмних рішень та середовища розгортання

При проектуванні сучасної системи відеоспостереження для медичного установи вибір відповідного програмного забезпечення та середовища розгортання є надзвичайно важливим рішенням, яке безпосередньо впливає на надійність, зручність використання, масштабованість та безпеку системи. Замість розробки власної платформи управління відео з нуля, в цьому проекті використовується готове рішення від Hikvision, одного з провідних світових виробників технологій відеоспостереження.

3.1.1 Обґрунтування вибору готового рішення

Використання готової комерційної системи, такої як мережевий відеореєстратор (NVR) або HikCentral Professional від Hikvision, має кілька ключових переваг:

- Стабільність і надійність: системи Hikvision мають широке застосування в лікарнях, аеропортах, школах і проектах міського відеоспостереження, що свідчить про їхню довготривалу стабільність.
- Простота інтеграції: пристрої підтримують провідні галузеві стандарти, такі як ONVIF і RTSP, що спрощує підключення IP-камер і пристроїв інших виробників.
- Вбудовані функції: системи оснащені попередньо встановленим програмним забезпеченням для відеозапису, виявлення руху, розумних сповіщень про події та управління доступом користувачів.
- Економічність: використання готових систем на базі NVR дозволяє скоротити витрати на розробку програмного забезпечення, заощаджуючи час і фінанси.

- Технічна підтримка та документація: Hikvision пропонує розширену документацію, оновлення прошивки та локалізовану технічну підтримку.

3.1.2 Середовище розгортання

Програмне забезпечення для відеоспостереження розташоване на спеціальному мережевому відеореєстраторі (NVR), що знаходиться в захищеній серверній лікарні. Цей NVR підключений до локальної мережі через комутатори PoE, що дозволяє одночасно передавати дані та живити всі IP-камери в системі.

Основні компоненти середовища розгортання включають:

- Hikvision NVR (наприклад, DS-7732NI-I4) з підтримкою 32 каналів і вбудованим сховищем
- Гігабітні комутатори PoE (наприклад, серія Hikvision DS-3E)
- Робоча станція з клієнтським програмним забезпеченням Hik-Connect або iVMS-4200 для моніторингу та відтворення в режимі реального часу

Система налаштовується за допомогою веб-інтерфейсу або локального монітора, підключених безпосередньо до NVR, що спрощує встановлення та зменшує потребу в додаткових серверах.

3.1.3 Сумісність програмного забезпечення

Платформа Hikvision підтримує:

- Стиснення H.265 / H.265+ для зниження пропускної здатності
- Дистанційний доступ через мобільний додаток (Hik-Connect) для авторизованих користувачів
- Розподіл прав доступу за ролями для визначення прав адміністратора/оператора

- Інтеграція з системами інших виробників через ONVIF або Hikvision SDK, якщо потрібно
- Таке обладнання забезпечує безперебійну роботу системи відеоспостереження в інфраструктурі лікарні з урахуванням вимог до пропускної здатності, зберігання даних та безпеки.

3.2 Інтеграція та налаштування готового інтерфейсу панелі керування (NVR/VMS)

Інтеграція та налаштування готової системи управління відео є важливою частиною розгортання функціонального та зручного рішення для відеоспостереження. У цьому проекті Hikvision NVR (мережевий відеореєстратор) виконує роль центрального вузла для відеоспостереження, запису та керування пристроями. Замість розробки власного інтерфейсу користувача, система використовує вбудовану панель інструментів, що надається NVR.

3.2.1 Початкове налаштування та конфігурація

Після фізичної установки NVR і підключення до локальної мережі було виконано наступні кроки:

- Вхід і ініціалізація: Доступ до системи було отримано через локальний дисплей HDMI і налаштовано за допомогою USB-миші. Початкове налаштування включало встановлення пароля адміністратора, визначення часового поясу як вказано на рис. 3.1 та увімкнення доступу до мережі.
- IP-адресація: NVR було присвоєно статичну IP-адресу як вказано на рисунку(нижче) для забезпечення стабільного з'єднання в межах внутрішньої мережі лікарні.

– Оновлення прошивки: Прошивка NVR була оновлена до останньої стабільної версії(як вказано на рис. 3.3) для забезпечення сумісності з новими функціями та покращення безпеки.

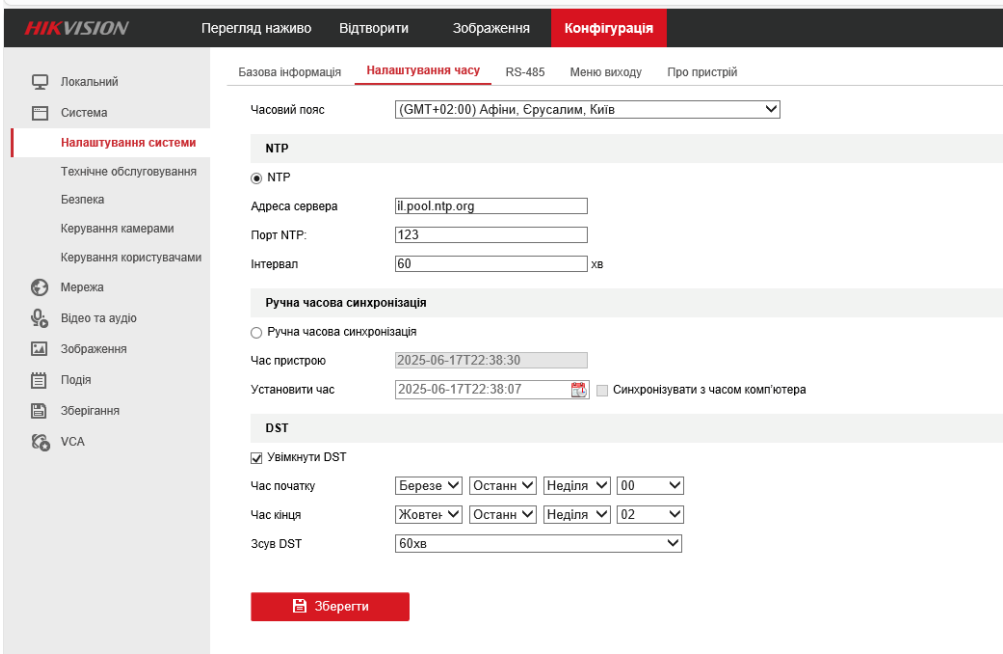


Рисунок 3.1 – Визначення часового поясу

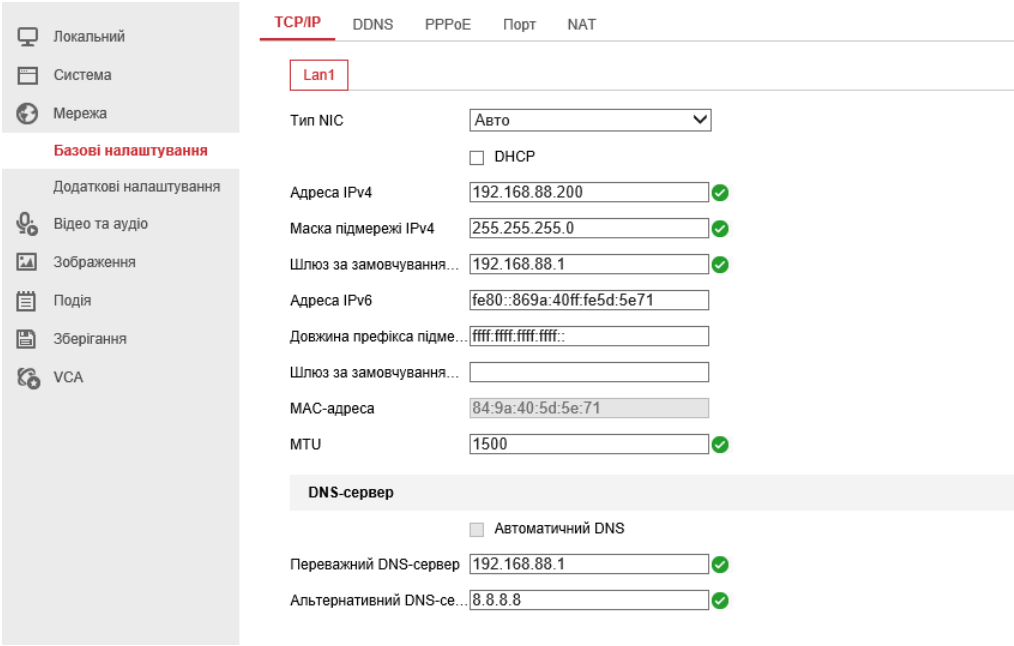


Рисунок 3.2 – Присвоєння статичної IP-адреси

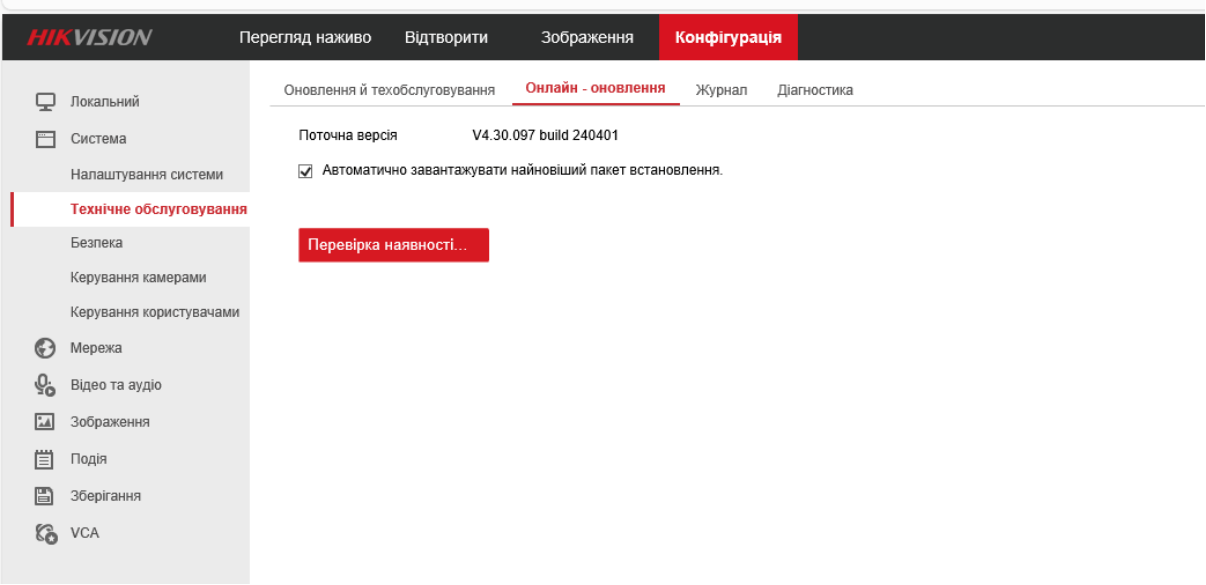


Рисунок 3.3 – Оновлення до останньої стабільної версії

3.2.2 Інтеграція камер

ІР-камери були підключені до портів PoE на NVR і через мережеві комутатори. Система автоматично виявила пристрої, сумісні з Hikvision, а камери сторонніх виробників, сумісні з ONVIF, були додані вручну.

Конфігурація включала:

- Присвоєння імені кожній камері за місцем розташування (наприклад, «ER_VHID », «ICU_STREET_1») як вказано на рис. 3.4
- Призначення графіків запису (як вказано на рис. 3.5) (безперервний, на основі руху, за подіями)
- Налаштування параметрів зображення (роздільна здатність, частота кадрів, яскравість тощо) як вказано на рис. 3.6

☐	Номер каналу	Назва камери	ІР-адреса	Номер каналу	Порт управління	Безпека	Статус	Протокол
☐	D1	DNZ-15_Street1	192.168.88.201	1	8000	Слабкий па...	Онлайн	HIKVISION
☐	D2	DNZ-15_Street2	192.168.88.202	1	8000	Слабкий па...	Онлайн	HIKVISION
☒	D3	DNZ-15_VHID	192.168.88.203	1	8000	Слабкий па...	Онлайн	HIKVISION

Рисунок 3.4 – Присвоєння імені кожній камері

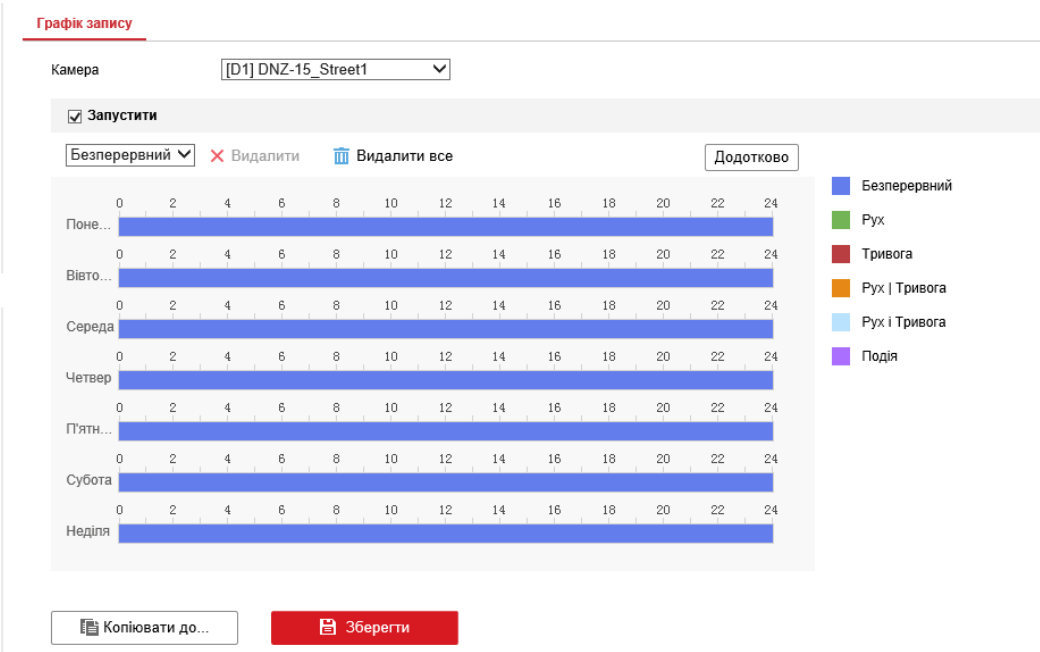


Рисунок 3.5 – Призначення графіків запису

Відео Показати інформацію в потоці Нульовий канал

Камера: [D1] DNZ-15_Street1

Тип потоку: Основний потік (у нормі)

Тип відео: Відеопотік

Роздільна здатність: 2688*1520

Тип бітрейту: Змінна

Якість відео: Середній

Частота кадрів: Повна частота кадрів fps

Макс. бітрейт: 3072 Kbps

Кодування відео: H.265

H.265+: ВИМК.

Рисунок 3.6 – Налаштування параметрів зображення

3.2.3 Налаштування віддаленого доступу через маршрутизатор MikroTik

Для увімкнення віддаленого доступу та адміністрування системи відеоспостереження віддалений доступ до NVR налаштовується за допомогою переадресації портів на маршрутизаторі MikroTik. Це дозволяє переглядати потокові відео та відтворювати записи з-поза меж локальної мережі лікарні через веб-інтерфейс, мобільний додаток (Hik-Connect)

Кроки для налаштування переадресації портів на MikroTik

- Увійти в MikroTik RouterOS:
- Отримати доступ можна через WinBox або веб-інтерфейс використовуючи локальну IP-адресу маршрутизатора.

- Створити правило NAT для переадресації портів:
- Перейдіть до IP > Firewall > NAT як вказано на рис 3.6.
- Додайте нове правило з такими параметрами як вказано на рис. 3.7

і 3.8:

- Chain: dstnat
- Протокол: tcp
- Dst. Port: 8000
- In. Interface: (ваш інтернет-інтерфейс, наприклад, ether1)
- Action: dst-nat
- To Address: 192.168.88.200
- To ports: 8000 (або те саме, що Dst. Port)

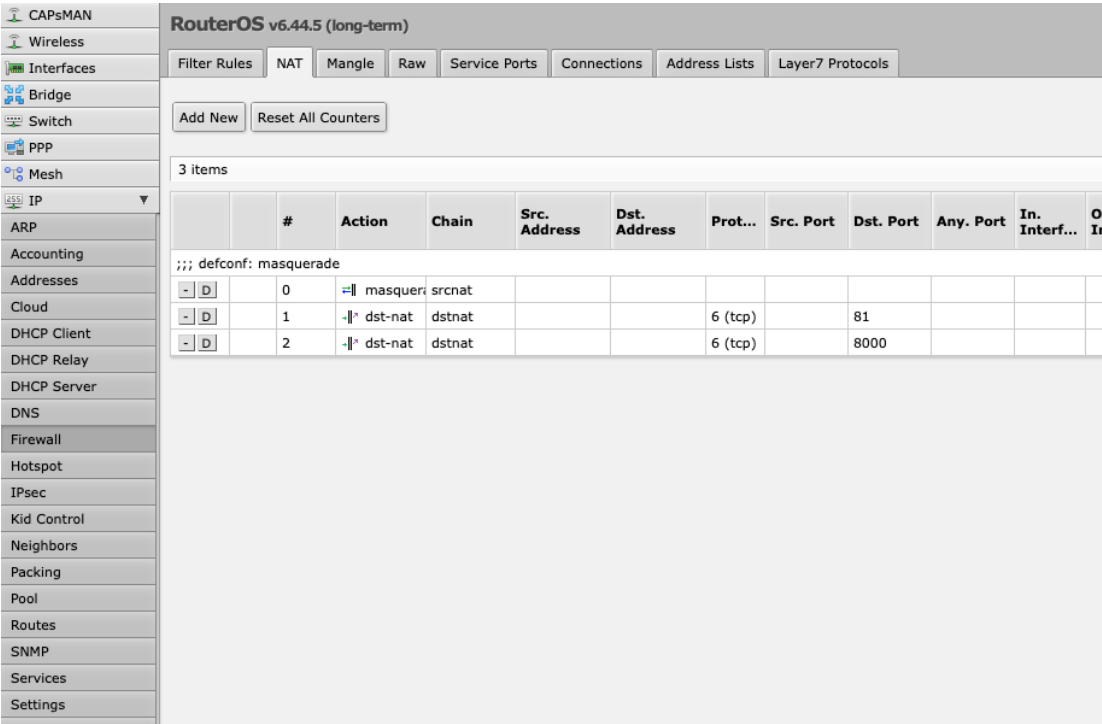


Рисунок 3.7 – NAT

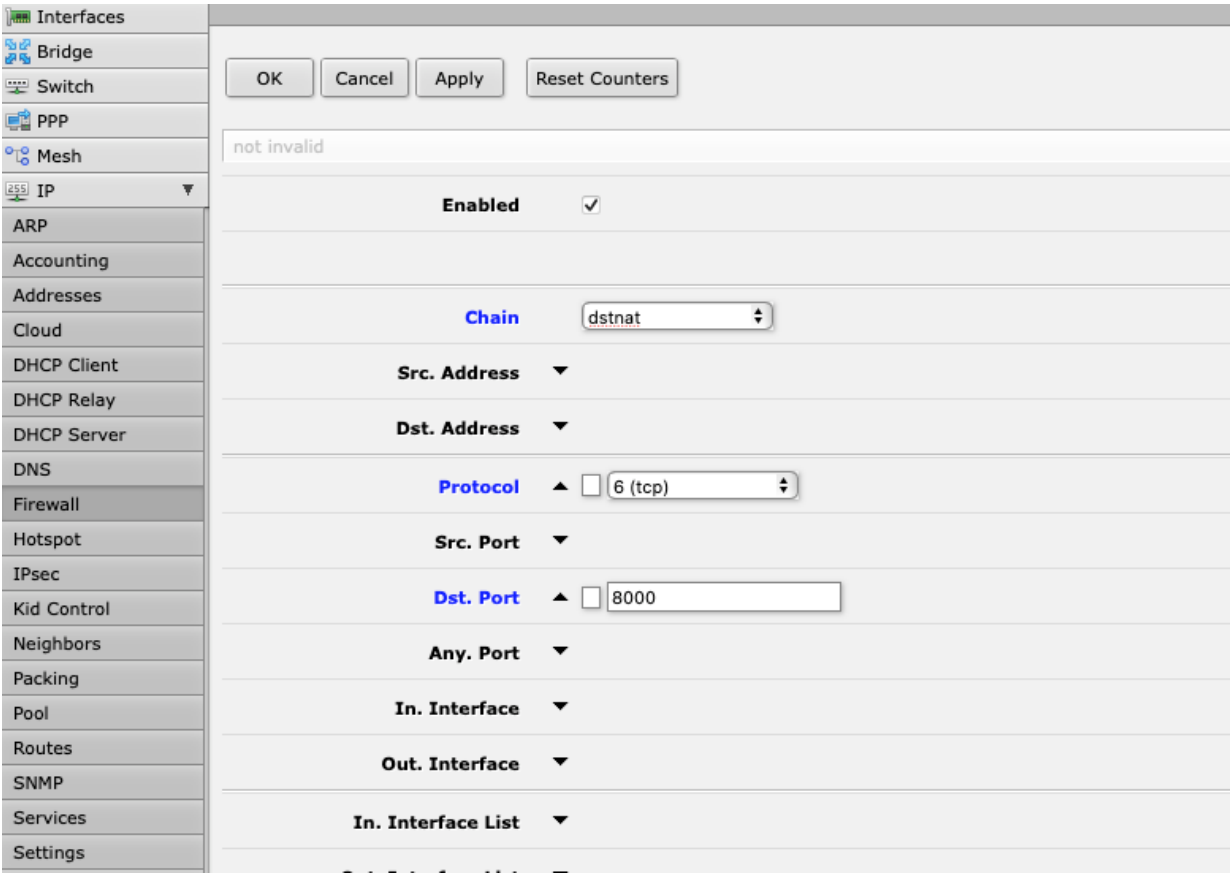


Рисунок 3.8 – Створення правила

Hotspot	▼
IP Fragment	▼
Action	dst-nat
Log	☐
Log Prefix	▼
To Addresses	192.168.88.200
To Ports	8000
Bytes	0 B
Packets	0
Rate	0 bps
Packet Rate	0 p/s

Рисунок 3.9 – Створення правила

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1. Вплив шуму на організм людини та розробка заходів по зниженню його рівня

Як відомо різні машини, механізми і агрегати, які використовуються на виробництві в багатьох випадках являються динамічно нестійкими. Їх робота супроводжується шумом і вібрацією.

Боротьба із шумом проводиться по трьох напрямках: зменшення шуму конструктивним і технологічним методами; зниження шуму методом обмеження; зменшення шкідливості шуму методом індивідуального захисту працюючих, зміною режимів роботи і відпочинку. Найбільший ефект дають конструктивні і технологічні заходи [23].

Шум розповсюджується, від джерела двома шляхами.

- по повітрі;
- по матеріалу конструкції.

В другому випадку слід використовувати ізолюючі прокладки, пружини або вібро- чи звукопоглиначі. Найбільший ефект одержують при використанні звукопоглинаючих пристроїв повної ізоляції.

Для захисту працюючих від прямої дії звукової енергії використовують відбивачі, екрани.

В тих випадках, коли шум передається по повітрі використовують ізоляції джерела шуму (бокси, звукопоглинаючі капоти).

Стандарт, який розповсюджується на машини, технологічне обладнання і інші джерела шуму відповідає ГОСТ 12.1-003-83 „Шум”. Для виміру рівня звукового тиску використовують шумоміри 1-го і 2-го класу по ГОСТ 17 187-81.

У розробленій, в дипломному проекті, автоматичній лінії шум виникає від роботи електродвигунів, насосів, зубчатих передач.

Розповсюджується шум як по повітрі, так і по матеріалу конструкції, додатково шум розповсюджується по трубопроводах. Тому для зниження шуму використовують слідуючі заходи: для зменшення шуму по трубопроводах використовують амортизатори, вставки між патрубками вібруючого агрегату і приєднаними до них трубопроводами.

При використанні редукторів, черв'ячних передач, клинопасових передач, зубчатих з'єднань виникає додатковий шум. Рівень шуму зубчатих передач визначається точністю зубчатих зачеплень, інерційними і жорсткими параметрами системи. Похибкою зачеплень являється збудники вимушених коливань, різниця кроків коліс приводить до удару зубів при вході в зачеплення.

Зниження шуму зубчатих передач можна досягти наступними методами:

- Зміною форми зубів (бочкоподібна форма). При даній формі зубів покращується контакт між зубами і шум зменшується на 3-4 дБ.
- Фланкування профілів зубів для компенсації похибки при виготовленні і монтажу зубчатих коліс.
- Заміна матеріалу коліс, наприклад із пластмаси. При заміні одного колеса в системі, ми відчутно знизимо рівень шуму.

При роботі електродвигунів і насосів також виникають негативні покази шумів [23].

При роботі даних агрегатів виникають наступні шуми: аеродинамічний, механічний і магнітний.

Для зменшення цих шумів використовують такі заходи:

- Використання електродвигунів більшої потужності. Запас потужності дозволяє зменшити магнітні складові шуму і відповідно зменшити шум на вентиляцію.
- Заміна підшипників кращими по якості промивки, заміни мастила. Використовувати мінімальні розміри підшипників, замінювати роликові підшипники на шарикові.

- Замінювати конфігурацію і розміри магнітопроводів.
- Проведення правильної центровки двигунів з приводними механізмами. Проведення загальної центровки, використання амортизованих і еластичних муфт.
- Регулярний огляд двигунів, надання при необхідності, якісного ремонту і заміну швидкозношувальних частин конструкції.

4.2. Заходи по захисту від ураження електричним струмом при роботі на автоматизованій лінії

Широка автоматизація виробничих процесів у багатьох галузях господарства супроводжується підвищеною енергозабезпеченістю і використанню електричної енергії різних параметрів.

Вплив електричного струму на організм людини може мати серйозні для здоров'я людини наслідки. Тому для захисту людей від ураження електричним струмом на автоматизованих лініях досягається наступними основними методами [24]:

- Відповідними пристроями, при яких струмоведучі частини, які знаходяться під напругою, недоступні для випадкового дотику завдяки застосуванню ізоляції, огороженню, розміщенню на недоступній висоті, блокуванні.
- Пристрої захисного заземлення, або автоматичного відключення, при якому у випадку пошкодження ізоляції і переходу напруги на металічні конструкції електрообладнання апаратура автоматично відключається.
- Регламентація величини допустимих напружень для даного приміщення.
- Повна, або часткова ізоляція підлоги.

Пошкодження ізоляції являється основними джерелами аварій і причин багатьох нещасних випадків. Ось чому в процесі експлуатації

електрообладнання ізоляція завжди повинна бути перевірена і задовольняти усі вимоги.

В якості ізоляції використовують фарфор, скло, смолу, картон, текстоліт, гуму і інші діелектричні матеріали.

Так як із часом якість ізоляції погіршується, тому ці пристрої, які знаходяться в експлуатації, необхідно періодично оглядати. Також перевірка повинна проводитись не менше одного разу в рік.

Основні вимоги які поставлені для експлуатації електрообладнання:

- Усі струмопровідні частини захищені в корпус.
- Електрообладнання захищене не тільки від випадкового дотику до його відкритих частин, а також від можливого впливу навколишнього середовища і інших факторів, які в кінцевому випадку можуть привести до електричного ураження, аварій.

Для захисту працюючих від випадкового ураження струмом (струмопровідні частини, які знаходяться близько робочих місць) використовують тимчасові огороження. Для огороження даних частин конструкції використовують щити, решітки. Щити виготовлені із сухого дерева. На щитах закріплюють передбачений плакат, або роблять відповідний напис.

Електричний струм, який проходить через живі тканини людини спричиняє термічну (опіки), електролітичну (електроліз крові та плазми) і біологічну дію, а також механічні ураження. Це призводить до порушень в організмі, спричиняє, як місцеве ураження тканин, так і загальне ураження всього організму. Розрізняють два види ураження електричним струмом: місцеві електротравми й електричні удари [24].

Основні причини нещасних випадків від дії електричного струму такі:

- випадковий дотик або наближення на небезпечну відстань до струму ведучих частин, які знаходяться під напругою;

- поява напруги дотику на метелевих конструкціях електрообладнання (корпусах, кожухах і т.п.) у результаті пошкодження або з інших причин;
- поява напруги на відімкнених струмо - ведучих частинах, на яких працюють люди, через помилкове вмикання установки;
- виникнення напруги кроку на поверхні землі у результаті замикання проводу на землю.

Для того, щоб на виробництві зменшити кількість нещасних випадків від ураження електричним струмом вживають таких заходів захисту:

- забезпечення недоступності струмоведучих частин під напругою для випадкового дотику;
- електричний поділ мережі;
- захисне заземлення, занулення і захисне вимкнення корпусів і кожухів електро установок, на яких може виникнути напруга;
- застосування малих напруг;
- захист від випадкового дотику до струмоведучих частин застосування кожухів, огорож, подвійної ізоляції;
- контролю і профілактика пошкоджень ізоляції;
- організація безпечної експлуатації електроустановок.

Шум і вібрація також негативно впливають на організм людини, послаблюють увагу, прискорюють втому, утруднюють реакцію на небезпеку. Все це знижує працездатність і може стати причиною нещасного випадку. Джерелом вібрації і шуму в даному випадку є клейонкопротяжний механізм.

Різноманітність впливу електричного струму на організм людини призводять до електротравм, котрі умовно поділяються на два види:

- місцеві електротравми, котрі означають місцеве ушкодження організму;

– загальні електротравми (електричні удари), коли уражається (або виникає загроза ураження) весь організм внаслідок порушення нормальної діяльності життєвоважливих органів та систем.

Згідно зі статистичними даними орієнтовний розподіл нещасних випадків внаслідок дії електричного струму в І промисловості за вказаними видами травм має наступний вигляд:

- місцеві електротравми — 20%;
- електричні удари — 25%;
- змішані травми (одночасно місцеві електричні травми та, електричні удари) — 55%.

Місцева електротравма — яскраво виявлене порушення щільності тканин тіла, в тому числі кісток, викликане впливом електричного струму або електричної дуги. Найчастіше — це поверхневі ушкодження, тобто ушкодження шкіри, а інколи й інших м'яких тканин, зв'язок та кісток. Небезпека місцевих електротравм та складність їх лікування залежать від місця, характеру та ступеня ушкодження тканин, а також від реакції організму на це ушкодження. Місцеві електротравми виліковуються і працездатність потерпілого відновлюється повністю або частково. Однак при важких опіках людина помирає. При цьому безпосередньою причиною смерті є не електричний струм, а місцеве ушкодження організму, викликане струмом. Характерні місцеві електротравми — електричні опіки, електричні знаки, металізація шкіри, механічні пошкодження та електроофтальмія.

Приблизно 75% випадків ураження людей струмом супроводжується виникненням місцевих електротравм.

Електричні опіки — це ушкодження поверхні тіла під дією електричної дуги або великих струмів, що проходять через тіло людини. Опіки бувають двох видів: струмові, коли струм проходить через тіло людини, та дугові (під дією електричної дуги температурою понад 3500 °C).

Електричний знак — це чітко окреслена пляма діаметром 1—5 мм сірого або блідо-жовтого кольору, що з'являється на поверхні шкіри людини, яка зазнала дії струму. В більшості випадків електричні знаки безболісні, з часом верхній шар шкіри сходить, а уражене місце набуває початкового кольору, відновлює пластичність та чутливість.

Електрометалізація — проникнення в шкіру частинок металу внаслідок його розбризкування та випаровування під дією струму. Вона може статися при коротких замиканнях, від'єднаннях роз'єднувачів та рубильників під навантаженням. При цьому дрібні частинки розплавленого металу під впливом динамічних сил та теплового потоку розлітаються у всі сторони з великою швидкістю. Кожна з цих частинок має високу температуру, але малий запас теплоти, і тому не здатна пропалити одяг. Тому ушкоджуються відкриті частини тіла — руки та обличчя. Уражена ділянка тіла має шорстку поверхню [25].

З плином часу хвора шкіра сходить, уражена ділянка набуває нормального вигляду та еластичності, зникають і всі хворобливі відчуття, пов'язані з цією травмою. Лише при пошкодженні очей лікування може виявитись тривалим та складним, а в деяких випадках потерпілий може позбутись зору. Тому роботи, при котрих можливе виникнення електричної дуги, повинні виконуватись в захисних окулярах. Металізація шкіри спостерігається у 10% потерпілих від електричного струму. Одночасно з металізацією виникає дуговий опік, котрий майже завжди викликає більш важкі ураження, ніж металізація.

Механічні ушкодження є в більшості випадків наслідком різких судомних скорочень м'язів під впливом струму, котрий проходить через тіло людини. Внаслідок цього можуть відбутися розриви сухожилів, шкіри, кровоносних судин та нервової тканини і навіть переломи кісток. Електротравмами не вважаються аналогічні травми, викликані падінням людини з висоти, ударами об предмети внаслідок впливу струму. Механічні

ушкодження мають місце при роботі в установках напругою до 1000 В при тривалому перебуванні людини під напругою. Механічні ушкодження виникають приблизно у 1% осіб, що зазнали впливу струму. Такі ушкодження завжди створюють електричні удари, оскільки їх викликає струм, що проходить через тіло людини. Деякі з них супроводжуються, крім того, контактними опіками тіла. На ступінь ураження людини струмом істотно впливають рід та величина струму, час його дії, шлях по тілу людини.

Електроофтальмія — це запалення зовнішніх оболонок очей, що виникає під впливом потужного потоку ультрафіолетових променів. Таке опромінення можливе при утворенні електричної дуги (при короткому замиканні). Електроофтальмія спостерігається приблизно у 3% потерпших від струму.

Інфрачервоні (теплові) промені також шкідливі для очей, але лише на близькій відстані або при інтенсивному і тривалому опроміненні. У випадку ж короткотривалої дуги основним фактором, що впливає на очі, є ультрафіолетові промені, хоч і в цьому випадку не виключена небезпека ураження очей інфрачервоними променями, а також потужним потоком світла та бризками розплавленого металу [25].

Електроофтальмія розвивається через 4—8 годин після ультрафіолетового опромінення. При цьому мають місце почервоніння та запалення шкіри, слизових оболонок повік, слъози, гнійні виділення з очей, судоми повік та часткова втрата зору. Потерпілий відчуває головний біль та різкий біль в очах, що посилюється на світлі.

Запобігання електроофтальмії при обслуговуванні електроустановок забезпечується застосуванням захисних окулярів зі звичайним склом, котре майже не пропускає ультрафіолетових променів і одночасно захищає очі від інфрачервоного опромінення та бризок розплавленого металу при виникненні електричної дуги.

Електричний удар — збудження живих тканин організму електричним струмом, що супроводжується судомним скороченням м'язів. Такий удар може

призвести до порушення і навіть повного припинення роботи легенів та серця. При цьому зовнішніх місцевих ушкоджень, тобто електричних травм, людина може і не мати.

Ступінь негативного впливу на організм електричних ударів різний. Найсильніший електричний удар викликає ледь відчутні скорочення м'язів поблизу місця входу або виходу струму. Може порушитись і навіть припинитись діяльність легенів та серця, тобто призвести до загибелі організму.

4.3. Порядок виконання основних заходів з реагування на загрозу та виникнення надзвичайної ситуації

Основні заходи ЦО та порядок їх виконання з урахуванням специфіки району, визначених термінів виконання, сил і засобів ЦО, які залучаються, відповідальних виконавців включаються в календарні плани дій органів управління та сил ЦО при загрозі та виникненні конкретних НС [25].

При загрозі виникнення надзвичайної ситуації включають:

- переведення районної ланки обласної підсистеми ЄДС НС в режим підвищеної готовності;
- запровадження в органах управління з НС та ЦО (у зонах можливого виникнення НС) цілодобового чергування керівного складу та чергових змін;
- приведення в готовність системи оповіщення та зв'язку, та уточнення текстів звернень про порядок дій населення в умовах виникнення даної конкретної НС;
- уточнення планів реагування на НС (Планів дій)
- приведення в готовність оперативної групи;

- приведення в стан підвищеної готовності сил і засобів ЦО, які згідно з розрахунками будуть залучені для проведення рятувальних та інших невідкладних робіт;
- організація і проведення попереджувальних інженерно-технічних, спеціальних та інших заходів, які спрямовані на недопущення (зниження) впливу можливих наслідків НС на населення та об'єкти економіки;
- приведення в готовність сил медичної допомоги та закладів МСЛК, посилення спостереження і контролю за станом довкілля, обстановкою на потенційно небезпечних об'єктах і прилеглий до них території;
- у разі необхідності – організацію і проведення розвідки можливих небезпечних зон та осередків аварій;
- організацію систематичного одержання інформації від організацій МСЛК за навколишнім середовищем, диспетчерів потенційно небезпечних об'єктів;
- проведення заходів щодо запобігання виникненню НС;
- проведення підготовки транспортних засобів до перевезення сил ЦО у район можливої НС і для евакуації (відселення) населення із небезпечних районів, вивезення матеріальних та інших цінностей;
- проведення заходів щодо захисту населення і територій, забезпечення стійкого функціонування об'єктів економіки;
- організацію всебічного забезпечення заходів ЦО, які плануються провадити у районі НС;
- інформування сусідніх територіальних органів управління з питань НС та ЦО про обстановку.

Рішеннями начальників ЦО можуть проводитись і інші додаткові заходи (в залежності від специфіки відповідної території, об'єкта), які спрямовані на захист населення і територій, зменшення збитків і втрат у випадку розвитку небезпеки виникнення НС. При виникненні надзвичайної ситуації:

- переведення районної ланки територіальної підсистеми ЄДС НС в режим діяльності у НС;
- здійснення відповідною комісією з ПТЕБ та НС в межах її повноважень безпосереднього керівництва функціонуванням ланок і структурних підрозділів районної ланки територіальної підсистеми ЄДС НС;
- термінове оповіщення (з використанням усіх засобів оповіщення та зв'язку): оперативним черговим – населення, яке проживає в небезпечних зонах поза межами адміністративно-територіальної одиниці, де розташований потенційно небезпечний об'єкт, черговими службами потенційно небезпечних об'єктів – керівництва, працівників та населення, яке проживає в небезпечних зонах;
- доповіді про НС: по лінії диспетчерських служб – оперативному черговому райдержадміністрації, черговим установ і організацій, яким підпорядковані ці об'єкти; по лінії оперативного чергового – начальнику відділу з питань НС та ЦЗН, начальнику ЦО району, оперативному черговому управління з питань НС та у СЗН від НЧК;
- виїзд оперативної групи в район виникнення НС;
- термінове проведення в районах НС заходів по локалізації НС та захисту населення, що проживає в небезпечній зоні;
- проведення оповіщення і збір керівного складу органів управління з питань НС та ЦО, які у разі необхідності переводяться на цілодобовий режим роботи;
- введення в дію відповідних планів реагування на НС (Планів дій);
- приведення в готовність відповідних формувань ЦО району та відправлення їх у район НС для нарощування зусиль по проведенню рятувальних та інших невідкладних робіт;
- проведення в районах НС рятувальних та інших невідкладних робіт, лікувально-евакуаційних, санітарно-гігієнічних та протиепідемічних заходів;

- організація і проведення (у разі необхідності) евакуації (відселення) населення, вивезення матеріальних і інших цінностей;
- проведення всебічного забезпечення виконання заходів і дій сил ЦО у районі НС;
- організація проведення робіт, направлених на забезпечення сталого функціонування об'єктів економіки та об'єктів першочергового життєзабезпечення постраждалого населення;
- здійснення постійного контролю за станом навколишнього середовища на території, що зазнала впливу наслідків НС;
- організація взаємодії між силами ЦО, що виконують завдання в місцях проведення рятувальних та інших невідкладних робіт.

У разі неможливості власними силами виконати весь обсяг заходів ЦО по захисту населення та ліквідації наслідків НС начальник ЦО району звертається до обласної державної адміністрації [26].

Висновки

У цій роботі розроблено проект автоматизованої системи відеоспостереження, яка відповідає потребам медичного закладу. Розробка охоплює як програмні, так і апаратні компоненти з урахуванням сучасних вимог до безпеки, конфіденційності та надійності. Під час дослідження було проаналізовано існуючі рішення, визначено практичність використання цифрових IP-камер, розроблено архітектуру системи та обґрунтовано вибір технічних засобів. Особливу увагу було приділено оптимальному розміщенню камер відповідно до функціонального зонування медичного закладу, а також інтеграції з централізованим інтерфейсом моніторингу.

Результатом роботи є концепція системи, здатної забезпечити цілодобове відеоспостереження, виявлення подій, зберігання відеоданих та можливість оперативного реагування на надзвичайні ситуації. Запропоноване рішення сприяє підвищенню безпеки, організаційної дисципліни та створює умови для оперативного інформування відповідальних осіб або правоохоронних органів у разі загрози.

Таким чином, мета дипломної роботи досягнута, запропонована система має практичне значення і може бути впроваджена в реальних умовах з подальшим розвитком і масштабуванням.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Joint Commission (2022). Workplace Violence Prevention Standards. <https://www.jointcommission.org/>
2. Cleveland Clinic Security System Overview. Internal hospital publication, 2023.
3. BMJ Innovations (2020). Use of Video Surveillance to Reduce Falls in Dementia Patients. <https://innovations.bmj.com/>
4. NHS Digital (2021). AI Surveillance Pilot for Infection Control Compliance. <https://digital.nhs.uk/>
5. IHS Markit. (2019). Video Surveillance in Healthcare Sector: Market Overview.
6. Allied Market Research. (2021). Global IP Video Surveillance Market by End-Use Sector.
7. Axis Communications. (2020). Advantages of IP Cameras Over Analog.
8. Bosch Security Systems. (2023). Healthcare Security Solutions Whitepaper.
9. U.S. Department of Health & Human Services (HHS). HIPAA Privacy Rule and Security Rule.
10. European Commission. General Data Protection Regulation (GDPR), 2016.
11. Закон України «Про захист персональних даних», № 2297-VI від 01.06.2010.
12. Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles.
13. Axis Communications. (2021). Video Surveillance in Healthcare: Privacy Considerations.

14. Milestone Systems. (2023). XProtect® Video Management Software. Retrieved from: <https://www.milestonesys.com>
15. Avigilon. (2023). Avigilon Control Center 7. Retrieved from: <https://www.avigilon.com/products/video-security/software/acc>
16. Axis Communications. (2022). AXIS Camera Station and AXIS Object Analytics. Retrieved from: <https://www.axis.com>
17. OpenCV. (2024). Open Source Computer Vision Library. Retrieved from: <https://opencv.org>
18. BriefCam. (2023). Transform Video into Actionable Intelligence. Retrieved from: <https://www.briefcam.com>
19. Pritchard, D. (2020). IP vs. Analog Video Surveillance Systems: Pros and Cons. SecurityToday.
 - Axis Communications. (2023). The Benefits of IP Surveillance for Healthcare. Retrieved from: <https://www.axis.com>
20. Milestone Systems. (2023). Choosing the Right VMS for Healthcare. Retrieved from: <https://www.milestonesys.com>
21. Motorola Solutions. (2022). Surveillance Technologies for the Healthcare Sector.
22. World Health Organization (WHO). (2021). Health Facility Safety and Security Guidelines.
23. Bernas, M., Mykytyshyn, A., Kartashov, V., Levytskyi, V. & Martjanov, D. (2023) The Role of Cyber-Physical Systems and Internet of Things in Development of Smart Cities for Industry 4.0. CEUR Workshop Proceedings. Vol. 3468,. P. 91–102.
24. Бедрій І.Я., Нечай В.Я. Безпека життєдіяльності. Навчальний посібник. – Львів: Манголія 2006, 2007. 499 с. 43
25. Зеркалов Д.В. Безпека життєдіяльності. Навчальний посібник. - К.: Основа, 2011.

26. Організація праці операторів комп'ютерів. URL: https://pidru4niki.com/92832/bzhd/organizatsiya_pratsi_operatoriv_komp_yuteriv (дата звернення: 10.05.2025).

27. Заходи для покращення умов праці операторів комп'ютерів. URL: https://pidru4niki.com/92831/bzhd/zahodi_pokraschennya_umov_pratsi_operatoriv_kompyuteriv (дата звернення: 10.05.2025).