

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

**Колледж программирования и кибербезопасности**

КУРСОВОЙ ПРОЕКТ

СПЕЦИАЛЬНОСТЬ 10.02.05

Обеспечение информационной безопасности автоматизированных систем

**на тему:**

Внедрение системы безопасности IP-видеонаблюдения в корпоративную сеть «ГУП Московский метрополитен»

Выполнил студент:

группы ЩИКО–02–22 (ИБ–42)

Маркаров М.О.

подпись ФИО студента

Руководитель

Мителев И.А.

подпись ФИО руководителя

Москва 2025

|  |  |
| --- | --- |
|  | **Утверждаю** |
|  | Председатель ПЦК  «Информационной безопасности» .\_\_\_\_\_\_\_\_\_\_\_\_\_\_.*Герасим Ю.В.*.  *подпись ФИО* |
|  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_2025 г. |
| **ЗАДАНИЕ** | |
| **на курсовой проект** | |

|  |  |  |
| --- | --- | --- |
| студенту | Маркарову Михаилу Оганесовичу | группы ЩИКО–02–22 |
| по специальности | 10.02.05 Обеспечение информационной безопасности  автоматизированных систем | |

|  |  |
| --- | --- |
| **Тема** | Внедрение системы безопасности IP-видеонаблюдения в корпоративную сеть «ГУП Московский метрополитен» |
| **Пояснительная записка** | |
| **Введение** | |
| **1 Аналитический раздел**  1.1 Анализ структуры объекта ГУП «Московский метрополитен»  1.2 Анализ структуры объекта внедрения  1.3 Нормативно-правовая база, регламентирующая безопасность систем видеонаблюдения и защиту информации  **2 Исследовательский раздел**  2.1 Исследование модели угроз для системы IP-видеонаблюдения в соответствии с определяемой защищаемой информации  2.2 Проектирование защищенной архитектуры системы IP-видеонаблюдения  2.3 Выбор и обоснование выбранных решений защиты информации для компонентов системы видеонаблюдения  **3 Практический раздел**  3.1 План внедрения IP-видеонаблюдения в офис ГУП Московский метрополитен  3.2 Подготовка и настройка компонентов в офис ГУП Московский метрополитен  3.3 Подготовка правил реагирования IP-видеокамер | |
| **Заключение**  **Список использованных источников** | |

Приложение к заданию на курсовой проект

|  |  |  |  |
| --- | --- | --- | --- |
| Задание на курсовой проект выдал | « » 202 г. |  | *Мителев И.А.* |
|  |  | *Подпись руководителя проекта* | *ФИО руководителя проекта* |
| Задание на курсовой проект получил | « » 202 г. |  | *Маркаров М.О.* |
|  |  | *Подпись студента– исполнителя проекта* | *ФИО студента– исполнителя проекта* |

**Срок представления к защите курсового проекта: до** « » 2025 г.

## **СОДЕРЖАНИЕ**

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УЛОВНЫХ ОБОЗНАЧЕНИЙ 3

ВВЕДЕНИЕ 4

1 АНАЛИТИЧЕСКИЙ РАЗДЕЛ 6

1.1 Анализ структуры объекта ГУП «Московский метрополитен» 6

1.2 Схема офиса ГУП «Московский метрополитен» 9

1.3 Нормативно-правовая база, регламентирующая безопасность систем видеонаблюдения и защиту информации 12

2 ИССЛЕДОВАТЕЛЬСКИЙ РАЗДЕЛ 15

2.1 Исследование модели угроз для системы IP-видеонаблюдения в соответствии с определяемой защищаемой информации 15

2.2 Проектирование защищенной архитектуры системы IP-видеонаблюдения 18

2.3 Выбор и обоснование выбранных решений защиты информации для компонентов системы видеонаблюдения 22

3 ТЕХНИЧЕСКИЙ РАЗДЕЛ 25

3.1 План внедрения IP-видеонаблюдения в офис ГУП Московский метрополитен 25

3.2 Подготовка и настройка компонентов в офис ГУП Московский метрополитен 28

3.3 Подготовка правил реагирования IP-видеокамер 31

ЗАКЛЮЧЕНИЕ 35

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 36

# **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ**

|  |  |  |
| --- | --- | --- |
| АРМ | — | автоматизированное рабочее место |
| ГУП | — | государственное унитарное предприятие |
| ИТ | — | информационные технологии |
| КИИ | — | критическая информационная инфраструктура |
| НПА | — | нормативно-правовые акты |
| ОС | — | операционная система |
| ПДн | — | персональные данные |
| ПЗ | — | пояснительная записка |
| РФ | — | Российская Федерация |
| СБ КИИ | — | система безопасности критической информационной инфраструктуры |
| СЗИ | — | средства защиты информации |
| СИБ | — | служба информационной безопасности |
| СКУД | — | система контроля и управления доступом |
| ФЗ | — | Федеральный закон |
| ФСТЭК | — | Федеральная служба по техническому и экспортному контролю |
| CPU | — | Central Processing Unit (центральный процессор) |
| DDoS | — | Distributed Denial of Service (распределённая атака на отказ в обслуживании) |
| DMZ | — | Demilitarized Zone (демилитаризованная зона) |
| DDR4 | — | Double Data Rate 4 (четвёртое поколение памяти с удвоенной скоростью передачи данных) |
| IP | — | Internet Protocol (межсетевой протокол) |
| NVR | — | Network Video Recorder (сетевой видеорегистратор) |
| NVMe | — | Non-Volatile Memory Express (протокол для высокоскоростных накопителей) |
| OS | — | Operating System (операционная система) |
| PoE | — | Power over Ethernet (питание через Ethernet) |
| RAM | — | Random Access Memory (оперативная память) |
| RTSP | — | Real Time Streaming Protocol (протокол потоковой передачи в реальном времени) |
| TLS | — | Transport Layer Security (протокол защиты транспортного уровня) |
| UPS |  | Uninterruptible Power Supply (источник бесперебойного питания) |
| VLAN | — | Virtual Local Area Network (виртуальная локальная сеть) |
| VMS | — | Video Management System (система управления видео) |
| VPN | — | Virtual Private Network (виртуальная частная сеть) |
| WDR | — | Wide Dynamic Range (широкий динамический диапазон) |

# 

# **ВВЕДЕНИЕ**

В характеризующемся высокой концентрацией населения и транспортных потоков, системы безопасности и управления становятся цифровым фундаментом обеспечения общественного порядка и бесперебойности информацию имеющую важное значение для безопасности. Особую роль в этом играют технологии видеоаналитики и IP-видеонаблюдения, трансформирующиеся из инструмента записи в интеллектуальные комплексы обеспечения безопасности и оперативного реагирования. Однако интеграция таких масштабных и распределенных систем в существующую корпоративную сеть организации создает новые вызовы в сфере информационной безопасности.

Корпоративная сеть ГУП «Московский метрополитен», являясь основой для работы жизненно важных служб, уже несет нагрузку систем управления движением, оплаты и коммуникаций. Внедрение в эту среду высоконагруженной системы IP-видеонаблюдения, включающей тысячи камер, серверов обработки видео и аналитических модулей, неизбежно расширяет периметр атаки и создает потенциально уязвимые точки. Информация с видеопотоков, содержащие информацию персонального характера и критичную для безопасности инфраструктуры, становятся целью для злонамеренных действий. Угрозы варьируются от перехвата и подмены видеопотоков, выводящих из строя систему контроля, до атак на серверы хранения и анализа с целью компрометации данных или нарушения работоспособности.

В связи с этим задача безопасной интеграции становится не менее важной, чем техническая реализация самой системы видеонаблюдения. Актуальность вопроса заключается в создания не изолированного сегмента, а защищенного, управляемого и глубоко интегрированного в общую архитектуру безопасности комплекса. Это требует перехода от разрозненных мер защиты к разработке целостной концепции, учитывающей как специфику сетевого трафика видео, так и строгие требования к отказоустойчивости и конфиденциальности данных ГУП «Московский метрополитен».

Целью курсового проекта является разработка архитектуры и плана внедрения защищенной системы IP-видеонаблюдения в корпоративную сеть ГУП «Московский метрополитен». Проект включает сегментацию сетевой инфраструктуры, обеспечение конфиденциальности и целостности видеоданных, реализацию контролей доступа и мониторинга, направленных на минимизацию и создание отказоустойчивого решения, отвечающего оперативным нуждам и современным стандартам информационной безопасности.

Для достижения поставленной цели в работе последовательно решаются следующие задачи:

* изучить организационную структуру и технологические процессы ГУП «Московский метрополитен», связанные с обеспечением безопасности;
* проанализировать существующую нормативно-правовую базу, регулирующую использование систем видеонаблюдения и защиту персональных данных;
* исследовать текущую сетевую инфраструктуру и телекоммуникационные возможности для интеграции системы IP-видеонаблюдения;
* сформировать модель угроз и провести оценку рисков для выявления уязвимостей в проектируемой и существующей инфраструктуре;
* спроектировать защищенную архитектуру системы IP-видеонаблюдения, включая сегментацию сети, схемы управления доступом и резервирования;
* исследовать и выбрать специализированные средства защиты для систем видеонаблюдения (VPN, шифрование видеопотоков, системы обнаружения вторжений для IP-камер и серверов);
* разработать механизмы контроля целостности, конфиденциальности видеоданных и аутентификации устройств;
* провести тестирование и оценку эффективности предложенных решений на предмет устойчивости к кибератакам и соответствия требованиям безопасности.

Практическим результатом выполнения работы является разработанная архитектура и комплексный план внедрения защищенной системы IP-видеонаблюдения, интегрированной в корпоративную сеть ГУП «Московский метрополитен». Модель обеспечивает отказоустойчивость, конфиденциальность видеоданных и эффективную защиту от современных киберугроз при оптимальном использовании существующей инфраструктуры.

# **Аналитический раздел**

## **1.1 Анализ структуры объекта ГУП «Московский метрополитен»**

Государственное унитарное предприятие (ГУП) «Московский метрополитен» является ключевым элементом транспортной инфраструктуры столицы. Предприятие осуществляет комплекс задач, непосредственно влияющих на безопасность города и жизнедеятельность миллионов граждан.

Основные виды деятельности включают:

* организацию регулярных пассажирских перевозок;
* эксплуатацию, техническое обслуживание и ремонт подвижного состава и инфраструктуры;
* обеспечение транспортной доступности и бесперебойности функционирования метрополитена.

Руководство текущей деятельностью осуществляет начальник метрополитена, которому подчиняются первые заместители по ключевым направлениям: пассажирская работа, инженерно-технический комплекс. Эксплуатационный штат составляют сотрудники депо, служб движения, электромеханики и другой технический персонал.

Административно-управленческий аппарат предприятия размещается в центральном офисе, где сосредоточена конфиденциальная информация: финансовая отчётность, кадровые данные, проектная документация, коммерческие переговоры и данные системы управления. Именно офисные помещения являются объектом защиты в рамках внедрения системы IP-видеонаблюдения.

Для обеспечения управляемости, безопасности и технологического развития в структуре предприятия функционируют Дирекция по информационным технологиям (ИТ) и Служба информационной безопасности (СИБ). Именно эти подразделения несут ключевую ответственность за проектирование, внедрение и эксплуатацию инженерно-технических средств защиты, включая систему IP-видеонаблюдения, а также за обеспечение кибербезопасности всей корпоративной сети.

Организационная структура ГУП «Московский метрополитен» представлена на рисунке 1. Схема отражает подчиненность и взаимодействие между эксплуатационными (линейными) и обеспечивающими (функциональными) отделами, в число которых входят:

1. Административно-управленческий блок:

* Бухгалтерия;
* отдел кадров;

1. Операционно-технический блок:

* служба движения;
* электротехническая служба;
* служба связи и информационных технологий.

1. Блок информационных технологий и безопасности, а также дирекции по информационным технологиям (ИТ):

* отдел администрирования сети;
* отдел сопровождения и технической поддержки;
* отдел обработки данных;
* отдел службы иб;
* отдел реагирования на инциденты.

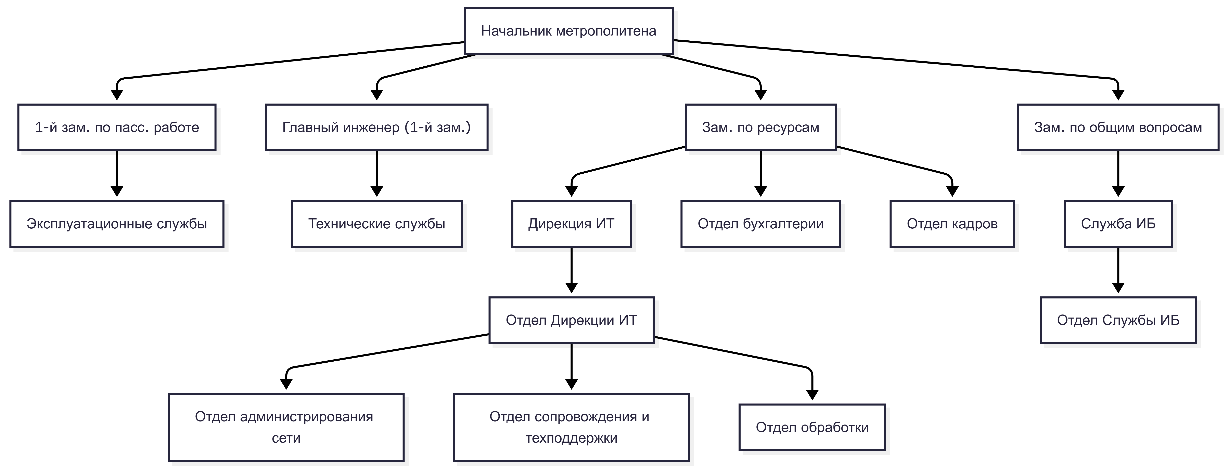


Рисунок 1 — Схема организационной структуры ГУП Московский метрополитен

Описание функций ключевых отделов:

* отдел Дирекции ИТ осуществляет общее руководство, стратегическое планирование и координацию всех ИТ-проектов предприятия, включая утверждение архитектурных решений и бюджетирование системы видеонаблюдения;
* отдел администрирования сети обеспечивает проектирование, развертывание и поддержку сетевой инфраструктуры, включая сегментацию и настройку VLAN для изоляции видео-трафика, а также настройку межсетевых экранов и QoS;
* отдел сопровождения и технической поддержки осуществляет техническое обслуживание оборудования, установку и настройку IP-камер, взаимодействие с пользователями системы и замену неисправного оборудования;
* отдел обработки данных управляет серверами хранения видеозаписей (NVR/VMS), обеспечивает архивирование, резервное копирование и целостность архивных данных, а также интеграцию с корпоративными системами;
* отдел Службы ИБ проводит оценку рисков и угроз, контролирует соответствие системы требованиям защиты персональных данных (ФЗ-152), осуществляет аудит настроек безопасности и мониторинг инцидентов;
* отдел бухгалтерии учитывает материальные ценности оборудования, контролирует финансовые расходы на приобретение и эксплуатацию системы, ведет расчеты с поставщиками и участвует в бюджетном планировании;
* отдел кадров формирует штатное расписание и должностные инструкции для сотрудников, обслуживающих систему, организует обучение персонала и контролирует допуск к конфиденциальной информации.

Анализ структуры ГУП «Московский метрополитен» показал, что предприятие представляет собой сложную организационно-техническую систему с чётким разделением на эксплуатационные, административные и обеспечивающие подразделения. Центральный офис предприятия является местом сосредоточения конфиденциальной информации, включая финансовые, кадровые и управленческие данные, что определяет его как ключевой объект для внедрения системы IP-видеонаблюдения.

## **1.2 Схема офиса ГУП МОСКОВСКИЙ МЕТРОПОЛИТЕН**

На рисунке 2 представлена схема офиса ГУП «Московский метрополитен» с обозначением помещений и проектируемой расстановкой IP-камер видеонаблюдения. Размещение оборудования спроектировано на основе анализа планировки, функционального назначения помещений и требований защиты конфиденциальной информации, установленных нормативными документами, включая Федеральный закон № 152-ФЗ «О персональных данных».

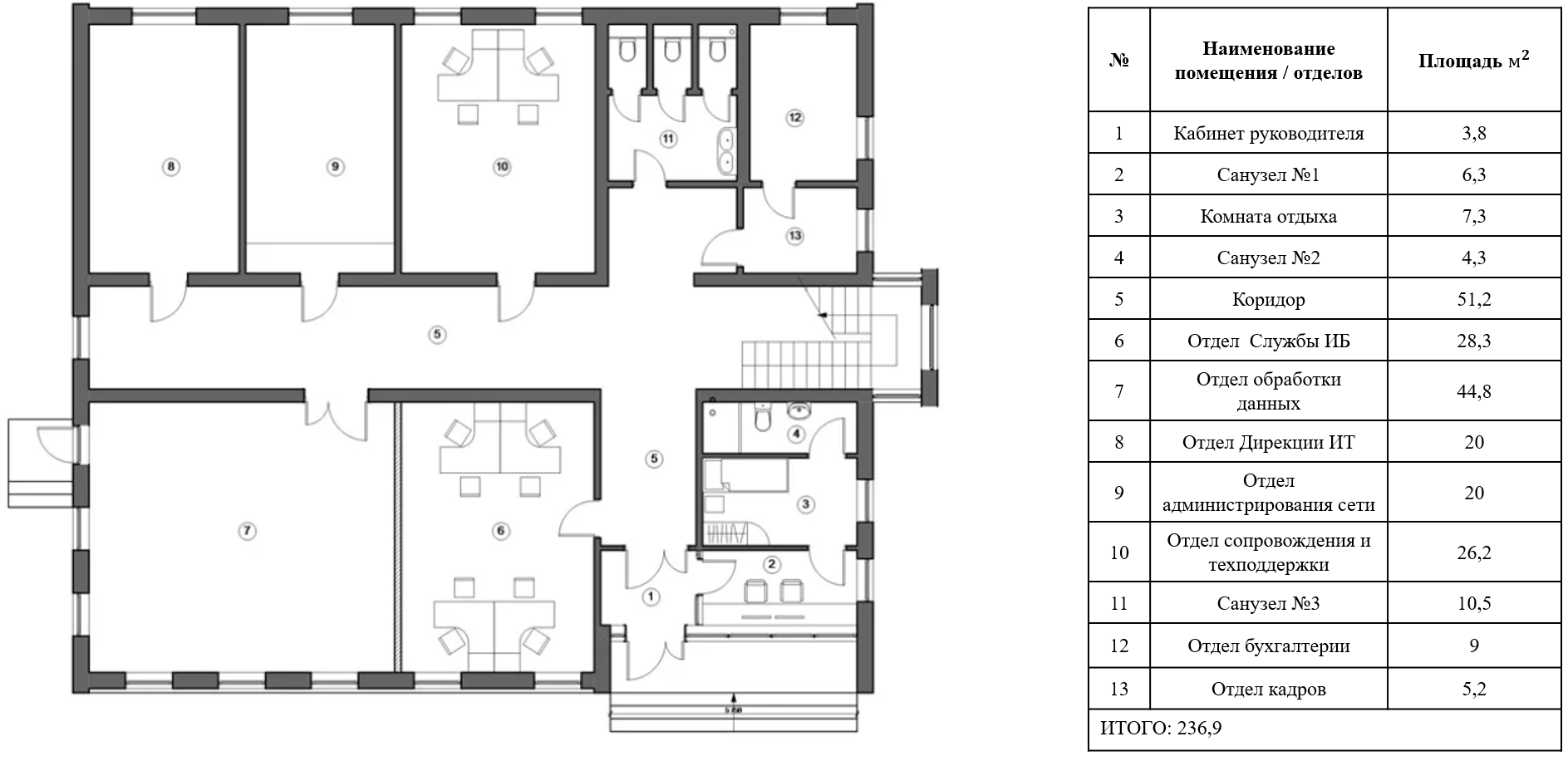


Рисунок 2 — Схема офиса ГУП Московский метрополитен

В общественных и вспомогательных зонах, таких как коридоры и холлы, установлены купольные IP-камеры Hikvision DS-2CD2347G2-LU. Эти камеры обеспечивают широкий угол обзора для контроля общего порядка, перемещения сотрудников и посетителей, а также оперативного реагирования на нештатные ситуации. Наличие встроенной ИК-подсветки позволяет им работать круглосуточно, включая условия слабого освещения. Для повышения детализации наблюдения на ключевых пересечениях коридоров и в зонах с повышенной проходимостью используются поворотные PTZ-камеры, способные осуществлять панорамный обзор и автоматическое слежение за движущимися объектами.

На входах в отделы, работающие с конфиденциальной информацией такие как Отдел Службы ИБ, Отдел обработки данных, Дирекция ИТ, бухгалтерия и отдел кадров установлены фиксированные камеры с высоким разрешением. Их задача обеспечить чёткую идентификацию лиц и фиксацию времени входа и выхода, что предотвращает несанкционированный доступ и позволяет контролировать соблюдение режима информационной безопасности.

Основными задачами спроектированной системы размещения являются:

* + контроль физического доступа в защищаемые зоны;
  + мониторинг рабочих процессов и действий персонала;
  + оперативное документирование инцидентов, таких как попытки проникновения, кражи или порча имущества;
  + формирование архивов видеоданных для последующего анализа и проведения служебных расследований.

Данная схема является основой для монтажа и настройки системы видеонаблюдения, обеспечивая полный контроль над офисными помещениями ГУП «Московский метрополитен» в соответствии с требованиями информационной безопасности

## **1.3 Нормативно-правовая база, регламентирующая безопасность систем видеонаблюдения и защиту информации**

Деятельность ГУП «Московский метрополитен» и, в частности, внедрение системы IP-видеонаблюдения, строго регламентированы следующими законодательными и нормативными актами:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»:

* + статья 3. определяет видеозаписи с изображением граждан как биометрические персональные данные;
  + статья 6 и 9. устанавливают условия их обработки и получения согласия субъекта ПДн (требование реализуется через информационные табло в зонах видеонаблюдения);
  + статья 19. требует от оператора (метрополитена) применения необходимых и достаточных организационных и технических мер для защиты ПДн, включая шифрование, контроль доступа и регистрацию событий.

Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности»:

* + статья 1 и 3. определяют метрополитен как объект транспортной инфраструктуры и устанавливают цели обеспечения его безопасности.
  + статья 5, 6, 7. обязывают субъекта транспортной инфраструктуры проводить оценку уязвимости объектов и разрабатывать планы обеспечения транспортной безопасности, где системы видеонаблюдения являются ключевым техническим элементом.

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...». Служит методической основой для выбора конкретных средств защиты информации при обработке видеопотоков.

Деятельность ГУП «Московский метрополитен» и, в частности, внедрение системы IP-видеонаблюдения, строго регламентированы следующими законодательными и нормативными актами Российской Федерации.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»:

* + статья 3 определяет видеозаписи с изображением граждан как биометрические персональные данные;
  + статьи 6 и 9 устанавливают условия их обработки и получения согласия субъекта ПДн (требование реализуется через информационные табло в зонах видеонаблюдения);
  + статья 19 требует от оператора (метрополитена) применения необходимых и достаточных организационных и технических мер для защиты ПДн, включая шифрование, контроль доступа и регистрацию событий.

Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности»:

* + статьи 1 и 3 определяют метрополитен как объект транспортной инфраструктуры и устанавливают цели обеспечения его безопасности;
  + статьи 5, 6, 7 обязывают субъекта транспортной инфраструктуры проводить оценку уязвимости объектов и разрабатывать планы обеспечения транспортной безопасности, где системы видеонаблюдения являются ключевым техническим элементом.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»:

* + устанавливает требования к обеспечению безопасности объектов КИИ, к которым может относиться система управления метрополитеном;
  + определяет порядок категорирования объектов КИИ и применения мер защиты.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

* + регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;
  + устанавливает требования к защите информации.

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»:

* + служит методической основой для выбора конкретных средств защиты информации при обработке видеопотоков;
  + определяет перечень организационных и технических мер защиты ПДн.

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»:

* + устанавливает конкретные требования к защите значимых объектов КИИ;
  + определяет меры защиты для систем, обрабатывающих информацию, имеющую важное значение для безопасности государства.

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

* + устанавливает требования к защите информации в государственных информационных системах;
  + определяет меры по обеспечению безопасности информации при её обработке в ГИС.

Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации»:

* + устанавливает требования к применению средств криптографической защиты информации при обработке ПДн;
  + определяет порядок использования СКЗИ для защиты видеопотоков.

ГОСТ Р 51558-2014 «Системы охранные телевизионные. Общие технические требования. Методы испытаний»:

* + устанавливает общие технические требования к системам охранного телевидения;
  + определяет методы испытаний систем видеонаблюдения.

ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»:

* + определяет требования к системам контроля доступа, которые могут интегрироваться с системами видеонаблюдения.

ГОСТ Р ИСО/МЭК 27001-2022 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»:

* + устанавливает требования к системам менеджмента информационной безопасности;
  + может применяться для организации процессов управления ИБ при эксплуатации системы видеонаблюдения.

ГОСТ Р 59120-2021 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»:

* + определяет критерии оценки безопасности информационных технологий;
  + может использоваться для оценки защищённости системы IP-видеонаблюдения.

Данная нормативно-правовая база формирует комплексную основу для проектирования, внедрения и эксплуатации системы IP-видеонаблюдения в корпоративной сети ГУП «Московский метрополитен», обеспечивая соответствие требованиям законодательства в области защиты информации, персональных данных и транспортной безопасности.

# **Исследовательский раздел**

## **Исследование модели угроз для системы IP-видеонаблюдения в соответствии с определяемой защищаемой информации**

Основными объектами защиты в проектируемой системе IP-видеонаблюдения являются следующие категории информации (активов), обработка которых производится в офисных помещениях ГУП «Московский метрополитен»:

1. Биометрические персональные данные (ПДн):
   * видеоизображения лиц сотрудников предприятия, постоянно работающих в офисе;
   * видеоизображения лиц посетителей, включая клиентов, контрагентов и иных физических лиц;
   * правовой статус согласно ст. 3 Федерального закона № 152-ФЗ, видеозаписи с изображением граждан относятся к биометрическим ПДн. Обработка таких данных требует применения специальных мер защиты, установленных ст. 19 того же закона и приказом ФСТЭК России № 21. Нарушение конфиденциальности данных этой категории влечёт максимальные репутационные и финансовые риски для предприятия.
2. Служебная информация ограниченного доступа:
   * визуальная фиксация рабочих процессов в помещениях с повышенным режимом секретности: кабинеты руководства, отдел Службы ИБ, бухгалтерия, отдел кадров, переговорные комнаты.
   * возможная фиксация содержимого экранов мониторов, бумажных документов, переговоров, содержащих коммерческую тайну, планы, отчётность или иную служебную информацию.
   * правовой статус защита регулируется режимом коммерческой тайны, внутренними регламентами предприятия и общими требованиями к защите служебной информации.
3. Данные, обеспечивающие работоспособность и целостность системы:
   * Конфигурационные параметры IP-камер, серверов записи (NVR/VMS) и сетевого оборудования.
   * Архивы видеозаписей и связанные с ними метаданные (время, камера, событие).
   * Видеопотоки в реальном времени и управляющие команды.
   * Правовой статус: Нарушение доступности или целостности этих данных приводит к отказу системы видеоконтроля, что недопустимо для объекта транспортной инфраструктуры (ФЗ-16).

Таким образом, система является информационной системой персональных данных (ИСПДн), обрабатывающей биометрические ПДн, и одновременно системой, обрабатывающей служебную информацию ограниченного доступа. Последующие меры защиты проектируются с учётом приоритета каждой категории.

На основе анализа нормативно-правовой базы (Приказ ФСТЭК России № 21), специфики обрабатываемых данных (биометрические ПДн, служебная информация) и архитектуры проектируемой системы разработана модель угроз информационной безопасности. Модель построена в соответствии с методологией ФСТЭК России и ГОСТ Р 53114–2008 и направлена на выявление угроз, связанных с нарушением конфиденциальности, целостности и доступности видеоданных, обрабатываемых в офисных помещениях ГУП «Московский метрополитен».

Перед построением модели определены возможные категории нарушителей:

1. Нарушитель Н1. Внешний нарушитель (хакер, конкурентная организация):
   * потенциальный (исходный) потенциал высокий;
   * технический потенциал высокий;
   * технологический потенциал средний-высокий;
   * мотивация получение конфиденциальной информации, нарушение работоспособности системы, нанесение репутационного ущерба;
   * доступ несанкционированный удалённый доступ.
2. Нарушитель Н2. Внутренний нарушитель (сотрудник предприятия без административных привилегий):
   * потенциальный потенциал: средний;
   * технический потенциал: ограниченный;
   * технологический потенциал: низкий-средний.

Мотивация для осуществления правонарушения включают в себя:

* + умышленные действия корысть, месть, промышленный шпионаж;
  + случайные действия ошибки при настройке оборудования, неосторожное обращение с данными;
  + доступ легитимный доступ в рамках должностных обязанностей.

1. Нарушитель Н3. Внутренний нарушитель с расширенными правами (администратор системы / сотрудник службы безопасности):
   * потенциальный потенциал очень высокий;
   * технический потенциал очень высокий;
   * технологический потенциал очень высокий;
   * мотивация злоупотребление полномочиями, несанкционированный сбор данных вне служебной необходимости;
   * доступ легитимный привилегированный доступ.

В модели используется классификация угроз в соответствии с Приказом ФСТЭК России № 21, имеющая следующие аналоги в Банке данных угроз (БДУ) ФСТЭК:

* + УНК (угрозы нарушения конфиденциальности) → соответствует классу «Утечка информации» в БДУ;
  + УНЦ (угрозы нарушения целостности) соответствует классу «Модификация информации» в БДУ;
  + УНД (угрозы нарушения доступности) соответствует классу «Отказ в обслуживании» в БДУ.

На предварительном этапе составлен следующий перечень актуальных угроз с указанием идентификаторов из БДУ ФСТЭК:

1. УБИ.ИК.01 Несанкционированный доступ к видеопотоку в реальном времени;
2. УБИ.ИК.02 Компрометация сервера видеозаписи (NVR/VMS) с целью получения доступа к архивам;
3. УБИ.ИД.01 Отказ в обслуживании (DDoS) компонентов системы;
4. УБИ.ИЦ.01 Подмена или модификация видеопотока (MITM-атака);
5. УБИ.ИК.03 Несанкционированный доступ к интерфейсу управления камерой;
6. УБИ.ИК.04 Утечка данных через облачный сервис видеонаблюдения;
7. УБИ.ИК.05 Неавторизованный просмотр архивов оператором;
8. УБИ.ИД.02 Физический доступ к оборудованию (камеры, кабельная инфраструктура) с целью вывода из строя.

На основе данного перечня и анализа уязвимостей сформирована детализированная модель угроз, представленная в Приложении 1.

Проведённый анализ показал, что наиболее критичными для системы IP-видеонаблюдения являются угрозы, связанные с нарушением конфиденциальности биометрических и служебных данных (УНК.1), а также угрозы нарушения целостности видеоданных (УНЦ.1). Высокая критичность данных угроз обусловлена строгими требованиями Федерального закона № 152-ФЗ «О персональных данных» и потенциальным ущербом для деловой репутации предприятия. Угрозы нарушения доступности (УНД.1) также являются значимыми, так как могут привести к полной потере оперативного контроля над охраняемыми зонами.

Меры противодействия:

* + шифрование видеопотоков по протоколу tls 1.3, сегментация сети с использованием vlan, организация vpn-туннелей для удалённого доступа;
  + внедрение строгой аутентификации и авторизации (ролевая модель), ведение детального журнала действий (logging), шифрование данных на дисках (bitlocker/luks), применение межсетевого экрана уровня приложений (waf);
  + сегментация сети, внедрение систем обнаружения и предотвращения вторжений (ids/ips), настройка qos для приоритизации видео-трафика, резервирование каналов связи и источников питания (ups);
  + применение сквозного шифрования видеопотоков, аутентификация устройств по стандарту ieee 802.1x, использование цифровых сертификатов (x.509);
  + обязательная смена паролей по умолчанию, внедрение двухфакторной аутентификации (2fa), изоляция камер в отдельном vlan с ограниченным доступом;
  + отказ от публичных облачных сервисов или использование сквозного шифрования (e2ee), регулярный аудит настроек безопасности облачного провайдера, резервное копирование на локальные носители;
  + внедрение системы разграничения прав доступа (rbac), обязательный аудит всех действий операторов, нанесение цифрового водяного знака (watermark) на архивные записи;
  + физическая защита камер и кабельных трасс (антивандальные кожухи, запираемые боксы), использование poe-коммутаторов с мониторингом состояния питания, периодический осмотр точек установки.

Данная модель угроз служит прямым основанием для проектирования защищённой архитектуры системы и выбора конкретных средств и мер защиты информации, направленных на нейтрализацию выявленных рисков.

## **Проектирование защищенной архитектуры системы IP-видеонаблюдения**

Для нейтрализации угроз, выявленных в разделе 2.1, и выполнения требований Федерального закона № 152-ФЗ «О персональных данных» проектируется защищённая архитектура системы IP-видеонаблюдения для офисных помещений ГУП «Московский метрополитен». Её ключевым принципом является строгая сегментация сетевой инфраструктуры, направленная на изоляцию видеотрафика, ограничение зоны воздействия при компрометации и контроль всех информационных потоков.

Выделение изолированных сетевых сегментов (VLAN) по функциональному признаку:

* + сегмент «общедоступные зоны» (vlan 10): объединяет камеры в холле, зоне ресепшена, основных коридорах. является источником биометрических персональных данных (пдн) посетителей и требует высокого уровня защиты конфиденциальности;
  + сегмент «конфиденциальные зоны» (vlan 20): включает камеры в кабинетах руководства, переговорных комнатах, отделах бухгалтерии и кадровой службы. защита этого сегмента направлена на обеспечение максимальной конфиденциальности служебной и коммерческой информации;
  + сегмент «технические помещения» (vlan 25): включает камеры в серверной, ит-помещениях, телекоммуникационных узлах. задача — обеспечение доступности и целостности видеоинформации о критической инфраструктуре.

1. Создание защищённого серверного сегмента (VLAN 30 – Видеонаблюдение): все IP-камеры направляют потоки строго в этот изолированный сегмент, где размещаются основной и резервный серверы записи (NVR/VMS). Прямой доступ к камерам и серверам из офисной сети (например, из сегмента пользователей) технически исключён.
2. Организация контролируемых каналов доступа для мониторинга:
   * внутренний мониторинг автоматизированное рабочее место (арм) оператора безопасности, расположенное на посту охраны в офисе, получает доступ к серверам vms через выделенный интерфейс из сегмента административного доступа (vlan 40). весь трафик между этими сегментами фильтруется и контролируется межсетевым экраном, настроенным на основе модели «наименьших привилегий».
   * удалённый мониторинг доступ для уполномоченных лиц (руководство, администраторы системы) организуется исключительно через криптографически защищённый vpn-туннель (ipsec/ikev2). терминация vpn происходит в демилитаризованной зоне (dmz), что предотвращает прямой контакт внешней сети (интернет) с внутренним сегментом видеонаблюдения.

Логическая схема защищённой сети IP-видеонаблюдения для офисных помещений представлена на рисунке 3.

Архитектура, реализует принцип глубокой эшелонированной обороны. Она обеспечивает выполнение ключевых требований информационной безопасности: сегментацию корпоративной сети, контроль информационных потоков, защиту персональных данных (в соответствии с ФЗ-152) и минимизацию ущерба от инцидентов ИБ.

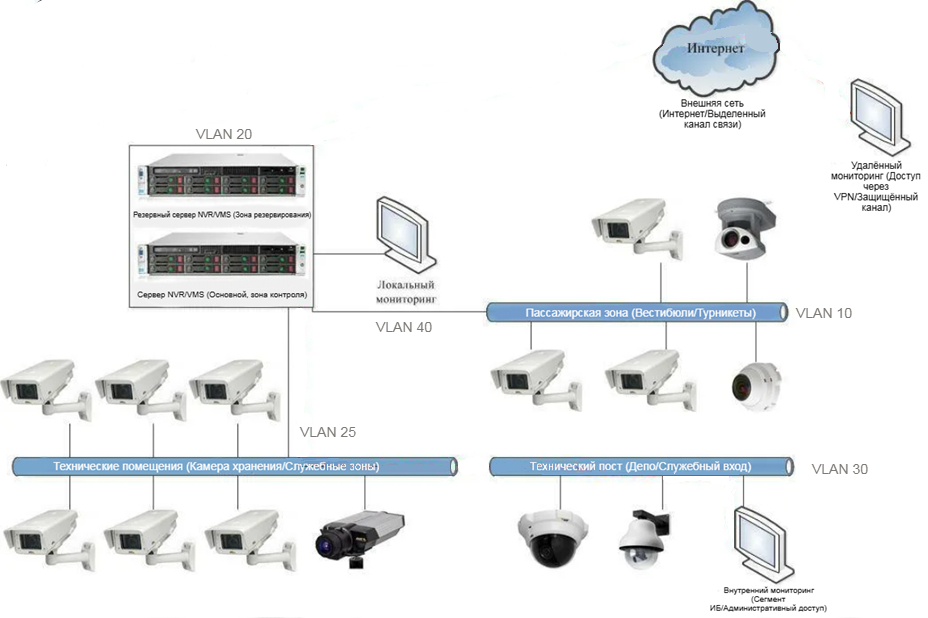


Рисунок 3 — Логическая схема защищенной сети IP-видеонаблюдения

Таким образом, предложенная архитектура на основе строгой сегментации контролируемых каналов доступа (межсетевой экран, VPN, DMZ) обеспечивает эффективное противодействие угрозам. Изоляция видеотрафика на уровне отдельных сетевых сегментов предотвращает его смешивание с общим корпоративным трафиком и ограничивает зону потенциального воздействия в случае компрометации одного из сегментов. Организация доступа через выделенные защищённые каналы гарантирует конфиденциальность биометрических и служебных данных при их просмотре и управлении. Данная архитектура служит технической основой для следующего этапа выбора конкретных средств защиты информации (СЗИ) для каждого компонента системы.

## **2.3 Выбор и обоснование выбранных решений защиты информации для компонентов системы видеонаблюдения**

Внедряемая система IP-видеонаблюдения предназначена для защиты ключевых активов и информации в офисных помещениях ГУП «Московский метрополитен»:

* + конфиденциальная информация коммерческая тайна (ход переговоров, стратегические документы), служебная информация, биометрические персональные данные сотрудников и посетителей.
  + критическая инфраструктура серверное и сетевое оборудование в серверных и телекоммуникационных узлах.
  + физическая безопасность обеспечение безопасности персонала и материальных ценностей.

На основе спроектированной защищённой архитектуры и модели угроз осуществляется выбор технических средств защиты, направленных на нейтрализацию рисков и выполнение требований Федерального закона № 152-ФЗ «О персональных данных» и Приказа ФСТЭК России № 21.

Для обеспечения масштабируемости, упрощения управления и снижения эксплуатационных затрат для всех сегментов офисной сети видеонаблюдения выбрана единая модель купольной IP-камеры Hikvision DS-2CD2347G2-LU представленной на рисунке 4. Данный выбор обоснован следующими характеристиками, удовлетворяющими требованиям всех зон:



Рисунок 4 — Hikvision DS-2CD2387G2-LSU/SL

1. Технические характеристики, отвечающие требованиям различных зон:
   * разрешение 4 мп (2560 × 1440): обеспечивает достаточную детализацию для идентификации лиц в общедоступных зонах и фиксации событий в служебных помещениях.
   * технология colorvu: гарантирует цветное изображение высокой чёткости в условиях слабого искусственного освещения коридоров, холлов и кабинетов без использования ик-подсветки, сохраняя эстетику офисного пространства.
   * универсальность установки: купольный корпус является ненавязчивым и подходит для монтажа на потолке или стене в любом типе помещения.
2. Встроенные механизмы информационной безопасности:
   * шифрование видеопотока (tls 1.2/1.3): ключевая мера защиты от угроз перехвата (унк.1) и подмены видеоданных (унц.1). шифрование трафика между камерой и сервером nvr обеспечивает конфиденциальность и целостность передаваемых биометрических пдн и служебной информации.
   * аутентификация по стандарту 802.1x: позволяет реализовать строгую сетевую аутентификацию устройства, предотвращая несанкционированное подключение к сегментам vlan видеонаблюдения.
   * защита интерфейса управления: обязательная смена паролей по умолчанию и поддержка политик сложных паролей блокирует несанкционированный доступ к настройкам камеры.
3. Надёжность и эксплуатационная устойчивость:
   * степень защиты ip67: обеспечивает полную защиту от пыли и влаги, что гарантирует работу в условиях влажной уборки и в запылённых серверных помещениях.
   * поддержка power over ethernet (poe): питание по сетевому кабелю упрощает развёртывание, снижает затраты на монтаж и позволяет организовать централизованное резервное питание всех камер через poe-коммутаторы с ибп, повышая отказоустойчивость системы.

Адаптация камеры для различных сетевых сегментов (VLAN)

* + для vlan 10 (общедоступные зоны): высокое качество цветного изображения достаточно для выполнения задач общего наблюдения и фиксации биометрических данных посетителей.
  + для vlan 20 (конфиденциальные зоны): интеграция с системой управления видео (vms) позволяет использовать функцию масок приватности (privacy masking). это даёт возможность программно исключить из обзора камеры области с рабочими столами, мониторами, документами и сейфами, добавляя дополнительный уровень защиты коммерческой тайны.
  + для vlan 25 (технические помещения): высокая степень защиты корпуса и устойчивость к внешним воздействиям обеспечивают круглосуточную работу в специфичных условиях серверных.

Для реализации принципов спроектированной архитектуры также выбраны:

* + система управления видео (vms): по ivideon (или аналог), поддерживающее ролевое разграничение доступа (rbac), детальный аудит действий операторов, шифрование архивов и нанесение цифрового водяного знака. это нейтрализует угрозы несанкционированного доступа к архивам (унк.1) и компрометации сервера (унк.1, унц.1).
  + сетевое оборудование: управляемые poe-коммутаторы с поддержкой vlan для реализации сегментации и межсетевой экран для фильтрации и контроля трафика между vlan 30 (серверный сегмент) и vlan 40 (административный доступ).

Выбор единой модели IP-камеры Hikvision DS-2CD2347G2-LU в сочетании с указанными программными и сетевыми решениями является технически и экономически обоснованным. Данный комплекс обеспечивает:

* + соответствие требованиям фз-152 и приказа фстэк №21 за счёт применения шифрования, аутентификации и разграничения доступа.
  + прямое противодействие выявленным угрозам (несанкционированный доступ, перехват, подмена данных, нарушение доступности).
  + создание унифицированной, управляемой и отказоустойчивой инфраструктуры видеонаблюдения для офисных помещений гуп «московский метрополитен».
  + оптимизацию затрат на закупку, внедрение, обучение персонала и техническое обслуживание системы.

Данные решения формируют техническую основу для практической реализации системы, описанной в следующем разделе.

# **Практический раздел**

## **План внедрения IP-видеонаблюдения в офис ГУП Московский метрополитен**

Реализация проекта внедрения защищенной системы IP-видеонаблюдения в корпоративную сеть ГУП «Московский метрополитен» осуществляется в соответствии с детально проработанным планом. Данный план обеспечивает последовательное выполнение всех этапов работ — от проектирования до ввода системы в эксплуатацию — с учетом требований информационной безопасности, выявленных в исследовательском разделе.

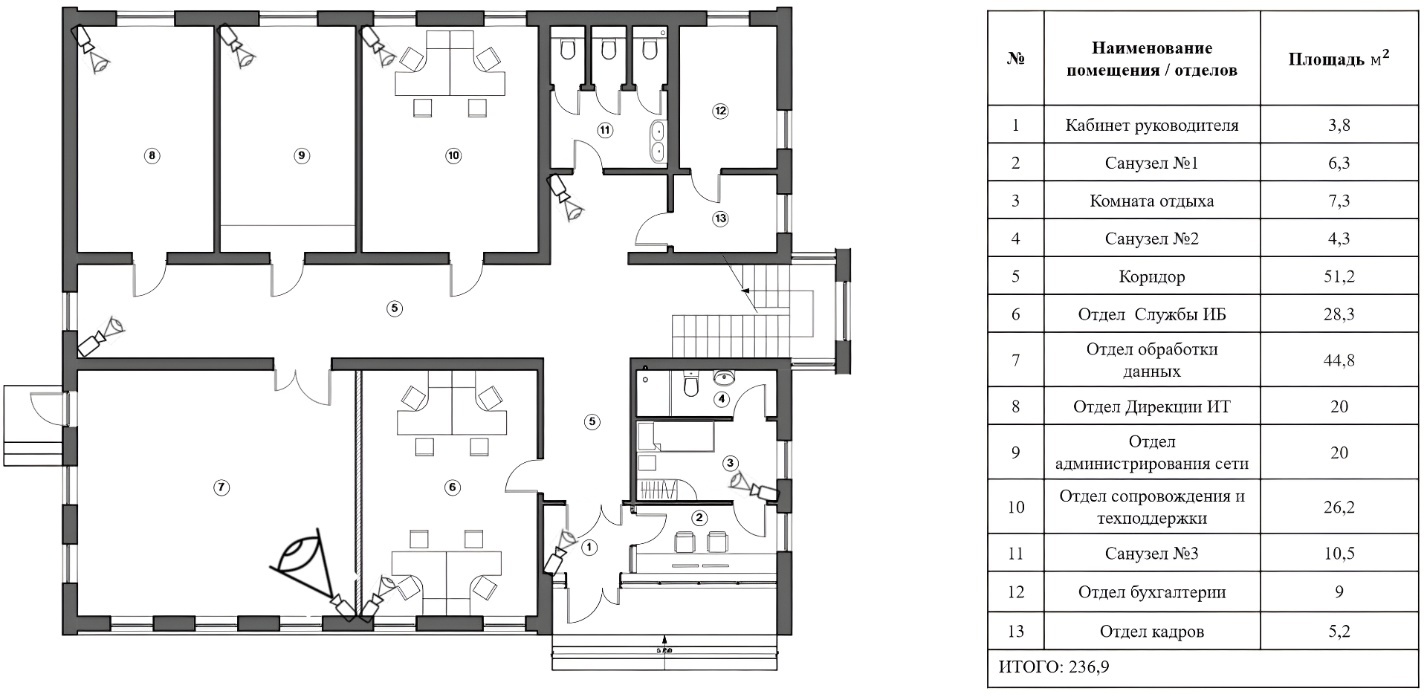


Рисунок 5 — План внедрения IP видоенаблюдения

План внедрения состоит из следующих ключевых этапов:

1. Этап 1. Предпроектное обследование и проектирование:
   * анализ существующей сетевой инфраструктуры офиса;
   * уточнение и согласование мест установки ip-камер на основе схемы помещений (см. рисунок 2);
   * разработка и утверждение технического задания, включая требования по информационной безопасности (сегментация, шифрование, контроль доступа);
   * создание логической схемы защищенной сети (см. рисунок 3) и спецификации оборудования.
2. Этап 2. Закупка и подготовка оборудования:
   * приобретение согласованного комплекта оборудования: ip-камеры hikvision ds-2cd2347g2-lu, poe-коммутаторы, серверы nvr/vms, межсетевые экраны, средства организации vpn;
   * предварительная настройка оборудования в лабораторных условиях (прошивка, базовые настройки безопасности).
3. Этап 3. Монтажные и пусконаладочные работы:
   * физический монтаж камер, прокладка и маркировка кабельных линий (витая пара категории 6а);
   * установка и коммутация сетевого оборудования (коммутаторы, патч-панели);
   * размещение и подключение серверного оборудования в защищенной серверной;
   * настройка сетевой инфраструктуры: создание и конфигурация VLAN (10, 20, 25, 30, 40) на управляемых коммутаторах.
4. Этап 4. Настройка системы безопасности и интеграция:
   * настройка межсетевого экрана для фильтрации трафика между сегментами VLAN и организации DMZ;
   * настройка VPN-шлюза (IPsec/IKEv2) для защищенного удаленного доступа;
   * настройка IP-камер: присвоение статических IP-адресов, включение шифрования TLS, настройка аутентификации 802.1X, изменение паролей по умолчанию;
   * установка и настройка системы управления видео (VMS): создание базы камер, настройка ролевого доступа (RBAC), планирования записи и детекции движения;
   * интеграция камер в VMS и настройка потоковой записи.
5. Этап 5. Тестирование и приемо-сдаточные испытания:
   * комплексная проверка работоспособности всех компонентов системы;
   * тестирование мер безопасности: проверка изоляции сегментов, работоспособности шифрования, корректности правил межсетевого экрана и VPN-доступа.
   * проведение нагрузочного тестирования и проверка отказоустойчивости;
   * составление и подписание актов выполненных работ.
6. Этап 6. Обучение персонала и ввод в эксплуатацию:
   * проведение инструктажа и обучение администраторов системы и операторов безопасности;
   * разработка и утверждение регламентов эксплуатации и обслуживания системы;
   * официальный ввод системы в промышленную эксплуатацию.

Данный план, представленный на рисунке 5, носит итерационный характер и предполагает возможность корректировки на каждом этапе по согласованию с ответственными подразделениями ГУП «Московский метрополитен» (Дирекция ИТ, Служба ИБ). Его выполнение гарантирует создание не просто работоспособной, но и соответствующей всем современным требованиям информационной безопасности системы видеонаблюдения.

## **Подготовка и настройка компонентов системы безопасности IP-видеонаблюдения**

Практическая реализация проекта начинается с настройки IP-камер, входящих в состав системы видеонаблюдения. Работы включают подключение к веб-интерфейсу, конфигурацию сетевых настроек, выбор видеокодека и интеграцию с системой хранения и обработки видео.



Рисунок 6 — Вход в веб-интерфейс IP-камеры

Для доступа к интерфейсу настройки IP-камеры используется её локальный IP-адрес как показано на рисунке 6. После ввода адреса в браузере открывается окно авторизации, где необходимо ввести логин и пароль, установленные производителем или заданные ранее администратором.

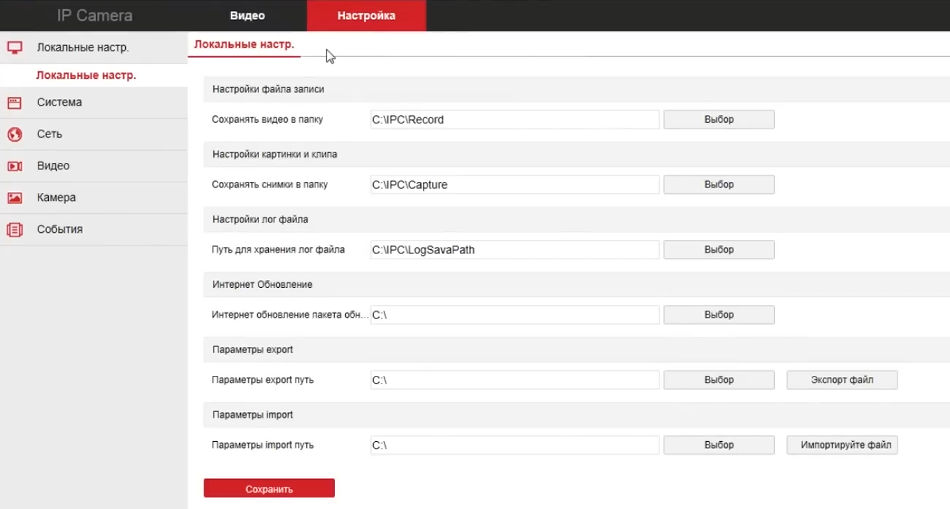


Рисунок 7 — Главное меню настроек камеры

После успешной авторизации открывается главное меню управления камерой, где доступны разделы: Основные настройки, Сеть, Видео, Аудио, Детекция движения, События показанные на рисунке 7.

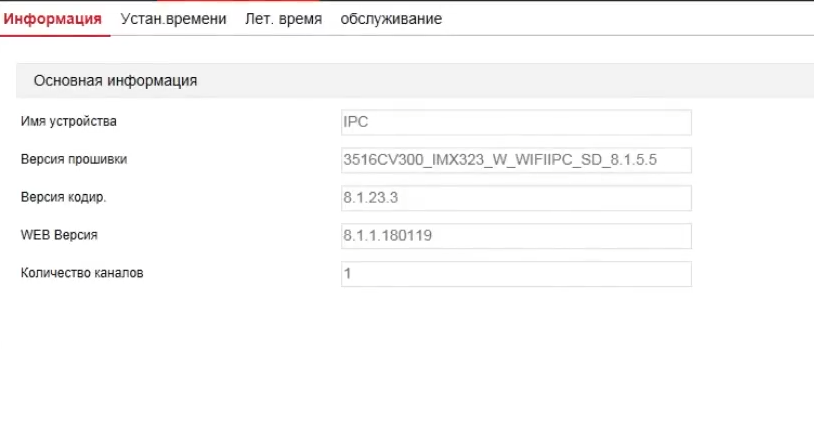


Рисунок 8 — Доступ к настройкам с локального компьютера

На рисунке 8 представлено, что с любого компьютера в локальной сети можно получить доступ к веб-интерфейсу камеры для изменения параметров в реальном времени, что удобно для удалённого администрирования.

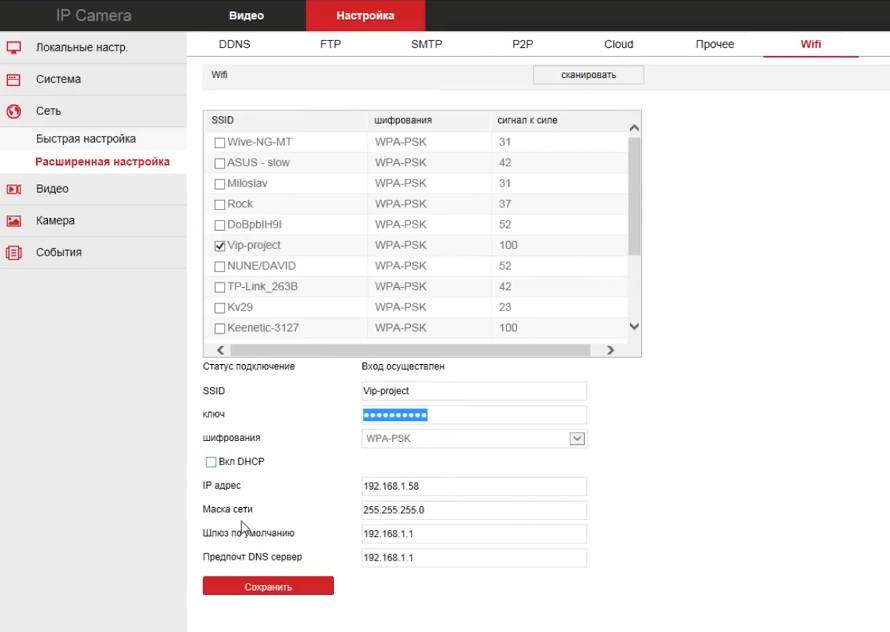


Рисунок 9 — Информация об устройстве

Настройка камеры в облачный сервис. Теперь отключить камеру от роутера или даже отключить её от сети и включить её заново там где ей предназначено стоять это озночает что оно автоматически всегда привязываться к wifi сети что представлено на рисунке 9.



Рисунок 10 — Настройка подключения к облачному сервису

Для обеспечения удалённого доступа и резервного копирования записей камера интегрирована с облачным сервисом что показано на рисунке 10. После настройки устройство автоматически подключается к сети Wi-Fi при перезагрузке.

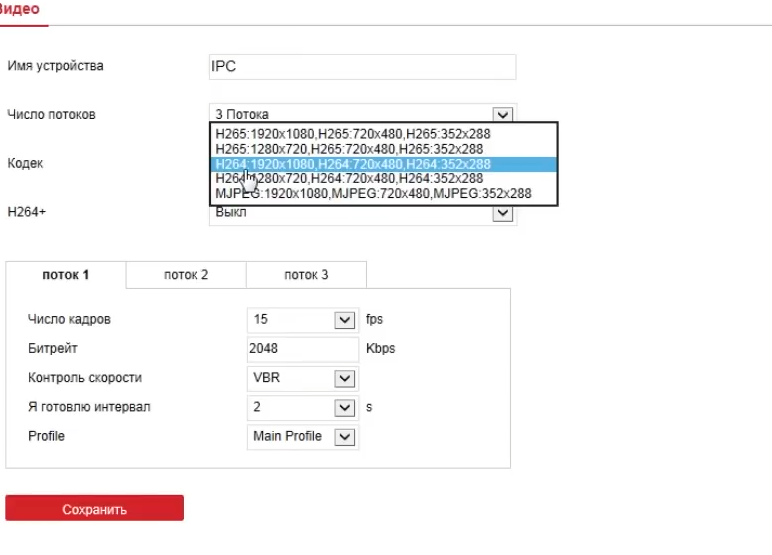


Рисунок 11 — Назначение статического IP-адреса

Для стабильной работы в корпоративной сети камере присвоен статический IP-адрес, что исключает его изменение при перезагрузке роутера что представлено на рисунке 10.

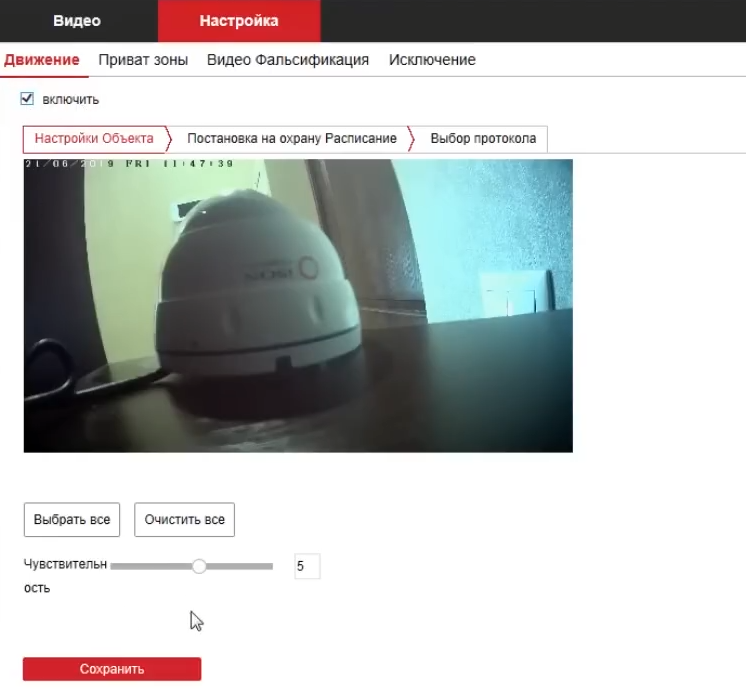


Рисунок 12 — Дополнительные сетевые настройки

В этом разделе настроены параметры DNS, шлюза и маски подсети, а также проверено подключение к сети как демонстрируется на рисунке 12.

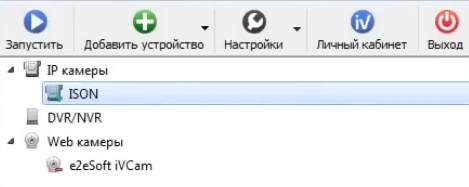


Рисунок 13 — Настройка видеокодека для оптимизации трафика

Для снижения нагрузки на сеть выбран видеокодек H.264 и настроен битрейт. Это позволяет уменьшить размер видео без значительной потери качества что показано на рисунке 13.

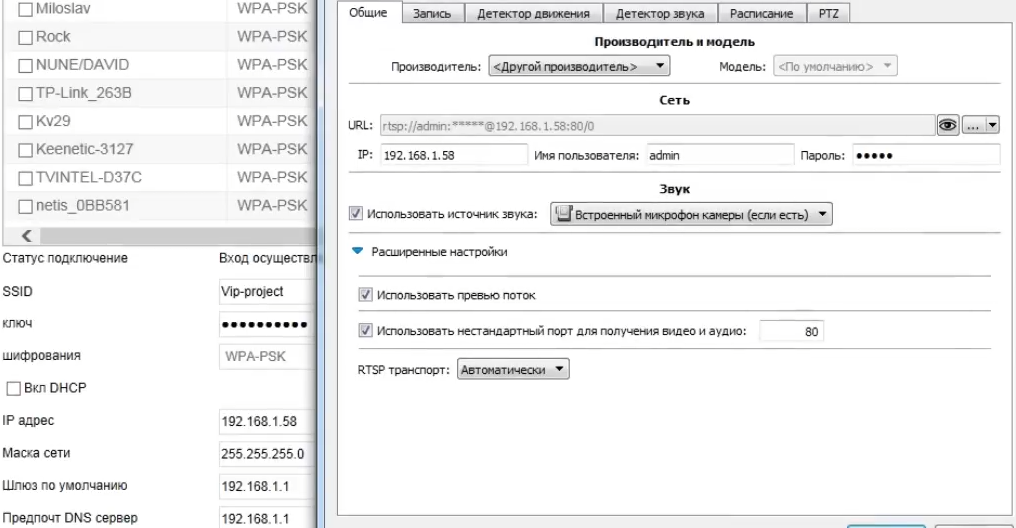


Рисунок 14 — Подключение к системе видеозаписи (NVR/VMS)

Для централизованного хранения записей камера подключена к сетевому видеорегистратору через RTSP-поток. Указан IP-адрес камеры и путь к видеопотоку как показано на рисунке 14.

## **3.2 Подготовка правил реагирования IP-видеокамер**

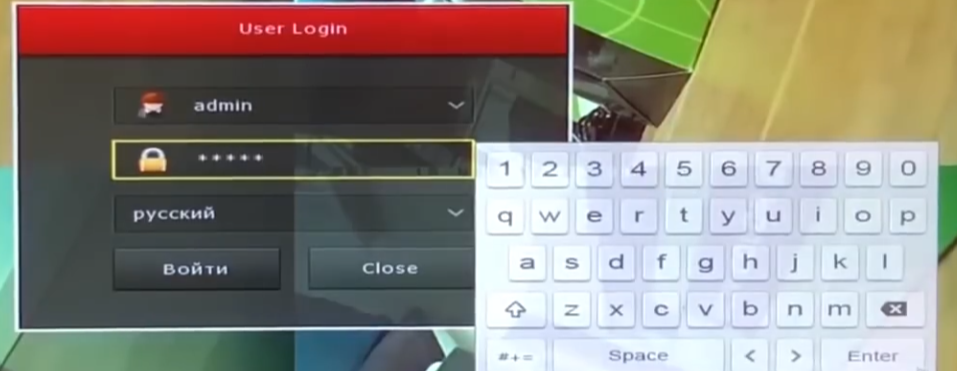


Рисунок 15 — Вход в меню управления функциями камеры

В этом интерфейсе доступны настройки расписания, детекции движения, записи по событию и отправки уведомлений что представлено на рисунке 15.

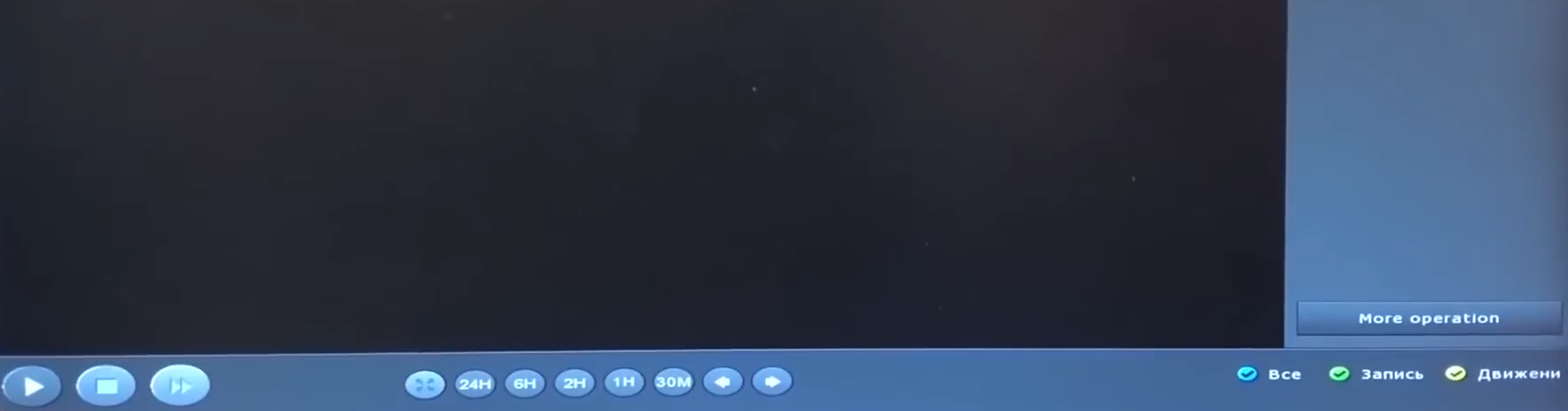


Рисунок 16 — Просмотр архивных записей

На рисунке 16 представлен раздел позволяет оперативно находить и воспроизводить записи по дате и времени, что актуально для расследования инцидентов.

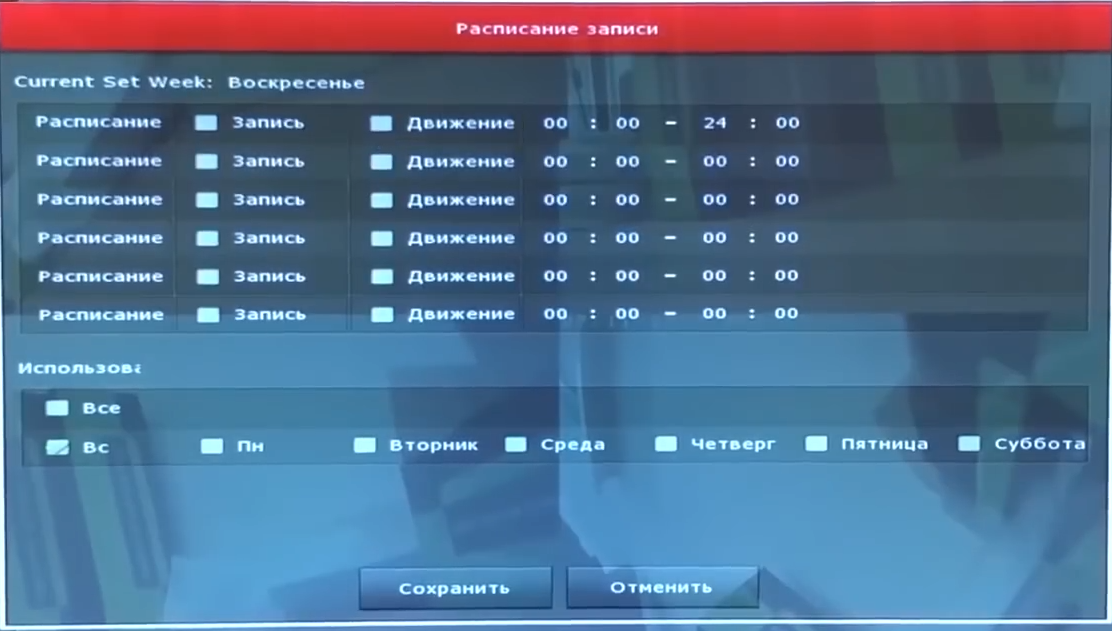


Рисунок 17 — Настройка расписания работы камеры

Задано расписание, в соответствии с которым камера автоматически активируется и деактивируется в заданные временные интервалы что представлено на рисунке 17.

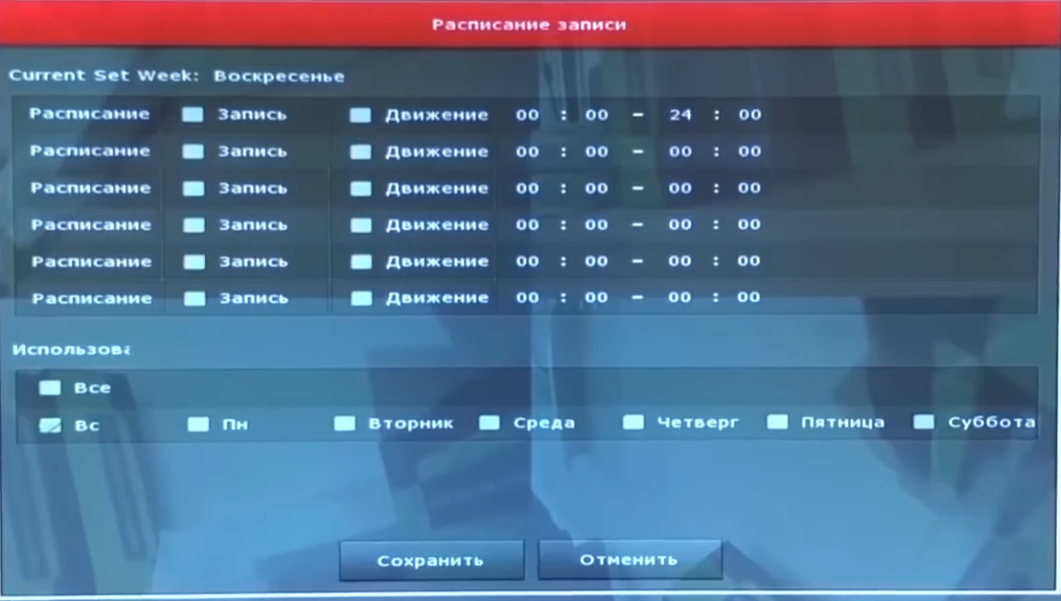


Рисунок 18 — Настройка детекции движения

Определены зоны детекции движения в кадре, что позволяет снизить количество ложных срабатываний и сфокусироваться на важных областях что показанно на рисунке 18.



Рисунок 19 — Настройка параметров записи

Установка параметров записи продолжительность фрагмента, условия начала записи (по движению/непрерывно), настройки перезаписи архива демонстрируется на рисунке 19.

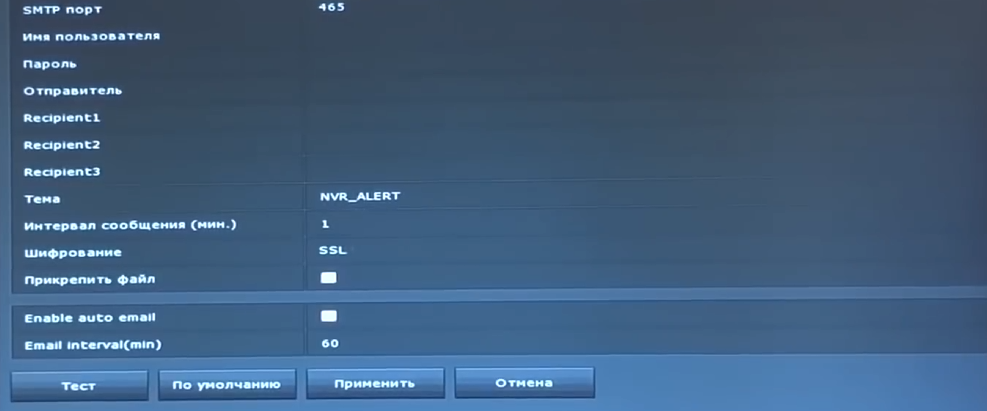


Рисунок 20 — Настройка уведомлений по e-mail

Для оперативного реагирования настроена отправка уведомлений что представлено на рисунке 20 на электронную почту при срабатывании детектора движения.

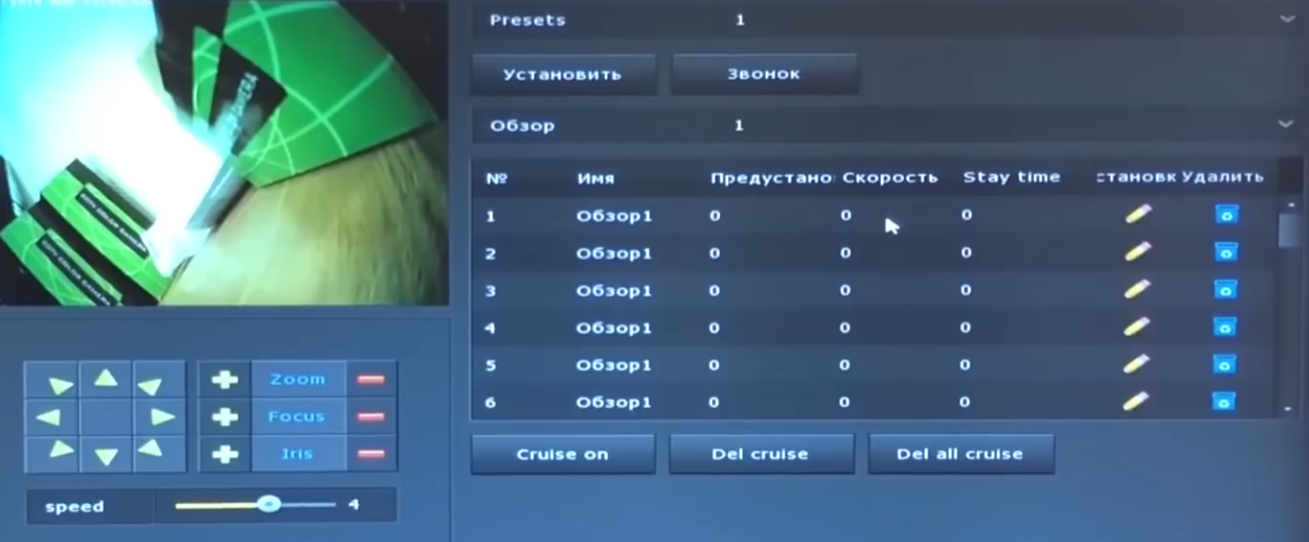


Рисунок 21 — Настройка поворотной (PTZ) камеры

Для камеры с функцией панорамирования и наклона заданы предустановленные позиции и маршруты патрулирования что показано на рисунке 21.

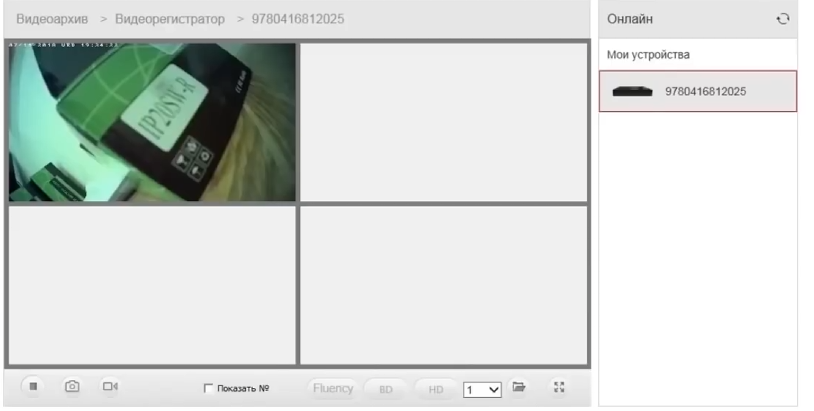


Рисунок 22 — Просмотр видео через веб-браузер

Реализована возможность просмотра видеопотока в реальном времени через веб-браузер с поддержкой технологии ActiveX как показано на рисунке 22.

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсового проекта достигнута поставленная цель разработана архитектура и реализован план внедрения защищенной системы IP-видеонаблюдения в корпоративную сеть ГУП «Московский метрополитен».

Успешно решены все поставленные задачи: проанализирована структура предприятия (объекта внедрения) и нормативно-правовая база, сформирована модель угроз, спроектирована архитектура с глубокой сегментацией сети, осуществлен выбор и обоснование оборудования с встроенными механизмами ИБ, а также проведена практическая настройка компонентов и тестирование системы.

Ключевым результатом проекта является комплексное решение, которое обеспечивает не только выполнение оперативных задач видеоконтроля, но и строгое соответствие требованиям ФЗ-152, ФЗ-16 и приказов ФСТЭК России. Внедренные меры сегментация, шифрование трафика, контроль доступа, централизованное управление эффективно нейтрализуют выявленные риски, связанные с конфиденциальностью биометрических данных и доступностью системы, создавая отказоустойчивую платформу безопасности для критически важного объекта транспортной инфраструктуры.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (последняя редакция от 24.02.2025).
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (последняя редакция от 24.02.2025).
3. Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» (последняя редакция от 26.07.2022).
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (последняя редакция от 24.02.2025).
5. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: Монография. — М.: Издательство «Юрайт», 2023. — 315 с.
9. Лапонина О.Р. Криптографические основы безопасности: Учебное пособие для вузов. 2–е изд., перераб. и доп. — СПб.: БХВ–Петербург, 2024. — 448 с.
10. Волкова Е.А., Сидоров В.П. Системы видеонаблюдения и видеоаналитики: проектирование и внедрение: учебное пособие. — М.: Инфра-Инженерия, 2023. — 278 с.
11. Методология тестирования на проникновение – PositiveTechnologies [Электронный ресурс] // URL: [https://www.ptsecurity.com/ru–ru/services/pentest/](https://www.ptsecurity.com/ru%E2%80%93ru/services/pentest/) (дата обращения: 12.02.2025).
12. Техническая документация по системам видеонаблюдения Hikvision [Электронный ресурс] // URL: <https://www.hikvision.com/ru/support/technical-documents/> (дата обращения: 12.02.2025).
13. Рекомендации по защите IP-видеонаблюдения от кибератак – PositiveTechnologies [Электронный ресурс] // URL: <https://www.ptsecurity.com/ru-ru/research/analytics/ip-video-surveillance-security/> (дата обращения: 12.02.2025).

Таблица 1 — Модель угроз информационной безопасности системы IP-видеонаблюдения в офисных помещениях ГУП «Московский метрополитен»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Наименование угрозы | Категория угрозы (по ГОСТ/ФСТЭК) | Нарушитель (категория) | Вероятность реализации (1–5) | Критичность (1–5) | Возможные последствия |
| 1 | Несанкционированный доступ к видеопотоку в реальном времени | УНК.1 (утечка данных) | Внешний (хакер), внутренний (сотрудник) | 4 | 5 | Утечка биометрических ПДн, перехват переговоров, компрометация коммерческой тайны |
| 2 | Компрометация сервера видеозаписи (NVR/VMS) | УНК.1, УНЦ.1 (изменение данных) | Внутренний (администратор), внешний (взлом) | 3 | 5 | Утечка архивов, удаление или фальсификация доказательств |
| 3 | Отказ в обслуживании (DDoS) камер или серверов | УНД.1 (нарушение доступности) | Внешний (хакер), внутренний (злоумышленник) | 3 | 4 | «Ослепление» системы, невозможность мониторинга, срыв расследований |
| 4 | Подмена или модификация видеопотока (MITM-атака) | УНЦ.1 (нарушение целостности) | Внешний (хакер) | 2 | 4 | Фальсификация событий, введение в заблуждение службы безопасности |
| 5 | Несанкционированный доступ к интерфейсу управления камерой | УНК.1, УНЦ.1 | Внутренний (сотрудник), внешний | 4 | 3 | Изменение настроек камеры, отключение, перехват управления |
| 6 | Утечка данных через облачный сервис видеонаблюдения | УНК.1 | Внешний (хакер), внутренний (ошибка настройки) | 3 | 5 | Утечка ПДн в открытый доступ, нарушение ФЗ-152 |
| 7 | Неавторизованный просмотр архивов оператором | УНК.1 | Внутренний (сотрудник СБ) | 4 | 3 | Нарушение конфиденциальности, несанкционированный сбор данных |
| 8 | Физический доступ к камере или кабелю | УНК.1, УНД.1 | Внутренний (сотрудник), внешний (проникновение) | 2 | 3 | Отключение камеры, подключение сниффера |