Технические требования к системе видеонаблюдения с искусственным интеллектом

П. Б. Яковлев

Петербургский государственный университет путей сообщения Императора Александра I

pavel050458@mail.ru

Е. И. Иванова

Петербургский государственный университет путей сообщения Императора Александра I

elena.ivanova.pgups@mail.ru

Аннотация. **В статье рассмотрены вопросы применения систем видеонаблюдения с искусственным интеллектом на железнодорожном транспорте. Сформулированы цели и задачи такой системы для обеспечения безопасной работы объектов инфраструктуры на основе требований, сформулированных в нормативных документах Российской Федерации.**

Ключевые слова: система видеонаблюдения; искусственный интеллект; объект инфраструктуры железнодорожного транспорта; безопасность

I. Введение

В условиях интенсивного пассажиропотока и сложной инфраструктуры мегаполисов обеспечение безопасности на железнодорожном транспорте становится одной из приоритетных задач. Традиционные методы мониторинга зачастую не справляются с оперативным выявлением угроз, что повышает риски возникновения чрезвычайных ситуаций. Современные технологии, такие как интеллектуальные системы видеонаблюдения с искусственным интеллектом (ИИ), предлагают принципиально новые возможности для решения этих проблем. Они позволяют не только автоматизировать анализ видеопотока, но и прогнозировать потенциальные инциденты, минимизируя влияние человеческого фактора.

Данная статья раскрывает принципы организации интеллектуальных систем видеонаблюдения (ИСВН) на объектах железнодорожного транспорта, включая их архитектуру, нормативные требования и меры защиты информации. Особое внимание уделяется соответствию законодательству РФ, техническим стандартам и обеспечению отказоустойчивости, что делает систему надежным инструментом для повышения безопасности пассажиров и инфраструктуры.

II. Технические требования

Важной задачей для любого объекта железнодорожного транспорта является обеспечение безопасности пассажиров.

Решение этой задачи возможно при внедрении систем видеонаблюдения с искусственным интеллектом (ИИ), которые используют алгоритм машинного обучения для анализа видеопотока с камер видеонаблюдения.

Эта функция имеет ряд преимуществ, которые имеют ключевое значение для мониторинга объектов транспортной инфраструктуры. Благодаря использованию машинного обучения, видеонаблюдение с ИИ предоставляет более точные и детальные данные аналитики.

Такие системы анализируют паттерны поведения, прогнозируют события, определяют аномальное поведение, а также могут проводить счет и классификацию объектов на видео. Видеонаблюдение с искусственным интеллектом делает возможным автоматизацию процессов, не вовлекая в процесс обработки видеопотока операторов, тем самым снижая нагрузку на персонал и уменьшая влияние человеческого фактора.

Данные системы могут незамедлительно обнаружить и идентифицировать лица, связанные с нарушениями транспортной безопасности, что может помочь в предотвращении инцидентов и расследовании происшествий.

Технические требования, предъявляемые к системам интеллектуального видеонаблюдения, регламентируются Постановлением Правительства РФ от 26 сентября 2016 г. N 969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности" (в редакции Постановления Правительства Российской Федерации от 03.05.2024 № 565).

Системы охранные телевизионные должны соответствовать требованиям ГОСТ Р 51558-2014 "Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний" и Рекомендациям "Р 78.36.008-99. Проектирование и монтаж систем охранного телевидения и домофонов", утвержденным Главным управлением вневедомственной охраны Министерства внутренних дел Российской Федерации 27 июня 1998 г.

Для проектирования IP-видеонаблюдения используются стандарты ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования». Этот ГОСТ основан на международных стандартах, в частности основная его часть является интегрированным переводом ИСО/МЭК11801:2002, ANSI/TIA/EIA-568B и ANSI/TIA/EIA-604-3.

В соответствии с главой 5 постановления к техническим системам и средствам идентификации физических лиц и обнаружения тревожных ситуаций предъявляются следующие требования [1, 2]:

- вероятность ложного пропуска для алгоритмов и аппаратно-программных средств детекции – не более 5 %;
- вероятность ложноотрицательной идентификации для алгоритмов и аппаратно-программных средств – не более 15 %;
- вероятность ложноположительной идентификации для алгоритмов и аппаратно-программных средств – не более 1 %;
- пропускная способность аппаратно-программных средств идентификации – не более 3 секунд.

В состав технических систем и средств идентификации физических лиц и обнаружения тревожных ситуаций включаются средства регистрации видеоизображений, к которым предъявляются следующие требования:

- разрешение регистрируемого видеоизображения – минимум 1,2 мегапикселя;
- частота кадров – не менее 16 кадров в секунду;
- разрешающая способность – разрешение на рабочей дистанции съемки объектов размером не менее 2 миллиметров (значения для области в центре кадра и на расстоянии до 1/3 ширины, высоты и диагоналей кадра от центра включительно);
- глубина резко отображаемого пространства - не менее 1 метра (для области в центре кадра и на расстоянии до 1/3 ширины, высоты и диагоналей кадра от центра включительно);
- расстояние между центрами глаз на изображении лица, зарегистрированном на рабочей дистанции съемки, – не менее 60 пикселей (для области в центре кадра и на расстоянии до 1/3 ширины, высоты и диагоналей кадра от центра включительно);
- максимальное отношение "сигнал – шум" (с выключенной функцией автоматического усиления сигнала) – не менее 45 дБ;
- дисторсия – не более 5 % (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).

Технические системы и средства идентификации физических лиц и обнаружения тревожных ситуаций должны обеспечить:

- взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;
- обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

Архитектура системы интеллектуальной системы видеонаблюдения (ИСВН) строится по модульному принципу и должна обеспечивать:

- взаимодействие между подсистемами и элементами, основанное на унифицированном и открытом стандарте интерфейсов;
- возможность подключения информационной системы видеонаблюдения (ИСВН) к Единой многомодульной транспортной системе (ЕМТС) государственных органов Санкт-Петербурга;
- возможность интеграции с системой мониторинга и управления инженерными системами зданий и сооружений (СМИС), которая имеет структурированную форму;
- возможность масштабирования ИСВН по числу видеокамер;
- масштабируемость функциональности: возможность подключения новых модулей видеоаналитики без привлечения разработчиков ИСВН;
- масштабируемость по объему хранимых данных;
- масштабируемость по числу пользователей;
- возможность независимой модернизации отдельных компонентов ИСВН без влияния на другие компоненты ИСВН;
- единая отчетность, включая архивацию событий в системе;
- централизованное администрирование и управление политикой доступа пользователей к информационным ресурсам;
- централизованный мониторинг и управление состоянием системы, включая телекамеры, серверы и сеть передачи данных.

Подсистема видеонаблюдения имеет сетевую структуру, которая выполняется с использованием современных цифровых устройств и модулей регистрации и должна включать в себя:

- видеосерверы, которые поставляются с предустановленным программным обеспечением и имеют встроенное хранилище с RAID-массивом;
- удаленные рабочие места на основе компьютеров с предустановленным программным обеспечением;
- сетевые коммутаторы;
- жидкокристаллические мониторы;
- уличные стационарные IP-камеры "день-ночь" в гермокожухе с подогревом;
- стационарные IP-камеры "день-ночь" в гермокожухе для установки внутри зданий;
- структурированная кабельная система для передачи потоков данных по волоконно-оптическим линиям и медным кабелям (типа витая пара);

- система питания устройств по технологии PoE (Power over Ethernet) подачи электропитания на видеокамеры через кабель витая пара UTP Cat.5E;
- оборудование для защиты аппаратуры и обогрева.

Необходимо принять меры для обеспечения сохранности информации, минимизации ущерба от потери данных и восстановления в случае аварийных ситуаций или отказа технических средств. Это может включать такие действия, как обеспечение бесперебойного питания, использование RAID-массивов для повышения отказоустойчивости системы хранения данных, резервное копирование информации.

Для восстановления данных и программного обеспечения следует предусмотреть возможность как ручного, так и автоматического резервного копирования и архивирования информации. Также в системе должны быть источники бесперебойного питания (ИБП), которые обеспечат резервное питание устройств в течение 48 часов, позволяя переключиться на другие источники энергии или завершить работу системы. Все эти меры должны быть реализованы на уровне программного обеспечения и иметь организационно-техническую реализацию.

Информационная система видеонаблюдения (ИСВН) соответствует требованиям действующего законодательства Российской Федерации и нормативных документов в области защиты информации, таких как Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года N 149-ФЗ (ред. от 08.08.2024) и Приказ ФСТЭК России от 11.02.2013 года N 17 (ред. от 28.08.2024).

Обеспечение информационной безопасности ИСВН осуществляется с помощью комплекса программно-аппаратных средств защиты информации и организационных мероприятий, направленных на противодействие потенциальным угрозам. Эти угрозы могут нанести ущерб владельцу информационного ресурса, информационной системы и пользователям ее услуг.

Оценка угроз безопасности информации основывается на возможностях внешних и внутренних нарушителей, анализе уязвимостей системы и последствиях нарушений. Для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), который ведется ФСТЭК России в соответствии с установленными нормами и положениями.

К основным видам угроз информационной безопасности ИСВН относятся следующие:

- противоправные действия третьих лиц;
- ошибочные действия пользователей и обслуживающего персонала;
- вредоносные программно-технические воздействия на средства вычислительной техники и информацию, которые могут привести к уничтожению, изменению, блокированию, копированию или распространению информации;
- отказы и сбои программных средств ИСВН, включая периферийное оборудование.

Точками приложения угроз безопасности информации в системе ИСВН являются:

- активное сетевое оборудование, такое как концентраторы и коммутаторы;
- дисковые массивы систем хранения данных, накопители и серверы различного назначения;
- оборудование телекоммуникационной системы;
- рабочие места операторов и дежурных.

В системе ИСВН реализуются меры, соответствующие требованиям действующих законодательных и нормативных правовых документов по защите информации. Эти меры включают:

- размещение рабочих мест и серверов системы в специально выделенных помещениях метрополитена с ограниченным доступом для защиты информации от несанкционированного доступа;
- управление доступом и регистрацией для защиты информации от несанкционированного доступа.

Основные требования сопровождаются также отраслевыми, описанными для разных категорий объектов ведомственными нормативами. Их тоже обязательно учитывать при проектировании систем видеонаблюдения.

III. Заключение

Внедрение интеллектуальных систем видеонаблюдения с использованием искусственного интеллекта представляет собой стратегически важный шаг в модернизации транспортной безопасности. Такие системы не только обеспечивают круглосуточный мониторинг и автоматическое обнаружение угроз, но и значительно снижают нагрузку на персонал за счет исключения рутинных операций. Соответствие требованиям ГОСТ, Постановлений Правительства РФ и ФСТЭК гарантирует их надежность и легитимность применения.

Ключевыми преимуществами ИСВН являются: высокая точность аналитики на базе машинного обучения; масштабируемость и интеграция с существующей инфраструктурой (ЕМТС, СМИС); защита данных через RAID-массивы, ИБП и резервное копирование; соблюдение норм информационной безопасности.

Реализация подобных систем не только повышает уровень безопасности, но и создает основу для дальнейшего развития «умных» транспортных сетей, где технологии ИИ станут неотъемлемой частью управления критически важными процессами. В перспективе это позволит минимизировать риски, оптимизировать затраты и обеспечить максимальную защиту пассажиров и инфраструктуры.

Список литературы

[1] Постановление МинТранса РФ от 26 сентября 2016 г. № 969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и

Правил обязательной сертификации технических средств обеспечения транспортной безопасности".

[2] ГОСТ Р 51558-2014 "Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний".

[3] ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования».

[4] Яковлева Н.А, Яковлев П.Б. Особенности создания интеллектуальной системы видеонаблюдения на вокзалах и пассажирских станциях // 77-я научно-техническая конференция СПбНТОРЭС им. А.С. Попова, посвященная Дню радио: сборник трудов. СПб: СПбГЭТУ «ЛЭТИ», 2022. С. 190-1922.

[5] Рыжова В.А., Ярышев С.Н., Коротаев В.В. Интеллектуальные системы видеонаблюдения. СПб, Университет ИТМО, 2021. 107 с.