ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРЦИИ

ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА»

СБОРНИК СТАТЕЙ

СЕМИНАР «ПУТИ ПОВЫШЕНИЯ ИНФОРМАТИВНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ БЕЗОПАСНОСТИ» 25 МАРТА 2025 ГОДА

МОСКВА 2025 г.

СБОРНИК СТАТЕЙ

СЕМИНАР «ПУТИ ПОВЫШЕНИЯ ИНФОРМАТИВНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ БЕЗОПАСНОСТИ»

25 МАРТА 2025 ГОДА

Вып. 1. – Москва: Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, 2025 г. – 22 с.

Редакционная коллегия:

Председатель
В.С. Зарубин

Заместитель председателя
А.Р. Фамильнов

Ответственный секретарь
А.Н. Морозов

Технический редактор
М.А. Гасанов

© ФКУ «НИЦ «Охрана» Росгвардии, 2025

СОДЕРЖАНИЕ

Введение 3

Баринов И.А., Талышев Н.В.
Повышение информативности систем централизованного наблюдения посредством изменения режима работы объектового оборудования 4

Вихирев А.А., Занин А.Н.
Новые возможности при организации охраны объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, на основе применения программных интеграционных платформ 8

Лялевич В.Г., Серебряков С.В.
Передача видеоподтверждения от систем охранного телевидения, установленных на охраняемых объектах на мобильные устройства связи, как одно из направлений повышения информативности технических систем безопасности 11

Панфилов А.А.
Повышение эффективности мониторинга объектов за счёт расширения возможностей мониторингового программного обеспечения 14

ВВЕДЕНИЕ

В сборнике содержатся результаты выступлений на семинаре «Пути повышения информативности технических систем безопасности», проведенном Федеральным казенным учреждением «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации 25 марта 2025 года.

Издание представляет интерес для специалистов вневедомственной охраны Росгвардии, сотрудников правоохранительных органов, предприятий и организаций, работающих в сфере обеспечения безопасности.

УДК 654.949
ББК 32.99

БАРИНОВ ИГОРЬ АЛЕКСАНДРОВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ТАЛЫШЕВ НИКОЛАЙ ВАСИЛЬЕВИЧ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ, НАЧАЛЬНИК ОТДЕЛА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ПОВЫШЕНИЕ ИНФОРМАТИВНОСТИ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ ПОСРЕДСТВОМ ИЗМЕНЕНИЯ РЕЖИМА РАБОТЫ ОБЪЕКТОВОГО ОБОРУДОВАНИЯ

Аннотация. В работе рассмотрена информативность как один из важнейших параметров системы централизованного наблюдения. Приведен анализ основных режимов функционирования объектового оборудования современных систем. Предложен вариант повышения информативности за счет изменения режима работы оборудования в режиме тревоги.

Ключевые слова: охраняемый объект, система централизованного наблюдения, информативность, динамическая модель.

BARINOV IGOR ALEXSANDROVICH**, RESEARCHER AT THE FEDERAL STATE INSTITUTION "SCIENTIFIC RESEARCH CENTER "PROTECTION" OF ROSGVARDIYA**
TALYSHEV NIKOLAY VASILYEVICH**, HEAD OF DEPARTMENT AT THE FEDERAL STATE INSTITUTION "SCIENTIFIC RESEARCH CENTER "PROTECTION" OF ROSGVARDIYA**

INCREASING THE INFORMATIVENESS OF CENTRALIZED MONITORING SYSTEMS BY CHANGING THE OPERATING MODE OF FACILITY EQUPMENT

Annotation. The paper considers information content as one of the most important parameters of centralized monitoring system. An analysis of the main modes of operation of the facility equipment of modern systems is given. A variant of increasing the information content by changing the operating mode of the equipment in the alarm mode is proposed.

Keywords: protected object, centralized monitoring system, informativeness, dynamic model.

Информативность, наряду с надёжностью и оперативностью доставки извещений о тревоге, является одним из важнейших параметров систем централизованного наблюдения (далее – СЦН) [1]. Задача повышения информативности СЦН, то есть получения наиболее полных сведений о состоянии технических средств, размещенных на охраняемом объекте, является актуальной как для инженерно-технического персонала, контролирующего работоспособность элементов системы обеспечения безопасности, так и для дежурных сотрудников, осуществляющих оперативное управление действиями экипажей групп задержания. Рост осведомленности оперативного персонала пункта централизованной охраны (далее – ПЦО) позволяет значительно повысить эффективность принимаемых ими управленческих решений и заблаговременно провести обоснованные мероприятия по усилению сил реагирования на угрозу. Это влечет за собой усиление моральной, ресурсной и тактической подготовленности нарядов, прибывающих к охраняемому объекту и осматривающего его. Кроме того, рост информированности дежурных сотрудников ПЦО о текущем динамическом состоянии технических средств охраны в системе распределенных объектов обеспечит возможность в условиях массовых поступлений на пульты централизованного наблюдения (далее – ПЦН) тревожных сообщений осуществить взвешенный выбор первоочередных направлений применения людских ресурсов для купирования наиболее вероятных реализаций угроз безопасности. Поэтому следование технических разработок по повышению информативности СЦН в русле крылатого выражения «предупрежден – значит вооружен» является приоритетной задачей.

В настоящее время в большинстве случаев данная задача решается за счет увеличения

количества устанавливаемых на объекте технических средств охраны, например, посредством монтажа дополнительного количества извещателей или интеграцией с иными системами обеспечения безопасности, в том числе системами охранного телевидения. Вместе с тем повышение информативности СЦН может быть достигнуто и без увеличения номенклатуры размещаемых на объекте средств обнаружения. Предлагаемое техническое решение позволяет сделать это за счет изменения режимов работы, существующего в настоящее время объектового оборудования и пультового программного обеспечения.

В применяемых в текущих условиях подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, а также частными охранными организациями СЦН объектовое оборудование функционирует в трех основных режимах работы: снят с охраны, взят под охрану и состояние тревоги. В последний режим объектовые устройства переходят после фиксации средством обнаружения критического изменения параметров окружающей среды или характеристик каналов связи, в том числе шлейфов сигнализации (далее – ШС) с последующей передачей извещения о тревожном состоянии на ПЦН. Кроме того, данное оборудование имеет ряд вспомогательных и контрольно-диагностических режимов, не влияющих на основные функциональные характеристики объектового оборудования. К ним относят: режим самотестирования, конфигурирования, программирования (обновления программного кода) и им подобные.

Проведенный в ходе выполнения научно-исследовательской работы анализ функционирования различных СЦН, а также обобщение опыта по их применению в реальных условиях показали, что существует возможность повышения информативности рассмотренных систем посредством изменения алгоритма функционирования объектового оборудования и модернизации пультового программного обеспечения в режиме тревоги, то есть после выявления техническими средствами обнаружения угрозы безопасности охраняемому объекту, обработки извещения и передачи его на ПЦН. Несмотря на то, что у отечественных производителей СЦН реализованы различные алгоритмы функционирования объектового оборудования в режиме тревоги, в большинстве таких систем охранные приборы после фиксации нарушения канала связи (ШС) прекращают их контроль до получения команды снятия с охраны с ПЦН либо от пользователя с помощью использования различного вида идентификаторов.

Корректировка алгоритма функционирования СЦН, выполняемая с целью повышение информативности, должна заключаться в обеспечении контроля объектовым оборудованием состояния извещателей, нарушенных каналов связи (ШС) в течении всего времени от момента фиксации тревоги до получения команды о снятии объекта с охраны и передаче соответствующих извещений на ПЦН в случае их изменения. Реализация данного режима работы СЦН позволит с помощью пультового программного обеспечения сформировать своеобразную динамическую модель состояния охраняемого объекта, которая основывается на информации, получаемой в режиме онлайн от всех установленных на нем технических средств обнаружения. Программы автоматизированных рабочих мест (далее – АРМ) дежурного пульта управления и серверов ПЦН, используя полученную информацию, должны обеспечить для оперативного персонала ПЦО цветовое или графическое отображение на плане охраняемого объекта помещений, с находящимися в них в состоянии тревоги извещателями, каналами связи или ШС. Это должно осуществляться, таким образом чтобы по изменениям сигналов, поступающих на входы объектового оборудования, отслеживалось нахождение и перемещение правонарушителей, совершивших несанкционированное проникновение на объект. При этом по увеличению количества перешедших в тревогу и не восстановившихся зон обнаружения была предоставлена возможность в режиме реального времени оценить количественный состава преступников, вероятность и места ухода с объекта или приближения к местам хранения материальных ценностей. Кроме того, сформированная на плане охраняемого объекта динамическая модель его состояния, должна передаваться на мобильные устройства сотрудников групп задержания, что позволит качественно повысить эффективность их действий и уровень личной безопасности при проведении мероприятий по его блокированию и осмотру.

Для реализации таких алгоритмов необходимо на основе анализа режимов работы средств обнаружения, каналов связи, а также особенностей функционирования объектовых приборов различных СЦН в режиме тревоги, осуществить формирование технических предложений по изменению алгоритма их работы и проведению модернизации объектового оборудования посредством изменения программного кода

их микроконтроллеров. Кроме того, при доработке пультового программного обеспечения ПЦН должна быть предусмотрена возможность отображения в динамике на графических планах объектов состояния технических средств охраны или помещений, в которые совершено несанкционированное проникновение.

Главным техническим параметром в работе средств обнаружения, на который следует ориентироваться в части изучения возможностей повышения информативности СЦН, является время восстановления работоспособности извещателя из состояния тревоги в нормальное состояние [2]. При этом чем меньше времени ему требуется для выхода на дежурный режим, тем точнее, оперативнее и достовернее будет модель состояния объекта, сформированная пультовым программным обеспечением, отражать ситуацию в помещениях. В требованиях отечественных государственных стандартов на большинство наиболее распространенных типов извещателей, таких как: точечные магнитоконтактные, поверхностные вибрационные, поверхностные звуковые, поверхностные емкостные, линейные радиоволновые, объёмные оптико-электронные и комбинированные, указанный параметр не должен превышать 10 секунд, а в средствах обнаружения, передающих извещения формированием кодовой комбинации по беспроводным линиям связи, данное значение ограничено 70 секундами [3, 4]. Большее значение этого параметра в последнем случае связано с существующими особенностями организации циклической передачи такими средствами обнаружения тестовых и информационных посылок на объектовый прибор (устройство оконечное) и напрямую зависит от емкости развернутой на охраняемом объекте подсистемы. В связи с тем, что значение времени восстановления извещателей в нормальное состояние связано с физическими принципами, лежащими в основе работы их чувствительных элементов, то его уменьшение не представляется возможным. Однако наличие указанной информации для различных типов средств обнаружения будет востребовано на этапе формирования изменений в алгоритмы функционирования программного обеспечения серверов и АРМ ПЦН СЦН.

Проведенный анализ технических характеристик объектовых приборов, используемых в составе различных СЦН, применяемых подразделениями вневедомственной охраны и частными охранными организациями, показал, что в настоящее время компаниями-производителями реализованы различные варианты режимов функционирования данного оборудования после фиксации недопустимого воздействия на ШС или выявления нарушений извещателями. Наиболее раритетным на сегодняшнем рынке охранной техники является алгоритм, при котором объектовый прибор прекращает контроль ШС с момента получения тревожного сообщения до получения команды о снятии с охраны или обесточивания системы. Такой режим сохранился в радиоканальной СЦН «Струна-5» и программно-аппаратном комплексе «Астра».

Производители других СЦН, таких как «Заря» и «Молния» реализовали в объектовых приборах осуществление после фиксации тревоги однократной попытки контроля ШС через фиксированный интервал времени и в случае его восстановления производится повторная постановка данного оборудования под охрану с передачей соответствующего извещения на ПЦН. В СЦН «Центавр Проксима» разрешается осуществить три таких попытки и если в ходе их подтверждается сохранение недопустимых параметров на данном входе объектового прибора, то используемый им канал связи блокируется в тревожном состоянии. В настройках объектового прибора радиоканальной СЦН «Протон» предусмотрена возможность установить необходимый временной интервал в диапазоне от 20 до 240 сек, по прошествии которого осуществляется повторная попытка контроля ШС и взятие его под охрану. При этом таких попыток периодического контроля и повторной постановки канала связи с средствами обнаружения, установленными на объекте, под охрану может быть установлено в диапазоне от 5 до 15, после чего также прекращается его контроль.

Наиболее оптимальным алгоритмом работы объектовых приборов является режим постоянного контроля параметров на подключенных к входам объектовых приборов ШС все время от фиксации нарушения до получения команды снятия. В настоящее время функция непрерывного анализа состояния ШС и передачи фиксируемых объектовым оборудованием изменений соответствующими извещениями на ПЦН реализована в СЦН «Приток-А», «Ладога», «Ахтуба», «Юпитер». Использование указанного режима позволяет с помощью пультового программного обеспечения АРМ ПЦН и серверов сформировать на плане охраняемого объекта своеобразную динамическую модель, которая позволит предоставить дежурным сотрудникам подразделений вневедомственной охраны дополнительную информацию о состоянии технических средств обеспечения безопасности на охраняемом объекте, о нахождении и перемещениях по его помещениям лиц, осуществивших незаконное проникновение.

Реализация подобного режима работы в объектовых приборах СЦН, у которых оборудование при функционировании не обеспечивает непрерывный контроль параметров ШС, потребует проведения доработки встроенного программного обеспечения (прошивок) микроконтроллеров. При этом обновленный алгоритм работы объектового прибора СЦН должен обеспечивать фиксацию нарушения на своих входах, формирование и передачу тревожного извещения на ПЦН и не прерываясь продолжать контролировать состояния подключенных к нему средств обнаружения до получения команды о снятии объекта с охраны, а при изменении в течение этого периода работы входных параметров инициировать направление соответствующего извещения на ПЦН.

В свою очередь поддержка указанного режима работы оборудования на объекте потребует изменения алгоритмов функционирования АРМ ПЦН и серверов СЦН с соответствующей доработкой их программного обеспечения. Так как в настоящее время большинство производителей в АРМ ПЦН используют статические планы охраняемых объектов в графических форматах (bmp, jpg, jpeg и подобные), то одним из основных требований при модернизации пультового оборудования станет определение соответствующего технического решения, обеспечивающего визуализацию сформированной динамической модели состояния элементов объектового оборудования на планах объектов в онлайн режиме.

Кроме того, перспективой развития данного направления увеличения осведомленности сотрудников подразделений, обеспечивающих безопасность охраняемых с помощью СЦН объектов, представляется возможность доработки программного обеспечения АРМ и сервера ПЦН путем введения в их код интеллектуальных алгоритмов обработки поступающей с охраняемого объекта информации о функционировании средств обнаружения и состоянии каналов связи (ШС). Это позволит на основе анализа поступившей с них информации, данных о типах установленных извещателей, времени их восстановления в дежурный режим и других характеристик, реализовать в дальнейшем функцию прогнозирования действий лиц, осуществивших несанкционированное проникновение на объект, путем формирования раннее неиспользуемых дополнительных извещений, например, о примерном количестве нарушителей, их перемещениях или возможном направлении ухода с охраняемого объекта.

Подводя итог, следует констатировать, что в настоящее время повышение информативности СЦН посредством изменения режима работы объектового оборудования возможно обеспечить в большинстве существующих на рынке охранных услуг систем. Для реализации этого достаточно модернизировать имеющееся программное обеспечение, изменив алгоритм функционирования объектовых приборов, серверов ПЦН и АРМ в режиме тревоги. Это повысит эффективности действий сотрудников дежурных смен и нарядов групп задержания, направленных на охраняемый объект, и позволит повысить информативность СЦН в целом без введения в ее состав дополнительных технических средств охраны.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 52435-2015. Национальный стандарт Российской Федерации. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний. Утвержден и введен в действие приказом Росстандарта от 28 октября 2015 г. № 1659-ст.

2. ГОСТ 31817.1.1-2012 (IEC 60839-1-1:1988). Межгосударственный стандарт. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения, утвержден и введен в действие приказом Росстандарта от 22 ноября 2012 г. № 1034-ст.

3. ГОСТ Р 52650-2006. Национальный стандарт Российской Федерации. Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний. Утвержден и введен в действие Приказом Ростехрегулирования от 27 декабря 2006 г. № 417-ст.

4. ГОСТ Р 50777-2014. Национальный стандарт Российской Федерации. Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний. Утвержден и введен в действие Приказом Росстандарта от 11.11.2014 № 1525-ст.

УДК 654.924.39
ББК 32.99

ВИХИРЕВ АНАТОЛИЙ АЛЕКСАНДРОВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ЗАНИН АЛЕКСЕЙ НИКОЛАЕВИЧ, НАЧАЛЬНИК СЕКТОРА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

НОВЫЕ ВОЗМОЖНОСТИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ОБЪЕКТОВ, ПОДЛЕЖАЩИХ ОБЯЗАТЕЛЬНОЙ ОХРАНЕ ВОЙСКАМИ НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ, НА ОСНОВЕ ПРИМЕНЕНИЯ ПРОГРАММНЫХ ИНТЕГРАЦИОННЫХ ПЛАТФОРМ

Аннотация. В данной статье рассматриваются вопросы повышения уровня антикриминальной и антитеррористической защищённости объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации. Предложено с помощью применения программных интеграционных платформ повысить информативность интегрированных систем безопасности.

Ключевые слова: интегрированная система безопасности, программная интеграционная платформа, охрана объектов.

VIKHIREV ANATOLY ALEXANDROVICH, **RESEARCHER AT THE FEDERAL STATE INSTITUTION "SCIENTIFIC RESEARCH CENTER "PROTECTION" OF ROSGVARDIYA**
ZANIN ALEKSII NIKOLAEVICH, **HEAD OF SECTOR AT THE FEDERAL STATE INSTITUTION "SCIENTIFIC RESEARCH CENTER "PROTECTION" OF ROSGVARDIYA**

NEW OPPORTUNITIES FOR ENSURING THE SECURITY OF FACILITIES OBJECTS TO MANDATORY PROTECTION BY THE TROOPS OF THE NATIONAL GUARD OF THE RUSSIAN FEDERATION, BASED ON THE USE OF SOFTWARE INTEGRATION PLATFORMS

Annotation. The article discusses the issues of increasing the anti-criminal and anti-terrorist security of objects to mandatory protection by the troops of the national guard of the Russian Federation. It is proposed to use software integration platforms to increase the information content of integrated security systems.

Keywords: integrated security system, software integration platform, protected objects.

Постановлением Правительства РФ от 15 мая 2017 г. № 928-р [1] был утвержден Перечень стратегически важных объектов, подлежащих охране силами Росгвардии. В него вошли здания высших судебных и прокурорских органов, а также федеральные музеи, библиотеки и их хранилища. Кроме того, в данный перечень также включены объекты Банка России и ряда других финансовых учреждений, детские оздоровительные и образовательные учреждения, гидротехнические сооружения, объекты топливно-энергетического комплекса (ТЭК) и другие особо важные объекты и объекты критической инфраструктуры.

Охрана данных объектов сопряжена с рядом сложностей: необходимо контролировать большие территории, протяженные периметры, линейные объекты, а также обеспечивать безопасность множества разбросанных объектов. При этом допускается применение нелетальных средств активной защиты [2].

Особую актуальность вопросы организации охраны и антитеррористической защиты приобретают в условиях проведения специальной военной операции и на территориях Луганской и Донецкой народных республик, Херсонской и Запорожской областей.

Для эффективной охраны объектов, учитывая вышеперечисленные особенности, необходимо оснащение современными техническими средствами, способными обнаруживать потенциальные угрозы. Это охранные извещатели, работающие по различным физическим принципам, видеокамеры, тепловизоры, радиолокационные станции и другие системы обнаружения вторжений [3].

В настоящее время широко используются интегрированные системы безопасности (далее – ИСБ), которые объединяют различные источники

информации в единую систему с визуализацией данных на рабочих местах операторов [4].

Современные ИСБ включают не только базовые функции, такие как сигнализация, видеонаблюдение и контроль доступа, но и дополнительные системы. Количество устройств и источников информации о потенциальных угрозах постоянно растет. В связи с этим, обработка поступающих данных и оперативное реагирование на возникающие угрозы требуют значительных ресурсов – как материально-технических, так и людских. Оператор системы безопасности принимает окончательное решение о приоритетах реагирования, однако влияние человеческого фактора может приводить к неоптимальным решениям.

Перспективным решением в такой ситуации видится внедрение алгоритмов искусственного интеллекта – технологии машинной обработки данных, которая предлагает оператору возможные варианты действий. Эта технология реализуется посредством использования в составе систем программных интеграционных платформ (далее – ПИП), также известных как PSIM-системы (Physical security information management) [5].

Основные возможности таких платформ:

сбор данных от различных систем и устройств безопасности;

анализ данных, событий и сигналов для определения приоритетности угроз и исключения ложных срабатываний;

предоставление оператору информации об угрозах в удобном и понятном формате;

предоставление стандартных процедур реагирования, инструкций и инструментов для решения возникающих ситуаций;

отслеживание информации об угрозах и действиях оператора системы безопасности.

Использование ПИП в составе ИСБ обладает рядом неоспоримых достоинств по сравнению с традиционными системами. Ключевым преимуществом выступает полный контроль над техническими средствами каждой системы безопасности. Благодаря консолидации данных со всех подключенных систем, платформа способна проводить комплексный анализ текущей обстановки и предлагать оператору оптимальный план действий. Более того, ПИП используют стандартизированные протоколы взаимодействия, обеспечивающие совместимость с оборудованием различных производителей. Это расширяет возможности для масштабирования систем безопасности и потенциально снижает затраты на их внедрение за счет более широкого использования существующего оборудования [5].

К основным функциям ПИП относятся:

1. Функция фильтрации входящего потока данных для предотвращения создания дублирующийся записей об инцидентах. Все события, связанные с одной и той же ситуацией, объединяются в единый отчет. Это существенно снижает рабочую нагрузку на оператора системы безопасности.

2. Функция создания интерактивных инструкций пошагового реагирования на инциденты. В систему заложены готовые алгоритмы действий. При этом, ПИП обеспечивают возможность проактивной работы, основанной на анализе поступающей информации и прогнозировании развития событий. Такой подход позволяет минимизировать влияние человеческого фактора при принятии решений в критических ситуациях.

3. Функция гибкой цифровой интеграции – объединение различных, как уже существующих, так и планируемых систем, без привязки к оборудованию конкретного поставщика. В отличие от обычных охранных систем видеонаблюдения или систем контроля доступа, использующих проприетарные протоколы, расширение системы с ПИП возможно с помощью устройств от любого производителя, работающих по единому протоколу обмена данными. ПИП способны собирать сигналы от систем безопасности на уровне первичных данных. В ПИП реализован ситуационно-аналитический подход, позволяющий не только оперативно реагировать на произошедшие инциденты, получая и анализируя разнородные данные, но и использовать математические модели для управления факторами, приводящими к возникновению этих инцидентов, посредством обработки больших данных и генерации сценариев поведения и взаимодействия [5].

Для ПИП характерно единообразие в:

системе оповещения и помощи в принятии решений;

структурированной системе тревожных сообщений;

формате регистрации событий от всех систем, обеспечивающих безопасность объекта;

форме уведомлений и постановки задач ответственному лицу;

реализации регламентированных процедур [6].

Программно-аппаратный комплекс, лежащий в основе ПИП, построен по многоуровневой архитектуре и поддерживает иерархию сотрудников, ответственных за принятие решений по различным типам инцидентов. В случае невыполнения задачи назначенным специалистом в установленный срок или в соответствии с регламентом, ответственность за принятие решения переходит на следующий уровень,

но не в форме простой тревоги, а именно как передача ответственности.

Преимущества использования ПИП в составе ИСБ заключаются в значительном повышении удобства работы и наглядности благодаря улучшению осведомленности дежурных операторов системы безопасности объекта, обеспеченному интеллектуальной системой поддержки принятия решений, основанной на внутренних регламентах, базах данных и особенностях развития нештатных ситуаций, упрощению процесса мониторинга, снижению информационного перегруза операторов, автоматическому протоколированию действий операторов и фиксации ответственности за принятые решения.

Таким образом, внедрение ПИП в состав ИСБ открывает широкие перспективы для совершенствования существующих систем безопасности, в том числе для повышения скорости принятия решений при отработке информационных сообщений, поступающих с объектов, охраняемых войсками национальной гвардии Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Об утверждении перечня объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации: распоряжение Правительства Российской Федерации от 15 мая 2017 г. № 928-р // Собрание законодательства Российской Федерации, 2017. – № 21. – С. 3065.
2. Михайлов А.А., Талышев Н.В. Применение в общественных организациях технических средств активной защиты психофизиологического противодействия / Сборник статей ведомственной НПК «Безопасность личности, общества, государства», 30 октября 2024 года, Вып. 1. – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2025. – С. 140-143.
3. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. Р 089-2022 // URL: http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya-chast-2.html (дата обращения – 13.03.2025).
4. ГОСТ Р 57674-2017 Интегрированные системы безопасности. Общие положения : утв. и введен в действие приказом Росстандарта от 19 сентября 2017 г. № 1142-ст. – Москва : Стандартинформ, 2017.
5. Вихирев А.А., Серебряков С.В. Возможности PSIM - систем при организации охраны объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации / – Москва : Информационный бюллетень АТЦ СНГ, 2024. – № 41.– С. 21.
6. Система класса PSIM для управления ситуацией на объекте // URL: https://rtelecom.ru/solutions/psim.php/ (дата обращения – 01.10.2024).

УДК 654.9
ББК 38.482

ЛЯЛЕВИЧ ВИТАЛИЙ ГЕННАДЬЕВИЧ, **НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ**

СЕРЕБРЯКОВ СЕРГЕЙ ВЛАДИМИРОВИЧ, **НАЧАЛЬНИК СЕКТОРА – ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА ОТДЕЛА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ**

ПЕРЕДАЧА ВИДЕОПОДТВЕРЖДЕНИЯ ОТ СИСТЕМ ОХРАННОГО ТЕЛЕВИДЕНИЯ, УСТАНОВЛЕННЫХ НА ОХРАНЯЕМЫХ ОБЪЕКТАХ НА МОБИЛЬНЫЕ УСТРОЙСТВА СВЯЗИ, КАК ОДНО ИЗ НАПРАВЛЕНИЙ ПОВЫШЕНИЯ ИНФОРМАТИВНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ БЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются направления повышения информативности технических систем безопасности при помощи передачи видеоподтверждения от систем охранного телевидения на мобильные устройства связи.

Ключевые слова: системы охранного телевидения, пункт централизованной охраны, мобильные приложения, удаленный доступ, оперативность реагирования, удобство использования.

LYALEVICH VITALY GENNADIEVICH, **RESEARCHER OF FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA**
SEREBRYAKOV SERGEY VLADIMIROVICH, **HEAD OF THE SECTOR – DEPUTY HEAD OF THE DEPARTMENT OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA**

TRANSMISSION OF VIDEO CONFIRMATION FROM SECURITY TELEVISION SYSTEMS, INSTALLED AT PROTECTED FACILITIES TO MOBILE COMMUNICATION DEVICES, AS ONE OF THE WAYS TO INCREASE THE INFORMATION CONTENT OF TECHNICAL SECURITY SYSTEMS

Annotation. The article examines the directions of increasing the information content of technical security systems, using the transmission of video confirmation from security television systems to mobile communication devices.

Keywords: CCTV systems, centralized security point, mobile applications, remote access, response time, ease of use.

В современном мире безопасность объектов, имущества и людей является одной из приоритетных задач государства. Системы охранного телевидения (СОТ) прочно заняли свою нишу среди технических средств безопасности [1] наряду с системами охранной и тревожной сигнализации. Однако с развитием технологий передачи данных и увеличением мобильности пользователей возникает необходимость в более гибких и оперативных решениях. Одним из таких решений является передача видеоподтверждения тревожных извещений от СОТ, установленных на охраняемых объектах, на мобильные устройства сотовой связи пользователей. Этот подход позволяет не только повысить информативность систем безопасности, но и значительно улучшить скорость и качество реагирования на потенциальные угрозы.

Рассмотрим вопрос актуальности передачи видеоподтверждения тревожных извещений на мобильные устройства сотовой связи пользователя. Так, традиционные СОТ передают видеоизображение на стационарные мониторы, расположенные, как правило, в комнате охраны службы безопасности объекта. При этом один сотрудник службы безопасности без ослабления внимания может контролировать не более четырех окон с видеоизображениями. При увеличении на одном мониторе количества окон с видеоизображениями до 8, 16 или даже 32 время реагирования на тревожные ситуации со стороны оператора СОТ резко увеличивается, а качество

и эффективность реагирования значительно снижаются.

В то же время передача только одного тревожного извещения от системы охранной или тревожной сигнализации, установленной на охраняемом объекте, не вполне достаточна для комплексной оценки потенциальной угрозы. Передача видеоподтверждения тревожного извещения на мобильные устройства сотовой связи в дополнение к сигналу «Тревога», поступившему на пульт централизованного наблюдения службы безопасности, позволяет решить вышеуказанные проблемы, предоставляя следующие преимущества:

- мгновенное уведомление пользователя мобильного приложения. Служба безопасности, также, как и собственник охраняемого объекта, получает оповещение на мобильные устройства сотовой связи (смартфон и планшет группы задержания) о возникновении тревожного события в реальном времени, что позволяет более точно произвести оценку угрозы;
- удаленный доступ к системе охранного телевидения. Пользователю мобильного приложения предоставляется возможность просматривать видео с камер в любое время и из любой точки мира посредством информационно-телекоммуникационной сети Интернет, а также, при наличии технической возможности, управлять видеокамерой (PTZ-камера). Современные стандарты сжатия видеоданных, такие как H.264 и H.265, позволяют передавать видеопоток высокого качества при минимальном использовании Интернет-трафика;
- повышение информированности пользователя мобильного приложения. Видеоподтверждение тревожных извещений позволяет собственникам охраняемых объектов и сотрудникам службы безопасности более эффективно управлять силами и средствами реагирования;
- использование функции видеоподтверждения позволит уменьшить количество выездов групп задержания на охраняемый объект по ложным сигналам «Тревога»;
- видеоподтверждение тревожных извещений значительно способствует поимке лиц, подозреваемых в совершении противоправных действий в отношении охраняемого объекта, при проведении правоохранительными органами оперативно-разыскных мероприятий.

Перейдем к технологическим основам передачи видеоподтверждения тревожных извещений. Так как видеоподтверждение тревожных извещений является дополнением к передаче сигнала «Тревога» на пульт централизованного наблюдения от установленных на объекте технических средств охраны (приборы приемно-контрольные, различные средства сбора и обработки информации), то в первую очередь именно ТСО фиксируют нарушение режима охраны объекта. Сопряжение видеокамеры СОТ с техническими средствами охраны, как правило, производится на программном уровне. В автоматизированном рабочем месте оператора службы безопасности указывается локальный IP-адрес видеокамеры, а также осуществляется ее привязка к конкретной охранной зоне. При срабатывании извещателя ТСО автоматически производится передача видеоизображения от привязанной видеокамеры на мобильное устройство сотовой связи пользователя или сотрудника службы безопасности.

Специализированное программное обеспечение для мобильных устройств сотовой связи [1] – мобильные приложения – является неотъемлемой частью обеспечения видеоподтверждения тревожных извещений. Мобильные приложения разрабатываются для различных операционных систем смартфонов и планшетов, что позволяет собственнику объекта использовать функционал видеоподтверждения без дополнительных финансовых затрат. Мобильные приложения имеют возможность работы с архивом видеоданных. Настройка глубины архива производится непосредственно в СОТ. Мобильные приложения позволяют пользователю при необходимости более детально рассматривать отдельные элементы видеоизображения на стоп-кадре.

Мобильные приложения, как правило, имеют интуитивно понятный интерфейс. Однако при внедрении функционала видеоподтверждения тревожных извещений в общую систему безопасности объекта возникают определенные проблемы и вызовы.

В первую очередь на функционал видеоподтверждения тревожных извещений оказывает влияние качество каналов связи (Интернет-соединения). Низкая скорость Интернет-соединения или постоянные сбои в работе Интернет-провайдеров (операторов сотовой связи) могут привести к задержкам в передаче видеопотока от СОТ до мобильного устройства сотовой связи пользователя или сотрудника службы безопасности, а также к частичной потере данных. Особенно актуален данный вопрос при использовании систем радиоэлектронной борьбы.

Во вторую очередь передача видеоданных через информационно-телекоммуникационную сеть Интернет требует использования надежных методов шифрования для обеспечения информационной безопасности.

Еще одним вызовом является высокое энергопотребление мобильного приложения. Длительная передача видеопотока с охраняемого объекта может привести к быстрому разряду аккумуляторной батареи мобильного устройства.

Перейдем к перспективам развития технологии. В будущем можно ожидать дальнейшего совершенствования технологий передачи видеоподтверждения на мобильные устройства сотовой связи. Среди перспективных направлений можно выделить:

- использование сетей операторов сотовой связи стандарта 5G. Это позволит значительно увеличить скорость и объем передаваемых данных с повышением качества видеоизображения;
- более глубокую интеграцию существующих СОТ с техническими средствами охраны на объекте;
- использование видеоаналитики с элементами искусственного интеллекта для анализа видеоизображения и выявления подозрительных событий.

В заключение хочется отметить, что передача видеоподтверждения от систем охранного телевидения на мобильные устройства сотовой связи представляет собой важный шаг в направлении развития технических систем безопасности. Этот подход не только повышает информативность технических средств безопасности, но и оперативность реагирования служб безопасности на различные инциденты. Несмотря на существующие вызовы, такие как зависимость от качества предоставляемых каналов связи и вопросы информационной безопасности, дальнейшее развитие технологий открывает широкие перспективы для совершенствования систем безопасности в целом (интегрированные системы безопасности, PSIM-системы). Внедрение таких решений позволит значительно повысить уровень защищенности объектов и безопасности граждан, а также обеспечить более эффективное управление силами и средствами реагирования служб безопасности в условиях современного мира.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации (Утверждены решением расширенного заседания Технического совета ГУВО Росгвардии (Протокол № 1 от 27 – 30 мая 2024 г.))

УДК 654.949
ББК 32.99

ПАНФИЛОВ АРТЕМ АЛЕКСАНДРОВИЧ, **РУКОВОДИТЕЛЬ СЕКТОРА ТЕСТИРОВАНИЯ АРМ ОБЪЕКТОВЫХ И ЦЕНТРАЛИЗОВАННЫХ СИСТЕМ ПОДРАЗДЕЛЕНИЯ АО «НВП БОЛИД» В ОРЕХОВО-ЗУЕВО**

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МОНИТОРИНГА ОБЪЕКТОВ ЗА СЧЁТ РАСШИРЕНИЯ ВОЗМОЖНОСТЕЙ МОНИТОРИНГОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. Геополитическая и экономическая ситуация в Российской Федерации диктует новые требования к системам мониторинга состояния объектов охраны. Сейчас стандартным функциям охранного и противопожарного мониторинга добавляются задачи контроля состояния охранной сигнализации, видеомониторинг, взаимодействия с инженерными бригадами, группами реагирования, предоставления мобильных и облачных сервисов для абонентов и другие. Для решения подобных задач требуется модернизация применяемых программных и технических средств мониторинга.

Ключевые слова: охраняемый объект, мониторинг, программное обеспечение, автоматизированное рабочее место.

PANFILOV ARTEV ALEXANDROVICH, **HEAD OF THE SECTOR OF TESTING OF WORKPLACES OF OBJECT AND CENTRALIZED SYSTEMS OF THE DIVISION OF JSC «NVP BOLID» IN OREKHOVO-ZUEVO**

INCREASING THE EFFICIENCY OF FACILITY MONITORING BY EXPANDING THE CAPABILITIES OF MONITORING SYSTEMS

Annotation. The article discusses the issues of increasing the anti-criminal and anti-terrorist security of objects to mandatory protection by the troops of the national guard of the Russian Federation. It is proposed to use software integration platforms to increase the information content of integrated security systems.

Keywords: integrated security system, software integration platform, protected objects.

1. Отличия централизованной охраны от объектовой.

Взаимодействие с проектными организациями, заказчиками и специалистами самих мониторинговых центров показывает, что при проектировании, пуско-наладочных работах и обслуживании даже квалифицированные специалисты не учитывают особенности их работы, поскольку не всегда очевидны отличия автоматизированных рабочих мест (далее – АРМ) объектовых от централизованных. К особенностям централизованной охраны можно отнести, например, событийную схему взаимодействия с объектами, которая позволяет подключить тысячи объектов охраны, масштабируемость от входа до объекта охраны целиком, работа с распространёнными протоколами. Контроль каналов связи и схемы резервирования каналов, возможность работы с оборудованием разных производителей, мобильные сервисы для абонентов и различных служб и т.д. В таблице ниже приведены некоторые особенности, присущие объектовым и централизованным АРМ на основе сравнения АРМ «Орион ПРО» и АРМ ПЦО «Эгида-3» [1].

Таблица – Отличия объектового и централизованного АРМов

Объектовые АРМы	Централизованные АРМы
Основная задача Объектового программного обеспечения (далее – ПО) – мониторинг и управление техническими средствами охраны локальных объектов охраны, расположенных непосредственно рядом с рабочим местом	Основная задача АРМ ПЦО Эгида-3 – централизованный мониторинг рассредоточенных на большой территории, разных по объёму, техническому оснащению и статусу объектов охраны

Объектовые АРМы	Централизованные АРМы
оператора или в непосредственной близости от пункта диспетчера	
Локальная охрана одного объекта, работа, в основном по проводным линиям связи, с приборами одного конкретного производителя, непосредственный опрос приборов, полное управление системой сигнализации. Обычно есть ограничение на количество контролируемых элементов на одно рабочее место	Охрана множества объектов, разных по техническому оснащению и сложности (более тысячи на одно рабочее место), до 300 тыс. входов на один сервер. Управление режимами охраны, возможность сброса тревог, управление свободными выходами, запрос параметров входов и других адресных устройств.
Высокие требования к организации локальной сети, достаточно серьёзные ограничения на количество контролируемых элементов сигнализации. Соблюдение требований СП.481 и других нормативных актов по резервированию линий связи.	Использование смешанных каналов связи (чаще беспроводных) и возможность их резервирования и контроля. Передача по локальной сети и узким каналам мобильной сети коротких пакетов. Отдельные функции управления по GSM и проводным линиям связи. Поддержка работы со сторонним оборудованием
Управление СКУД на объекте (включая бюро пропусков, фотоидентификацию и видеофиксацию проходов на территорию охраняемого объекта) и возможность объединения СКД с видеоподсистемой	Ограничения по контролю работы СКУД, отсутствие управления доступом на объект в виду распределенности объектов охраны и специфики централизованной охраны
Полное управление IP видеокамерами или видеорегистраторами (DVR). Интеграция сторонних видеоподсистем, возможность использования сценариев и привязки видео к СКД и ОПС по событиям. Аналитика (распознавание движения, лиц, номеров, предметов, источников огня и т.д.).	Более урезанная по возможностям видеоподсистема, основное назначение которой – видеоверификация тревог. Поддержка протокола FTP. Получение видеофрагментов тревожных записей встроенного детектора IP камер. Получение «живого» видео с объекта, управление до 16 камер, возможность привязки триггеров для управления записью, и охраной
Один канал связи с приборами. Отсутствие схемы резервирования каналов связи. Преимущественное использование проводных подключений.	Система резервирования каналов связи, совмещение нескольких протоколов связи, контроль состояния каждого канала связи, возможность одновременной передачи событий с объекта по нескольким параллельным каналам связи
Нет возможности фильтровать контролируемые элементы по рабочим местам	Возможность распределения объектов по рабочим местам. Перекрёстный или локальный мониторинг. Есть сертифицированное решение для противопожарного мониторинга – ППО КСПИ Эгида. Нет возможности фильтровать контролируемые элементы по рабочим местам

2. Расширение сферы применения ПО для централизованного мониторинга.

Основное назначение подобных программных продуктов – централизованный распределённый мониторинг объектов, реагирование, вызов служб, оповещение абонентов. Однако применение мониторингового ПО часто не ограничивается охранным или пожарным мониторингом объектов, систему применяют организации, осуществляющие обслуживание и сопровождение охранно-пожарной сигнализации на объектах, жилищно-управляющие компании и организации, осуществляющие мониторинг и обслуживание инженерных, телекоммуникационных систем зданий и сооружений. Возможности мобильных приложений также позволяют расширять сферу применения систем мониторинга для контроля передвижных объектов, контроля передвижения граждан, предотвращения терактов (тревожные кнопки) и прочее (см. рис. 1).

Рисунок 1 – Сферы применения ПО для централизованного мониторинга в быту

Современное мониторинговое ПО решает целый ряд задач (см. рис. 2), его можно рассматривать как универсальный набор решений для дежурных операторов и администраторов центра мониторинга, групп быстрого реагирования (далее – ГБР), специалистов по обслуживанию системы сигнализации, абонентов объектов охраны и ответственных лиц. Например, для операторов, ПО должно предоставлять инструменты для наблюдения, и управления объектами охраны – управления режимом охраны, сбросом тревог, управления выходами, сбросом тревожных состояний объекта, взаимодействием с мобильными бригадами, управления режимом записи камер. Встроенный механизм контроля действий оператора должен обеспечить получение данных о недобросовестной работе или о фактах несвоевременного реагирования.

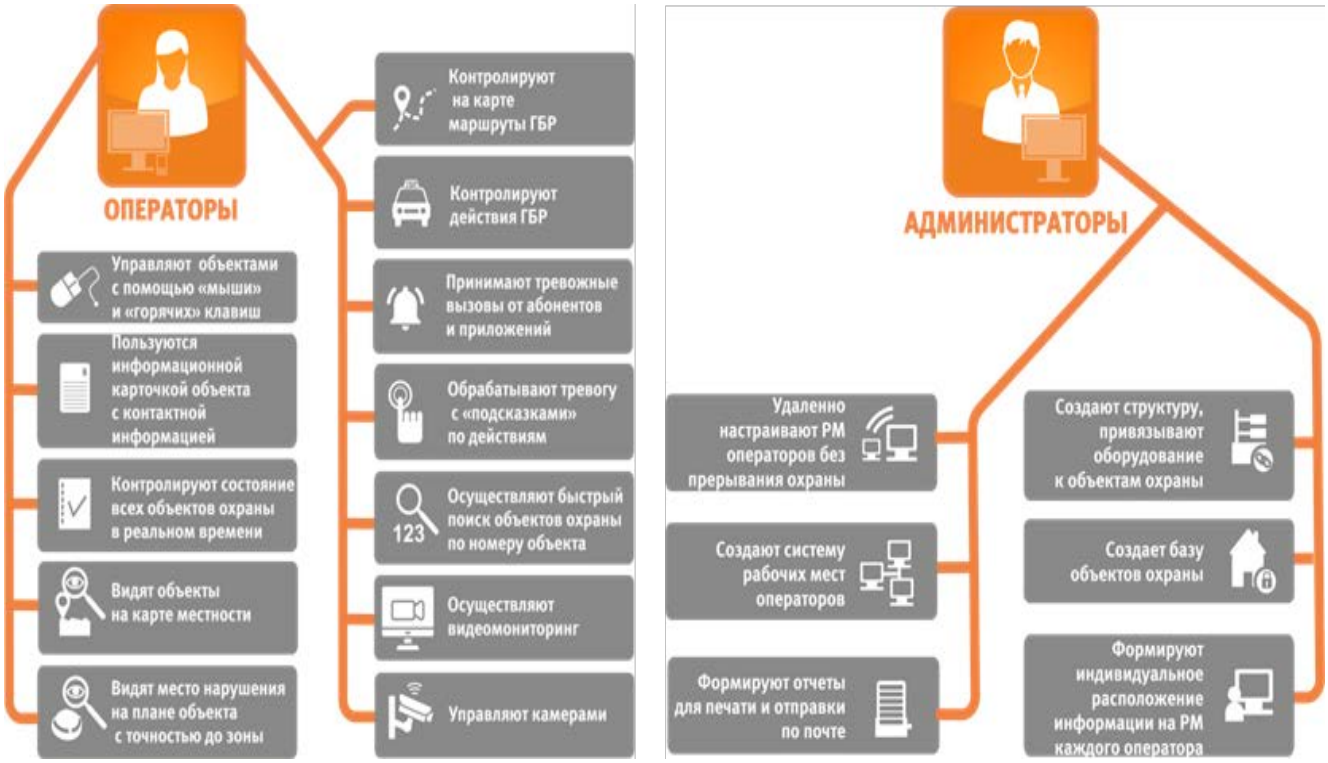

Рисунок 2 – Задачи, решаемые администратором и оператором ПЦО

Для реализации своевременного реагирования, получения максимальной информативности данных по объекту и состоянию каждого его элемента необходимо обеспечить гибкость настройки рабочих мест. АРМ ПЦО «Эгида-3» [2], например, решает вопрос информативности благодаря возможности произвольного размещения на одном или нескольких экранах более 10 графических модулей, которые позволяют оператору одновременно просматривать состояния всех объектов охраны и получать детализированную информацию о состоянии каждого элемента охраны на интерактивной карте местности и плане объекта, взаимодействовать с группами быстрого реагирования, обрабатывать извещения от объектов и абонентов, взаимодействовать с программой через систему диалоговых окон (см. рис. 3 и рис. 4). Каждый модуль может работать независимо друг от друга и при этом дополнять один другого в интерфейсе. Есть возможность вынести модули на отдельные вкладки на одном мониторе, или разнести их по нескольким мониторам. Такая гибкость должна обеспечивать возможность создания рабочего места под любой уровень информативности, разместить интерактивные

элементы так, чтобы они соответствовали принятым нормативам или регламентам. Сетевой режим позволяет организовать отдельные рабочие места для работы с мобильными бригадами, службами эксплуатации и ремонта, вести удалённое администрирование БД объектов.

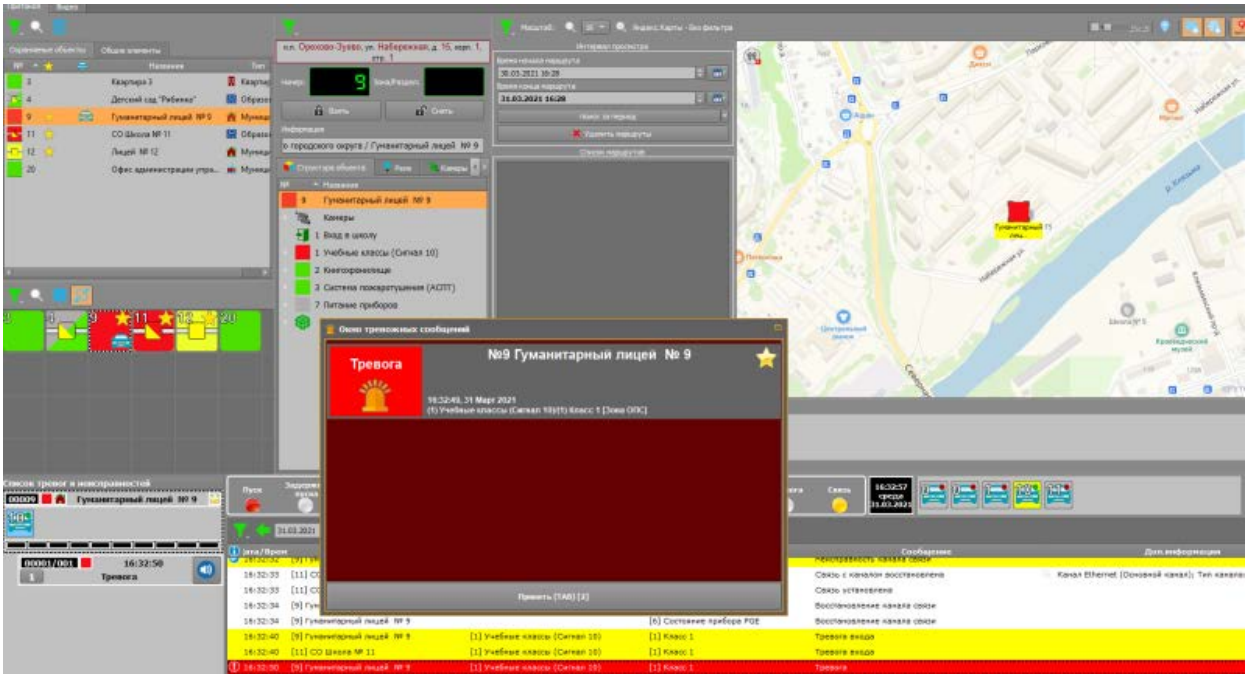

Рисунок 3 – Пример отображения рабочего места оператора АРМ ПЦО Эгида-3

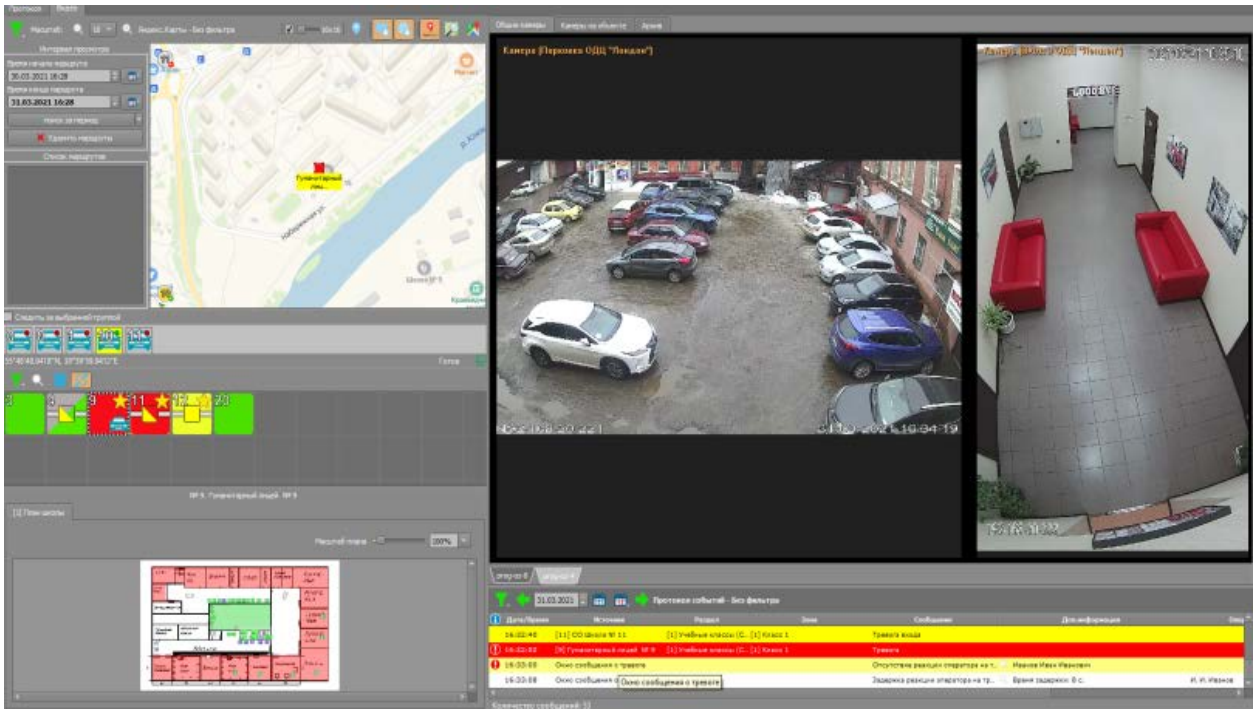

Рисунок 4 – Вариант размещения окна видеомониторинга на одном мониторе с другими элементами интерфейса (АРМ ПЦО «Эгида-3»)

Практика общения с клиентами показывает, что мониторинговое ПО также применяется как средство контроля состояния сигнализации, причём АРМ Инженера имеет определённый список своих решаемых задач. Во-первых, в системе должна быть предусмотрела возможность передачи и отображения диагностических сообщениях о различных неисправностях, отключениях, фактах выхода из строя, необходимости обслуживания и других сообщениях с точностью до контролируемого элемента сигнализации. Во-вторых, должна быть подсистема отчётов

с набором фильтров по неисправностям, служебным и системным событиям. Также в карточке объекта должно быть предусмотрено временное отключение от объекта или его элементов охраны по требованию персонала, абонентов объектов, или при завершении договора на обслуживание. В АРМ ПЦО Эгида-3, например, также предусмотрен режим кроссировки, когда сообщения с систему попадают, но не влияют на состояние объекта. Интересной особенностью Эгиды также является возможность периодического запроса АЦП адресных извещателей по запросу оператора, или по расписанию: уровня влажности и температуры, запылённости и задымлённости камер извещателей. Для источников питания есть возможность контролировать питающее напряжение, выходные значения тока и напряжения, уровень заряда аккумуляторной батареи.

При задействовании функций настройки в ПО пороговых величин различных контролируемых параметров для элементов сигнализации, появляется возможность заблаговременно выявлять участки, где требуется внеплановое обслуживание или ремонт, предотвращать выход оборудования из строя, своевременно реагировать инженерными бригадами (см. рис. 4). Таким образом, использование диагностических данных, сообщений о различных видах неисправностей с точностью до извещателя – это ещё одна из возможностей мониторингового ПО, способствующая повышению информативности данных о состоянии объектов.

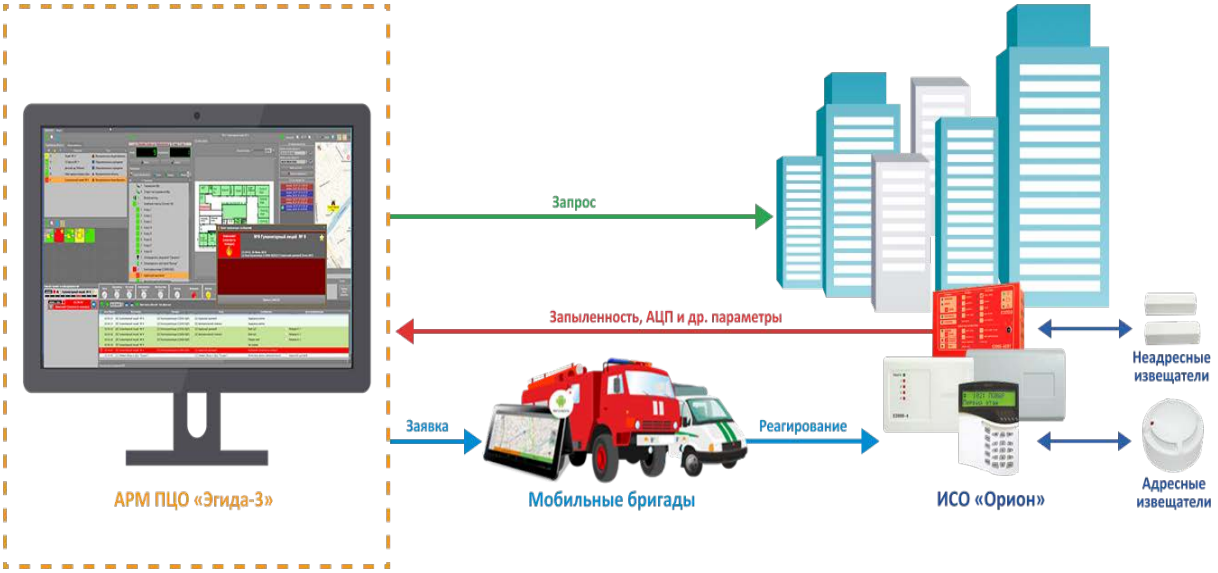

Рисунок 5 – Реагирование бригадами при превышении пороговых значений параметров устройств сигнализации

3.Мобильные сервисы и приложения.

Взаимодействие с абонентами и ответственными лицами контролируемых объектов – важная часть работы мониторинговых и ситуационных центров. С точки зрения повышения информативности, мониторинговое ПО должно иметь сервисы для информирования ответственных лиц о происходящих в системе событиях. Один из применяемых вариантов – это механизм оповещения абонентов по электронной почте с настраиваемым фильтром по событиям и элементам объекта, а также оповещение абонентов по СМС, через промышленные GSM модемы, подключенные к серверу. Помимо собственно оповещения, ПЦО может организовать доступ для абонентов и ответственных лиц через мобильные приложения, такие как Личный кабинет абонента. Тревожная кнопка, АРМ ГБР и др., при наличии возможности подключения сервера к сети Internet. Для абонентов появляется возможность в режиме реального времени отслеживать состояние контролируемых объектов, или совершать тревожные вызовы. Операторы же могут, определив местоположение абонента на ситуационной карте при нажатии, вызвать соответствующие службы или совершить звонок самому абоненту. Мобильное приложение АРМ ГБР тоже довольно часто применяют техники и специалисты по обслуживанию для выезда на объекты по заявкам оператора (см. рис. 5).

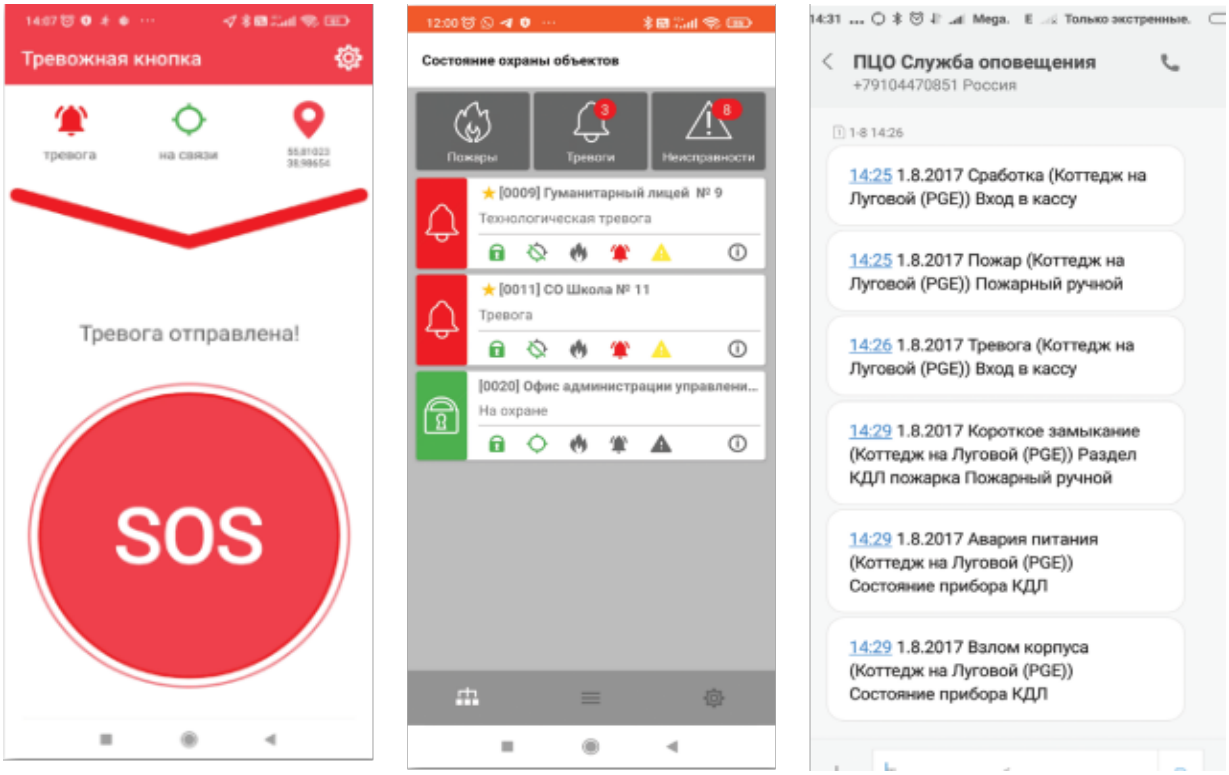

Рисунок 6 – Примеры интерфейсов мобильных приложений для абонентов объектов охраны

4. Интеграционные возможности мониторингового ПО, обеспечение надёжности доставки данных.

Ещё одной полезной опцией мониторингового ПО является возможность мониторинга объектов с установленной охранно-пожарной сигнализацией разных производителей или напрямую, через интеграцию прямого протокола производителя, или путём приёма извещений по совместимым протоколам. Многие производителя позволяют передавать извещения по распространённым протоколам Ademco CID, SurGard, SIA DC-09, PIMA это позволяет подключить к мониторинговому ПО уже существующие объекты без их модернизации и других дополнительных затрат. При этом есть возможность отобразить состояние объекта с точностью до входа ил выхода. Например, АРМ ПЦО «Эгида-3» может одновременно работать с несколькими каналами связи GSM, мобильной сетью Internet, локальной сетью, проводными линиями связи, ГТС и радиоканалом, спутниковой связью. Каждый из каналов связи с каждым объектом контролируется ПО и приборами передачи извещений, комплекс позволяет комбинировать и резервировать каналы связи. Организация контроля каналов связи и возможность подключения приборов разных производителей по прямым или совместимым протоколам – это важная составляющая мониторингового ПО, для повышения эффективности и информативности мониторинга.

Как обеспечить надёжность и безопасность доставки извещений с объекта? Конечно, путём использования резервирования каналов и маршрутов передачи извещений, шифрования протоколов передачи, настройки разграничений доступа к приборам и ПО. И чем важнее объект, тем более сложные схемы приходится применять. Приборы систем передачи извещений, согласно требованиям нормативных актов, должны позволять резервировать и контролировать собственные каналы связи, иметь на бору 2 разъёма для SIM карт и возможность работы с проводными каналами. ПО должно поддерживает возможность отслеживать переход каждого УОО на резервный канал, смену SIM карты. Например, в АРМ ПЦО «Эгида-3», при необходимости, логика, позволяет резервировать передачу не просто по разным каналам с одного устройства, но и через разные приборы передачи извещений, установленные на одном объекте охраны, как показано на рисунке 6.

Последнее время, на особо-охраняемых объектах, в парках крупных корпораций получают распространение особые защищённые варианты приёмных устройств, имеющих комплексное исполнение, представляющие собой, по сути, полноценное место диспетчера. Такие устройства

имею защищённое антивандальное исполнение корпуса, определённые степени защиты от радиочастотных и импульсных помех, имеют повышенную устойчивость к вибронагрузкам, обеспечивают высокую автономность работы при отключении внешнего питания.

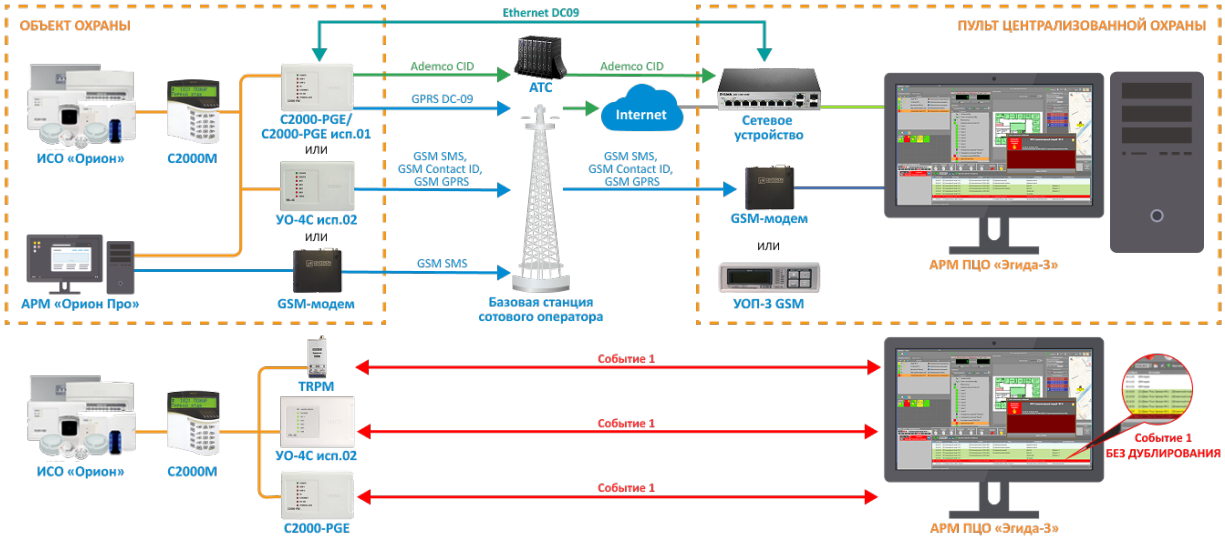

Рисунок 7 – Обобщённая схема взаимодействия с объектами охраны

Примером такого устройства может выступать пультовое устройство для противопожарного мониторинга – ППО КСПИ «Эгида». Прибор позволяет контролировать до 1 тысячи небольших объектов охраны, в него уже встроены все необходимые приёмные модули. Прибор имеет защищённое исполнение корпуса, все компоненты прибора имею повышенную степень защиты от электромагнитных помех, статики, прибор позволяет подключить дополнительные периферийные устройства – монитор, клавиатуру, мышь и т.п. для удобства мониторинга (см. рис. 7). Благодаря двум мощным аккумуляторам обеспечивается автономность работы до 2х суток. Данные приборы применяют также как готовое решение для контроля состояния объектов.

Рисунок 8 – Пример специального исполнения пультового приёмного устройства

5. Видеомониторинг, видеоверификация тревог как часть охранного мониторинга

Собственная видеоподсистема в мониторинговом ПО может применяться как непосредственно, средство визуального контроля состояния объекта, и как средство дополнительной видеоверификации различных тревог и неисправностей на контролируемых объектах. При работе с камерами по протоколу Onvif оператор может, собственно, получить видеопоток с камеры в режиме реального времени для визуального подтверждения происходящего. Полезной опцией в ПО может являться возможность привязки к камерам триггера, например в виде шлейфа, или выхода при получении тревоги с которого, камера включается на запись и передаёт изображение на видеомонитор. Данный способ подключения к камерам, как правило, ограничен в плане задействования общего количества камер в мониторе и на объекте и более требователен к ресурсам.

Распространение также получил вариант работы с камерами по FTP (см. рис. 8). В этом случае, видеоизображение с камер в мониторе получается только по тревоге детектора самих камер. После того, как камера или видеорегистратор сформировал видеоролик, применил алгоритмы сжатия и передал его на ПЦО, оператор видит только тревожно событие от конкретной камеры, но может посмотреть видеофрагмент в плеере монитора с целью подтверждения тревожной ситуации на объекте (см. рис. 9). Такой вариант взаимодействия с камерами позволяет подключать на ПЦО практически любое количество камер, при этом нет жёстких требований к качествам каналов связи и их пропускной способности.

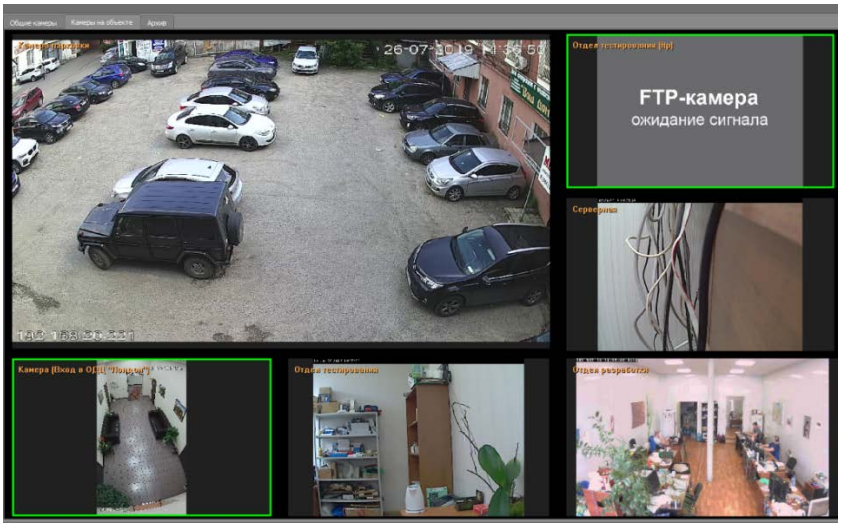

Рисунок 9 – Пример работы элементов видеоподсистемы на рабочем месте

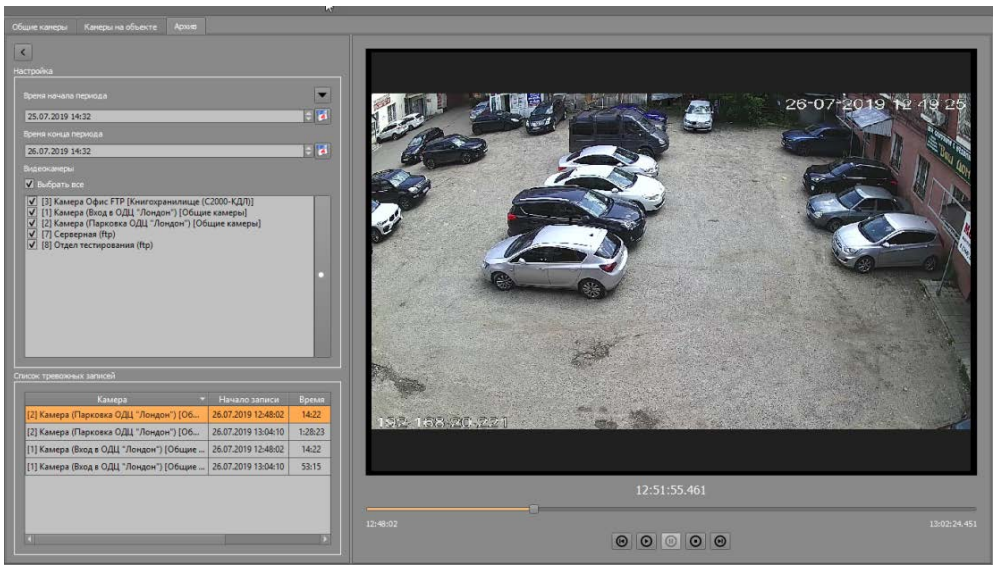

Рисунок 10 – Пример просмотра видеофрагмента в видеоподсистеме

6. Заключение.

Год от года к системам передачи извещений и системам мониторинга растут требования в плане надёжности, быстроты и точности доставки сообщений, информативности передаваемых и отображаемых данных, безопасности, обеспечения возможности однозначно адекватно оценить ситуацию и определить место инцидента. Мониторинг уже давно перестал быть просто средством реагирования, он решает всё более сложные и интересные задачи. Задача разработчиков мониторингового программного обеспечения - идти в ногу со временем и следить за постоянно меняющейся ситуацией и делать продукт, который был бы востребован всеми участниками процесса мониторинга безопасности объектов, транспорта и граждан.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Портал АО «НВП Болид» // [Электронный ресурс]. 12.03.2025. – URL: https://bolid.ru/projects/csntralized-security/characteristics/ (дата обращения 12.03.2025).
2. Комплекс пультовой охраны «Эгида-3». – М: АО «НВП Болид» Выпуск 9. 2024. – 54 с.