Рис. 3. Точечный пожарный извещатель ИП–212–3СУ

В качестве приемно-контрольного прибора используется «Юпитер–1931» (рисунок 4).

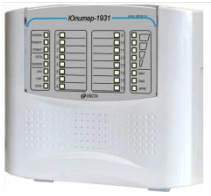

Рис. 4. Приемно-контрольный прибор «Юпитер–1931»

Передача информации проходит по каналам Ethernet и GSM. К техническим характеристикам данного прибора можно отнести следующие:

- возможность подключения до 16 зон охраны;
- две SIM−карты;
- отправка сообщений на телефон пользователя;
- благодаря Ethernet и GSM появилась возможность проводить обновление программного обеспечения удаленно;
- конфигурирование с помощью USB, SMS.

Основными компонентами системы оповещения и управления эвакуацией являются широкополосные настенные громкоговорители LPA–10W3. К основным достоинствам такого прибора можно отнести следующие: высокое качество звука; широкая диаграмма направленности; высокое звуковое давление; простота установки.

Обеспечение пожарной безопасности офисов достигается путем установки системы противопожарной защиты. Немаловажно и обучение персонала правилам пожарной безопасности.

Важнейшим условием предотвращения пожара является постоянный контроль за опасными участками офисного помещения и соблюдение правил пожарной безопасности. Проанализировав уровень защищенности помещения, можно сделать вывод, что дополнительные меры для улучшения пожарной безопасности в данном случае не требуются.

Список использованных источников:

1. Беляков Г.И. Пожарная безопасность: учебное пособие для вузов / Г.И. Беляков. – Москва: Издательство Юрайт, 2024. – 282 с. – (Высшее образование). – ISBN 978-5-534-17042-9. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https: // urait.ru/bcode/537038 (дата обращения: 14.01.2025).
2. Михайлов Ю.М. Пожарная безопасность в офисе / Ю.М. Михайлов. – М.: Альфа-Пресс, 2018. – 120 с.
3. Собурь С. В. Доступно о пожарной безопасности / С.В. Собурь. – М.: Пожарная книга**,** 2021. – 554 с.

ОБОРУДОВАНИЕ ДЛЯ ПЕРИМЕТРАЛЬНОЙ ЗАЩИТЫ УЧРЕЖДЕНИЯ С ОГРАНИЧЕННЫМ ДОСТУПОМ

Н.Ю. Дурнов[а], студент гр. З-17Г31, В.А. Шарапова, студент гр. 17Г21,
Научный руководитель: Деменкова Л.Г., к.пед.н., ст. преп.
Юргинский технологический институт (филиал)

Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: [a]manchester422442@gmail.com

Аннотация: в статье рассмотрены требования к оборудованию для периметральной защиты объектов УИС, в частности, внутренние и периметральные ограждения, инженерные заграждения, технические средства наблюдения, сигнализации, освещения, оповещения, контроля и управления доступом.

Ключевые слова: периметр, безопасность, оборудование, охрана, сигнализация, видеонаблюдение.

Abstract: the article considers equipment for perimeter protection of penal correctional facilities, in particular, internal and perimeter fences, engineering barriers, technical means of surveillance, signaling**,** lighting, notification, access control and management**.**

Keywords: perimeter, security, security equipment, security, security, alarm, video surveillance.

Не секрет, что охрана периметра является одним из наиболее распространенных инструментов снятия «головной боли» за сохранность имущества любого учреждения. Особенно это актуально для учреждений уголовно-исполнительной системы. Периметр охраняемого объекта – это первое, с чем столкнется злоумышленник при попытке осуществить несанкционированное проникновение. Экономическая целесообразность построения системы охраны периметра напрямую связана с величиной потенциального ущерба, который могут нанести «нежелательные гости» в результате незаконного проникновения. Поэтому стоимость решений для охраны периметра не должна выходить за рамки «разумного».

Эффективная система охраны периметра должна содержать сплошное наблюдение за периметром, инструменты подтверждения проникновения, комплекс тревожного оповещения по различным каналам связи, а также эффективную систему контроля и управления доступом, чтобы не превращать охраняемый объект в тюрьму для его вполне легальных обитателей. Опыт изучения различного рода источников в области видеонаблюдения, организации экстренного оповещения по различным каналам связи, а также применения технологий голосовой биометрии для разграничения доступа позволяет решить эти задачи тремя способами:

1. Внедрите сплошное видеонаблюдение.
2. Внедрите комплекс оповещения по различным каналам связи.
3. Внедрите систему голосовой биометрической верификации в качестве СКУД.

Защита периметра – важный элемент комплекса мер безопасности различных объектов, включая объекты с ограниченным доступом.

Успешное выполнение данных задач реально только при рациональном сочетании «человеческого фактора» с широким спектром современных и эффективных инженерно-технических средств охраны и надзора (ИТСОН). В комплекс ИТСОН входят внутренние и периметральные ограждения, инженерные заграждения, технические средства наблюдения, сигнализации, освещения, оповещения, контроля и управления доступом [1].

Для защиты периметра можно использовать следующее оборудование:

– физическая защита: заборы, колючие ограждения, инженерные конструкции и другие барьеры;
– охранная сигнализация: фиксирует происшествия и показывает, на каком участке случилось ЧП;
– видеонаблюдение: позволяет смотреть за происходящим;
– другие технические средства охраны: радары, лидары, тепловизоры и т. д.;
– патрулирование: человеческий глаз нередко замечает подозрительные объекты лучше приборов;
– охранники: могут на месте задержать нарушителей.

Особенность системы видеонаблюдения заключается в том, что она способна выступать как в роли системы обнаружения нарушения периметра, так и в роли системы подтверждения. Использование системы видеонаблюдения AVIDIUS™ способно успешно решить обе эти задачи. К примеру, в случае нарушения периметра в том месте, где «свои» не ходят, система способна детектировать движение, тем самым привлечь внимание к обнаружению «чужого».

С другой стороны, комплекс видеонаблюдения можно оснастить дополнительными внешними датчиками, чтобы оператор в нужный момент получал необходимое изображение на мониторе, служащее основанием для принятия решения. Критически важным для успешного обнаружения и подтверждения несанкционированного проникновения является возможность управления поворотом камер, расположенных по периметру и на внутренних рубежах охраны. Этот функционал позволяет расширить угол обзора и уменьшить общее количество камер в системе, что сокращает стоимость всего решения. Отличительным свойством систем видеонаблюдения, предназначенным для создания действительно эффективных комплексов охраны периметра, является возможность

записи звука. Аудиозапись расширяет возможности систем мониторинга нарушения периметра особенно в темное время суток, когда злоумышленники пытаются воспользоваться плохой видимостью для несанкционированного проникновения. В то же время звукозапись переговоров может служить в качестве профилактического средства в случае, когда удается детектировать подозрительные разговоры в радиусе действия видеокамер.

К тому же, необходим удобный интерфейс для управления множеством камер. Скорость и удобство переключения между камерами, управления их движением, приближения изображения и многих других функций – все это определяет скорость реагирования охраны на нарушение. Поэтому идеальным для системы видеонаблюдения является голосовое управление, позволяющее мгновенно произносить последовательность команд, ускоряющих работу оператора. Для любого средства обнаружения правонарушения критически важным является возможность привлечения внимания оператора к движению в поле зрения установленной камеры. Фраза «Движение на камере 1» в этом плане является наиболее эффективным средством, к тому же она подсознательно стимулирует оператора к произнесению голосовой команды «Камера 1 – полный экран». Таким образом, сокращается общее время реакции охраны на тревогу.

Следующим этапом после обнаружения и подтверждения факта правонарушения для эффективной системы охраны периметра является реагирование на него. И здесь возможен широкий спектр подходов. Функционал системы автоматического оповещения Рупор™ объединяет их в одном едином комплексе. Если объект имеет стратегическую важность, то группа реагирования, как правило, находится внутри периметра и имеет возможность достаточно оперативно выдвинуться на рубеж и пресечь несанкционированное проникновение. Однако для множества охраняемых зданий и сооружений бывает достаточным наличие одной группы реагирования на несколько объектов. При этом ключевым моментом является скорость реагирования, которая напрямую зависит от эффективности системы оповещения охраны. Оповещение охраны будет более эффективным, если оно осуществляется по различным каналам связи. Так, например, целесообразно одновременно оповещать и диспетчера группы охраны, и саму группу, оставив на совести диспетчера лишь подтверждение выезда группы и контроль. В результате сокращается количество передаточных звеньев, увеличивающих интервал между поступлением тревожного сигнала и выездом группы. При этом гибкость системы оповещения должна позволять использовать любые организационные решения в области оповещения (например, оповещение диспетчера – на монитор и по стационарной телефонной связи, а оповещение руководителей групп реагирования – через SMS или по рации). Это позволяет, с одной стороны, сохранить координирующую роль диспетчера охраны, а с другой – поддерживать постоянную готовность и мобильность групп реагирования.

Не менее важным фактором эффективного оповещения является способ формирования тревожного сообщения. Ведь разные каналы связи используют различные сигналы и воздействуют на ответственные за их прием органы чувств, а скорость распознавания сигнала критически важна для сферы безопасности. Поэтому оповещение на экран должно демонстрировать графически, на каком участке рубежа возникла угроза. Для формирования сообщений по телефону оптимально использование технологии синтеза речи, которая создает высокую степень гибкости для администратора системы. Комплекс автоматического оповещения Рупор™ сочетает в себе уникальные достижения в области речевых технологий и современных систем связи и передачи данных для формирования эффективной системы охраны периметра.

Охрана периметра не всегда осуществляется в ночное время суток, когда на объекте нет посторонних. Эта задача может быть поставлена и для обычного рабочего дня, когда охраняемый объект полон сотрудников и посетителей, имеющих право на нем находится согласно трудовому или иному распорядку. Таким образом, встает сложная задача по реализации прав доступа на объект для «своих» и охрана от проникновения «чужих». Одним из наиболее эффективных средств управления и контроля доступом является голосовая биометрическая верификация на базе технологии VoiceKey™. Преимуществом голоса над другими признаками служит его «бесконтактность» и «физическая неотделимость» от владельца.

Технология голосовой биометрической верификации VoiceKey™ способна значительно укрепить охрану объекта в будние дни и в рабочее время, когда интенсивность допускаемых к объекту посетителей значительно осложняет работу службе охраны. Голосовая биометрическая СКУД является мощным инструментом обеспечения безопасности охраняемого объекта.

Анализ литературы в сфере периметральной защиты позволяет прийти к следующим выводам: эффективная охрана периметра способна предотвратить несанкционированные посягательства на материальные и людские ресурсы учреждений с ограниченным доступом. В современных условиях следует применять комплексные решения для повышения эффективности системы охраны периметра на базе своих уникальных разработок в

области аудио- и видеонаблюдения, автоматического оповещения по различным каналам связи и передовых достижений в области синтеза, распознавания речи и голосовой биометрии.

Таким образом, чтобы построить эффективный охраняемый периметр, необходимо учесть несколько критически важных факторов: периметр должен быть сплошным, система охраны периметра должна не только фиксировать факт несанкционированного проникновения, но и наглядно его подтверждать; система обнаружения проникновения должна уметь оповещать ответственных лиц согласно установленному регламенту; система охраны должна иметь комплекс эффективного определения «свой-чужой» в рамках системы контроля и управления доступом для сокращения уровня ложных срабатываний на периметре и внутренних рубежах.

Список использованных источников:

1. Об утверждении Инструкции по служебной деятельности специальных подразделений УИС по конвоированию: совместный Приказ МЮ РФ и МВД РФ № 199/369 от 24 мая 2006 г.

2. Абдрахманов С.И. Системы охраны периметра. Общие требования к периметральным системам / С.И. Абдрахманов // Молодой ученый. – 2023. – № 52 (499). – 2025. – С. 4–6.

3. Мартяшин А.И. Преобразователи электрических параметров для системы контроля и измерения / А.И. Мартяшин, Э.К. Шахов, В.М. Шляндин. – М.: Энергия, 1976. – С. 378–389.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ПЕРЕВОЗКЕ ГРУЗОВ ТРАНСПОРТНЫМИ КОМПАНИЯМИ

С.М. Проскокова[а], студент гр. З-17Г11,
Научный руководитель: Деменкова Л.Г., к.пед.н., ст. преп.
Юргинский технологический институт (филиал)
Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: [а]smp3@tpu.ru

Аннотация: в статье рассмотрены основные задачи, функции и принципы деятельности транспортных компаний, изучена ответственность за нарушение правил перевозки в соответствии с действующим законодательством. Так же рассмотрены факторы и аспекты безопасности, влияющие на деятельность транспортных компаний.

Ключевые слова: мобильность, задачи, эффективность, грузоперевозки, безопасность, транспортные компании.

Abstract: the article discusses the main tasks, functions and principles of operation of transport companies, examines responsibility for violation of transportation rules in accordance with current legislation. The factors and aspects of safety affecting the activities of transport companies are also considered.

Keywords: mobility, tasks, efficiency, cargo transportation, safety, transport companies.

Проблема обеспечения безопасности грузоперевозок становится все более значимой в условиях роста объема транспортных услуг и увеличения числа инцидентов, связанных с утратой или повреждением грузов. По мере развития глобальных торговых связей и растущей интеграции различных экономик, транспортные компании сталкиваются с новыми вызовами, требующими внедрения и совершенствования системы безопасной логистики. Для избежания потенциальных проблем во время доставки грузов транспортными компаниями, важно гарантировать их безопасность и надежность, предотвращая возможные повреждения и потери.

Ответственность, возникающая из договора грузоперевозки, является взаимной и определяется статьёй 793 Гражданского кодекса РФ [1].

Транспортная компания обязана отвечать за такие нарушения, как несвоевременная подача транспортного средства, задержка в доставке, а также за утрату, недостачу и повреждение груза. Если груз потерян или имеется недостача, перевозчик должен компенсировать убытки в размере стоимости недостающего или утерянного товара. При повреждении или порче груза возмещение осуществляется в размере разницы между первоначальной стоимостью и стоимостью после повреждения [1].

Отправитель грузов отвечает перед перевозчиком в ряде ситуаций. В частности, он несет ответственность за следующее:

1. Если не выполнена заявка на перевозку;