АЛГОРИТМ
безопасности

№3, 2019

БЕЗОПАСНОСТЬ МАЛЫХ И СРЕДНИХ ОБЪЕКТОВ ТОРГОВЛИ И УСЛУГ

ОХРАННЫЙ МОНИТОРИНГ МАГАЗИНОВ

РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ШКОЛ

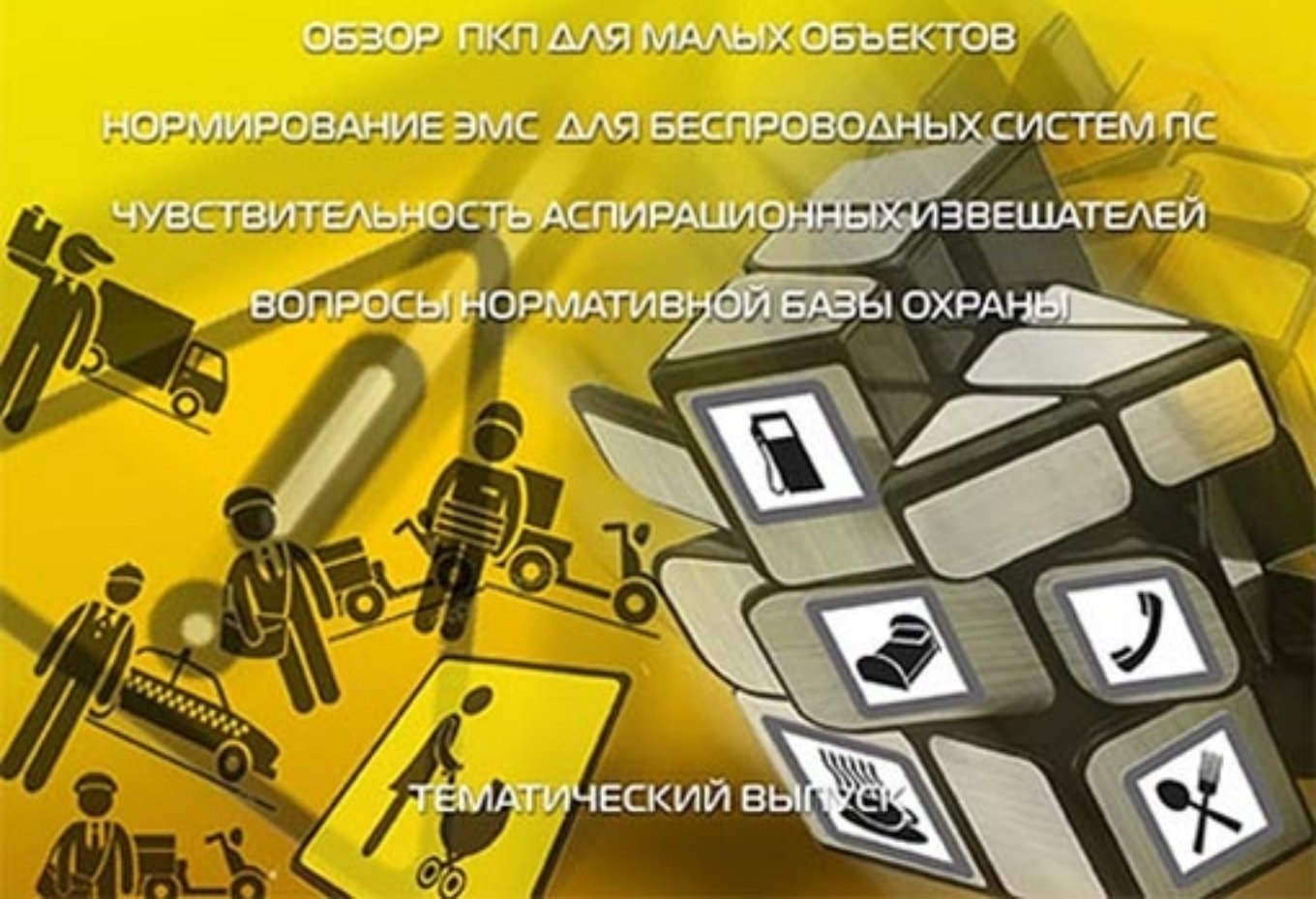
ПОЖАРНАЯ БЕЗОПАСНОСТЬ ДЕТСКИХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

ОБЗОР ПКП ДЛЯ МАЛЫХ ОБЪЕКТОВ

НОРМИРОВАНИЕ ЭМС ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ ПС

ЧУВСТВИТЕЛЬНОСТЬ АСПИРАЦИОННЫХ ИЗВЕЩАТЕЛЕЙ

ВОПРОСЫ НОРМАТИВНОЙ БАЗЫ ОХРАНЫ



ТЕМАТИЧЕСКИЙ ВЫПУСК

БЕЗОПАСНОСТЬ МАЛЫХ И СРЕДНИХ ОБЪЕКТОВ ТОРГОВЛИ И УСЛУГ: КОМПЛЕКСНЫЙ ПОДХОД

Брединский Анатолий Геннадьевич
основатель и руководитель проекта «Безопасность для всех» (www.sec4all.net), ст. преподаватель кафедры «Защита, охрана и безопасность» ГУФКиС РМ

КОМПЛЕКСНЫЕ СИСТЕМЫ

С проблемой криминальных посягательств на учреждения торговли и сферы обслуживания сталкиваются практически все владельцы бизнеса.

Однако если крупные предприятия, расположенные преимущественно в больших городах, в той или иной мере озабочены проблемой собственной безопасности и решают ее в зависимости от своих возможностей, то для небольших магазинов, салонов, ломбардов, заправочных станций и других объектов, расположенных на периферии, эта проблема стоит наиболее остро. Характерно, что владельцы подобных учреждений часто весьма легкомысленно относятся к обеспечению безопасности своего бизнеса. Среди них бытует заблуждение, что малые объемы и удаленное расположение сами по себе являются надежной гарантией от посягательств правонарушителей. На самом же деле это не так.

Можно в очередной раз напомнить, что на каждую жертву обязательно найдется свой преступник и что многих как раз привлекают такие предприятия, так как в них нередко накапливаются серьезные денежные суммы или хранятся значительные материальные ценности. При этом их защита весьма условна или отсутствует вовсе. Кроме этого, подобные объекты часто становятся объектом посягательств со стороны социально опустившихся местных жителей – алкоголиков, наркоманов, лиц без определенного места жительства, начинающих малолетних преступников, которые при этом могут вести себя цинично и агрессивно.

Излишне напоминать, что в некоторых регионах уровень преступности в разы выше, чем в городах, а раскрываемость преступлений, к сожалению, оставляет желать лучшего.

Можно ли этому что-либо противопоставить и как защитить свой бизнес – об этом мы поговорим в рамках данной статьи.

С ЧЕГО НАЧИНАЕТСЯ ПРЕСТУПЛЕНИЕ?

Далеко не каждый владелец бизнеса задумывается, что значительная часть хищений имущества совершается не спонтанно. Ей предшествует этап подготовки, в ходе которого злоумышленники выбирают себе потенциальную жертву путем сбора необходимой информации об объеме и времени скопления денежной выручки, наличию и расположению материальных ценностей, графике работы того или иного объекта, системе его защиты и охраны, уязвимых местах и т.п. Иногда в качестве источника информации выступают работники предприятия, которые могут быть как соучастниками преступника, так и просто снабжать злоумышленника информацией, не задумываясь о возможных последствиях.

Даже молодые, только начинающие свою криминальную «карьеру» преступники практически никогда не выбирают для кражи (и тем более – разбоя) не знакомые им предприятия. Как и хищник, преступник предпочитает выбирать наиболее уязвимую и слабозащищенную жертву, нападение на которую позволит достигнуть положительного результата с наибольшей вероятностью.

Этот этап наиболее важен, так как обнаружение признаков подготовки преступления, а также противодействие им, позволит избежать возможных негативных последствий. Существуют определенные, наиболее типичные признаки того, что преступники проявляют интерес к конкретному объекту торговли и услуг. Отметим следующие:

- Периодическое появление вблизи объекта посторонних лиц, в том числе из местных жителей, без явной цели, но с проявлением видимого интереса к режиму работы объекта. В некоторых случаях оно может сопровождаться фотографированием или видеосъемкой, как маскируемой, так и явной. В отдельных случаях подобные действия могут производиться из припаркованных автомобилей.
- Внезапно участившиеся визиты лиц, не являющихся постоянными или давними клиентами, которые под различными предлогами задерживаются на объекте. В некоторых случаях они пытаются получить интересующую их информацию в ходе различных бесед с персоналом.

- Проявление чрезмерного интереса к режиму работы, системе безопасности, объемам и месту хранения денег и материальных ценностей со стороны обслуживающего персонала, особенно если они были недавно приняты на работу, либо со стороны лиц, осуществляющих временные работы (монтаж, уборка, ремонт, погрузочно-разгрузочные работы).
- Попытки проникнуть в служебные помещения, особенно в места хранения материальных ценностей со стороны посетителей или иных лиц, которые объясняются ошибками («Ошибся дверью», «Я в бухгалтерию», «Ищу туалет»).
- Неудачные попытки проникновения на охраняемый объект путем подбора ключей, попыток взлома дверей, окон или иными способами.
- Участившиеся перебои в работе технических средств охраны, которые могут быть результатом действия преступников.
- Увеличившееся число тревожных сигналов охранной сигнализации. Зачастую преступники намеренно провоцируют срабатывание сигнализации для выявления скорости реакции и тактики действий охраны.
- Проявление необоснованного повышенного интереса к работе предприятия со стороны работников, особенно из числа недавно принятых.
- Резкое изменение поведения работников (например, участившиеся задержки на работе, увеличившиеся личные траты, злоупотребление спиртными напитками и т.п.).

Естественно, этот перечень не является исчерпывающим и требует постоянного и серьезного внимания к тому, что происходит на предприятии. Именно своевременное выявление признаков подготовки преступления позволит успешно его избежать.

КАДРЫ РЕШАЮТ ВСЕ!

В связи с этим, одной из важных задач сотрудников охраны предприятия, а при их отсутствии – персонала, является постоянное наблюдение за окружающей обстановкой и выявление подозрительных случаев. Администрации объекта следует проводить периодические инструктажи с персоналом, напоминать им о необходимости быть бдительными, доводить до их сведения информацию о возможных подозрительных действиях. К сожалению, практика показывает, что к подобной системе большинство относится чисто формально.

Большое распространение получили попытки возложения собственником предприятия ответственности за любую утрату или порчу имущества, в том числе являющиеся результатом преступных действий, – на подчиненных. В случае совершения кражи или разбойного нападения от работников требуют возместить причиненный ущерб. Некоторые бизнесмены даже считают, что именно такие действия заставят персонал более серьезно относиться к защите имущества предприятия, так как фактически они будут предотвращать собственные материальные потери.

Однако подобное следует признать порочным. Во-первых, в большинстве случаев эти действия являются противозаконными, и в случае их выявления собственник может быть привлечен к ответственности. Во-вторых, это крайне негативно влияет на лояльность персонала. Работники, поставленные в подобные условия, могут совершать хищения посредством краж и мошеннических действий, дабы компенсировать потери, которые были на них возложены.

Кроме того, это провоцирует формирование атмосферы недоверия, конфликтов в коллективе, недобросовестного исполнения служебных обязанностей и, в том числе, постоянную смену кадров, в результате которой предприятие теряет подготовленные ценные ресурсы.

Как минимум наивным следует признать довольно распространенное убеждение собственника, который ожидает, что персонал проявит героизм и будет рисковать своей жизнью и здоровьем, пытаясь защитить имущество предприятия от преступных посягательств. И речь даже не о надуманных обязанностях, большинство работников, будучи не готово к критической ситуации, не зная, как себя вести, просто не способно к адекватной реакции.

Решение подобных вопросов может производиться только в виде системного подхода, в ходе которого формируется дружеский коллектив с четко разделенными служебными обязанностями и системой поощрений и наказаний. Персонал должен уяснить, что любое преступное посягательство – это угроза не только имуществу собственника, но и непосредственно их здоровью и, возможно, жизни. А любые материальные потери также негативно повлияют на них, так как не будет возможности выплачивать премии, повышенные оклады, а в некоторых случаях, даже зарплату.

Поэтому очень многое зависит от бдительности сотрудников. Для начала необходимо разработать должностные инструкции с алгоритмом действий в критической ситуации. Для создания подобных инструкций целесообразно привлечь специалистов, имеющих практические знания и опыт в данной сфере. После того, как соответствующие инструкции будут разработаны и утверждены приказом руководителя предприятия, сотрудники проходят инструктаж и знакомятся с ними под роспись. Крайне важно не превращать подобное в пустую формальность.

В результате такого инструктажа и изучения инструкций работники предприятия должны четко знать:

- признаки потенциальных угроз и подготовки преступных действий в отношении предприятия;
- какие действия им следует предпринимать, если они обнаружили подозрительное поведение;
- к кому, когда и как следует обратиться с этой информацией;
- какие средства охраны установлены на объекте и как с ними взаимодействовать;
- как себя правильно вести в различных критических ситуациях;
- какая ответственность и в каком объеме ложится на них в случае кражи, грабежа или разбоя в отношении предприятия;
- в чем заключается система поощрений и наказаний за несоблюдение подобных инструкций.

Разъясняя персоналу тактику, следует довести до них идею о том, что не существует универсальных рецептов и каждый конкретный случай требует своего решения. Так, в целом ряде случаев смелые и решительные действия персонала позволяли предотвратить разбойные, в том числе вооруженные, нападения на предприятие. Но в то же время есть примеры, когда попытки оказания сопротивления нападающему приводили к причинению тяжкого вреда здоровью или смерти работников. Практика показывает, что неготовность к подобным ситуациям, отсутствие знаний о том, как необходимо действовать, страх перед возможными последствиями, в том числе наказания со стороны руководителя, в критической ситуации может провоцировать у работника панику и неадекватные поступки, которые лишь ухудшают ситуацию.

После закрепления теоретического материала необходимо провести практическую отработку. Ее целесообразно реализовывать в виде ролевых ситуаций с различными сценариями (кража, разбой, хулиганство, мошенничество и т.п.), в ходе которых участники не рассказывают о том, как они будут действовать, а на деле демонстрируют алгоритм в заданных условиях. В ходе таких «учений» можно быстро выявлять ошибочные действия и сразу давать рекомендации о том, как следует поступить. Сценарии могут повторяться с введением дополнительных усложняющих условий или иметь различные варианты развития событий, в зависимости от действий персонала.

Идеально, когда подобные действия проводятся в максимально приближенной к реальности обстановке, но при этом формируется положительная «живая» соревновательная атмосфера. Работников, которые проявили себя с лучшей стороны, следует публично выделить и поощрить, в том числе, материально.

ЗАЩИТА – В КОМПЛЕКСЕ

Естественно, работа с персоналом является не единственным элементом защиты. Владельцу не следует забывать об оборудовании на объекте инженерных средств защиты, установке технических средств охраны, системы видеонаблюдения и контроле доступа, противокражных системах и постах физической охраны. Все эти элементы формируют единое целое, дополняя друг друга.

ИНЖЕНЕРНЫЕ СРЕДСТВА ЗАЩИТЫ

Инженерные средства защиты представляют собой элементы конструкции или интерьера, целью которых является затруднение преступного посягательства на материальные ценности. К подобным средствам относятся строительные элементы (укрепленные конструкции, в том числе стены, полы и потолки), защитные двери и окна, решетки, роллеты, турникеты, шлагбаумы, сейфы, защитные шкафы и т.п.

К сожалению, многие объекты торговли не уделяют особого внимания этим средствам защиты. Даже в тех случаях, когда существуют рекомендуемые или даже обязательные требования к укрепленности объекта, они соблюдаются далеко не всегда. Зачастую торговые точки и учреждения сферы услуг размещаются в изначально не предназначенных для этого помещениях, при этом отсутствует время да и желание собственника что-либо менять.

Есть примеры, когда после переезда в помещение новых владельцев, предыдущие, зная уязвимые места, могли легко проникнуть на объект. В отдельных случаях для этого использовались ключи от замков, которые никто не посчитал нужным сменить. Именно поэтому перед открытием объекта производятся необходимые действия по оборудованию его необходимыми средствами инженерной защиты. Входные двери, особенно ведущие в торговые залы, складские и кассовые помещения устанавливаются с учетом максимальной взломостойкости. Если это возможно, их целесообразно установить в виде шлюза, одна за другой, таким образом, чтобы при вскрытии одной злоумышленник не имел свободного доступа и вынужден был заниматься взломом второй в условиях ограниченного пространства.

Окна оборудуются защитными роллетами или ставнями, которые препятствуют проникновению преступников и служат для защиты от повреждений, в том числе в результате действий природы (град, ураган). Весьма распространенная практика установки на окна решеток далеко не всегда эффективна, так как решетки устанавливаются с внешней стороны окна, что позволяет преступникам беспрепятственно производить с ними манипуляции (например, выдернуть их, зацепив тросом, прикрепленным к автомобилю). Кроме этого, в случае пожара, аварии или стихийного бедствия, решетки блокируют окна, не позволяя покинуть помещение. Более эффективным является установка внутренних раздвижных решеток или иных защитных элементов, взаимодействие с которыми невозможно без вскрытия окна.

Особое внимание следует уделить защите помещений, где хранятся денежные средства и материальные ценности. Располагать подобные помещения следует внутри объекта, желательно там, где нет внешних стен, выходящих на улицу или смежных с соседними помещениями, не принадлежащими собственнику. Материальные ценности, с которыми не осуществляется постоянные операции, а также не находящиеся без постоянного контроля, в обязательном порядке помещаются в защищенные шкафы или сейфы. Эта же процедура проделывается при покидании магазина персоналом, даже если оно краткосрочно (ночное время, выходные и праздничные дни, обед и т.п.).

В последние годы участились кражи, совершаемые группой лиц, нередко подростков. Вскрыв двери или разбив витрину, преступники быстро похищают товары, находящиеся в открытом доступе, и скрываются до приезда полиции или группы быстрого реагирования. За счет участия нескольких (иногда до 10) лиц, такие действия могут причинить значительный ущерб. В связи с этим, рекомендуется не оставлять ценные предметы вблизи к внешним окнам и дверям, укреплять внешние витрины защитными элементами (например, специальной защитной пленкой), крепить товары к стойкам и витринам или выставлять вместо них муляжи.

ОХРАННАЯ СИГНАЛИЗАЦИЯ

Оборудование объектов торговли и сферы услуг охраной сигнализацией является обязательной мерой. В ряде стран помещения, не оснащенные подобными системами, не подлежат страхованию, так как считается, что собственник не предпринял действия для сохранения своего имущества.

При оборудовании помещения охранной сигнализацией не следует экономить, так как наличие уязвимых мест и слепых зон в охране значительно снижает защищенность объекта. Целесообразно использование комбинированных извещателей охранной сигнализации, которые препятствуют их нейтрализации опытными преступниками. Установленная система охранной сигнализации подлежит постоянному контролю и проверке ее работоспособности. При необходимости осуществляется ее модернизация современными средствами. Особо внимательным к системе охранной сигнализации следует быть при проведении строительных и ремонтных работ на объекте. Нередко в ходе таких работ нарушается функциональность охранной сигнализации, появляются новые помещения, которые не оборудованы охранными средствами. Иногда собственники самостоятельно деактивируют сигнализацию на время проведения работ, чем могут воспользоваться преступники. Также не стоит забывать, что участившиеся сигналы тревоги или перебои в работе охранной сигнализации могут быть вызваны действиями преступников, которые таким образом добиваются снижения внимания или даже отключения охранной сигнализации.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Одними из самых распространенных технических средств безопасности, устанавливаемых на объектах малого и среднего бизнеса, являются камеры видеонаблюдения. И хотя эксперты утверждают, что системы видеонаблюдения предотвращают не более 10% криминальных посягательств, именно их собственники наиболее охотно устанавливают в своих торговых и сервисных залах.

Безусловно, польза от подобных систем есть. Во-первых, наличие видеонаблюдения на объекте, в тех случаях, когда осуществляется его мониторинг, позволяет выявить подозрительное поведение на этапе подготовки преступления. Во-вторых, в случае совершения нападения, будут получены ценные кадры происходящего, которые позволят точно понять, как именно действовали преступники. В ряде случаев именно с помощью записей систем видеонаблюдения удается получить изображения преступников, что даст возможность их идентифицировать и привлечь к ответственности. Даже если злоумышленники используют различные маскирующие внешность средства (маски, капюшоны и т.п.), видеозапись позволит эксперту получить ценную информацию о примерном росте, телосложении, ориентировочном возрасте преступников. А в некоторых случаях – их особые приметы или информацию об особенностях поведения (хромота, характерные жесты, действия, свидетельствующие о наличии преступного опыта и т.п.).

Однако следует упомянуть, что крайне часто владельцы бизнеса совершают типичные ошибки, не обладая достаточной компетенцией, но при этом активно желая сэкономить свои средства. Среди наиболее распространенных ошибок:

- выбор бюджетных камер от малоизвестных производителей;
- приобретение или использование давно устаревшего оборудования, не соответствующего современным требованиям;
- использование некачественного программного обеспечения;
- установка видеонаблюдения таким образом, чтобы оно, в основном, следило

за сотрудниками, в результате, при криминальных посягательствах такие камеры становятся малоэффективными.

Также следует упомянуть о весьма распространенной проблеме с организацией хранения видеоархива. Нередко он ведется бессистемно, не осуществляется должного контроля наличия записей и их хранения. Встречаются ситуации, когда запись вовсе не ведется в результате сбоев в работе регистратора или заполнения носителей информации. А владелец бизнеса узнает об этом лишь после совершения преступления, когда выясняется, что никаких записей нет.

Соответственно, чтобы видеонаблюдение стало эффективным элементом системы безопасности, требуется серьезный подход к выбору таких систем, их установке и обслуживанию. Необходимо внедрить современные программные средства видеоаналитики, которые значительно упрощают работу оператору. Не менее важно грамотно подобрать тип камер и правильно установить их на объекте, без «слепых зон». И, конечно, необходимо организовать хранение и архивацию видеоданных.

В некоторых случаях, на этапе подготовки преступления злоумышленники могут попытаться вывести камеры из строя (например, распылить на объектив лак или краску), изменить угол обзора камеры или предпринять какие-то другие действия. Данные факты должны быть своевременно выявлены операторами, и предприняты необходимые меры защиты.

Отдельного внимания заслуживает вопрос о соблюдении при видеонаблюдении нормативных положений о защите персональных данных, которым в последнее время уделяется все большее внимание.

КОНТРОЛЬ ДОСТУПА

К сожалению, система контроля и управления доступом (СКУД) не пользуется большой популярностью на средних и малых объектах торговли и услуг, особенно расположенных на периферии. Владельцы бизнеса предпочитают на этом экономить. На самом деле, это большая ошибка. Помимо вспомогательных функций по контролю за персоналом (время прихода и ухода с работы, контроль за опозданиями и перемещениями в течение рабочего дня) такие системы позволяют предотвратить незаконное проникновение в служебные помещения, в том числе, с целью кражи.

Практика показывает, что нередки случаи, когда преступники в течение рабочего дня свободно проникают в служебные помещения, пользуясь отсутствием должного контроля со стороны работников, где похищают денежные средства и материальные ценности, в том числе принадлежащие сотрудникам.

Иногда такие хищения совершаются и самими работниками, которые, обнаружив в открытых помещениях ценности, предпочитают их присвоить, оставаясь безнаказанными. Поэтому наряду с иными техническими средствами, такими как охранная сигнализация и видеонаблюдение, целесообразна установка систем контроля доступа, особенно в тех помещениях, где хранятся значительные материальные ценности или конфиденциальная информация предприятия.

ПРОТИВОКРАЖНЫЕ СИСТЕМЫ

К сожалению, количество хищений из торговых залов постоянно растет и принимает масштабы эпидемии. Среди молодых людей даже стал популярным шоплифтинг (от англ. shop – магазин и lift – поднимать, тягать), т.е. кражи, совершаемые зачастую не из корыстных, а скорее из хулиганских побуждений, «на спор», чтобы хвастаться этим перед знакомыми.

Подобные действия способны наносить огромный ущерб розничной торговле, при этом, ни наличие видеонаблюдения, ни охранники в торговом зале или персонал не способны полноценно противостоять. Одним из решений подобных ситуаций выступают противокражные системы, которые позволяют обнаруживать попытки выноса товаров, оснащенных специальными радиочастотными метками без оплаты на кассе. Естественно, что подобные системы не являются абсолютной гарантией от кражи, однако способны значительно снизить число хищений и, потенциально, заставить злоумышленников отказаться от своих планов.

ХИМИЧЕСКИЕ ЛОВУШКИ, МАРКИРОВОЧНЫЕ СРЕДСТВА

К сожалению, химические ловушки и маркировочные средства не являются распространенными элементами защиты. Большинство владельцев бизнеса даже не имеют о них элементарных представлений.

Вместе с тем, химическая ловушка – это оснащенные или обработанные специальными химическими веществами (красящими, люминесцирующими или запаховыми) приспособления или устройства, которые могут быть закамуфлированы под различные предметы (денежная пачка, образец товара, материальная ценность). Их также могут устанавливать в местах хранения ценностей (касса, сейф, склад), чтобы при попытке кражи ловушка срабатывала. В результате взаимодействия с такими средствами происходит окрашивание или маркировка похищенного либо непосредственно преступника специальными веществами, которые позволяют их дальнейшее обнаружение. Например, специальные вещества из химической ловушки способны окрасить злоумышленника ярким, хорошо заметным цветом, крайне устойчивым к попыткам его удалить. При наличии у правоохранительных органов образцов краски или маркирующего вещества дальнейшее обнаружение преступника или похищенного значительно упрощается. Однако не следует в этом вопросе прибегать к кустарным, самодельным устройствам, так как одним из требований к химическим ловушкам является их абсолютная безопасность для человека. Также следует помнить, что подобные средства не способны работать по принципу «свой/чужой», т.е. могут сработать и в отношении работника предприятия, клиента или иного лица, которое не было предупреждено или забыло об их наличии.

АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ

Большинство из вышеперечисленных технических средств охраны по своей сути являются пассивными. Т.е. они способны лишь обнаруживать тревожное событие или фиксировать произошедшее, непосредственные же действия должны предприниматься человеком. Однако опыт показывает, что в случае разбойных нападений или тщательно подготовленных краж их может быть не достаточно. В связи с этим получили распространение системы активной защиты, одной из которых являются генераторы тумана. Это специальные устройства, которые по ручному или автоматическому сигналу тревоги способны быстро заполнять замкнутые помещения непрозрачным туманом. В результате злоумышленник теряет ориентацию в пространстве и не способен завершить свои преступные намерения. Практика применения таких систем показывает, что чаще всего преступники предпочитают ретироваться в первые же секунды после срабатывания такой системы. При этом вещества, формирующие непрозрачный туман, не пачкают и не повреждают товары, они безвредны для человека. Подобные системы могут быть эффективны при разбойных нападениях, когда оказание сопротивления вооруженным преступникам может вызвать агрессию с их стороны и нанесение телесных повреждений сотрудникам охраны или персоналу.

ВЫВОДЫ

Подводя итоги, мы приходим к выводу, что легкомысленное отношение к защите своего бизнеса и желание сэкономить на безопасности приводит к печальным последствиям. Материальный ущерб даже от одной кражи, грабежа или разбоя способен превысить затраты на обеспечение безопасности. Поэтому к данному вопросу важно отнестись серьезно, применяя комбинированный комплексный подход и доверяя решение специалистам. Ведь стабильность и спокойствие, особенно, если они не ложные, – крайне важны для успеха бизнеса.

AJAX SYSTEMS РАЗВИВАЕТ РЫНОК БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Система безопасности компании Ajax Systems выделяется на фоне другого профессионального охранного оборудования простотой установки и легкостью использования. От этого выигрывают не только пользователи, но и профессионалы индустрии: инсталляторы и охранные компании. Сервис занимает часы, а не дни (и может осуществляться дистанционно), преимущества и возможности оборудования легко донести клиенту.

Результаты Ajax Systems показательны – более 200 000 клиентов в 80 странах мира защитили свои дома, квартиры и офисы техникой Ajax. Эти системы подключают на пульт централизованного наблюдения (ПЦН) более 700 охранных компаний, в том числе и 26 российских.

АРХИТЕКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ AJAX

В экосистеме Ajax можно выделить 2 структурных модуля: центр управления и устройства реагирования. Модули связаны двусторонними протоколами радиосвязи, их слаженная работа обеспечивается разработанным Ajax Systems программным обеспечением. Рассмотрим систему безопасности Ajax более детально.

ЦЕНТР УПРАВЛЕНИЯ

Хаб – централь системы безопасности Ajax. Она контролирует работу датчиков и устройств системы, принимает команды и передает сигналы тревог, используя Push-нотификации, SMS и звонки.

Централь связывается с датчиками на расстоянии до 2000 м по запатентованному радиопротоколу Jeweller с AES шифрованием и радиочастотным хоппингом. При помощи ретранслятора сигнала ReX зона покрытия радиосети Ajax увеличивается до 16 км² – для охраны больших объектов.

Централь управляется с помощью приложений Ajax Security System и Ajax PRO: Tools for Engineers, а также брелоков SpaceControl и клавиатур KeyPad.

Хаб работает под управлением операционной системы реального времени OS Malevich от Ajax Systems. Она защищена от вирусов и кибератак, снабжена страхующими каждый критичный процесс подсистемами и обновляется без участия пользователя и обслуживающей компании.

Удаленное управление системой безопасности осуществляется через облачный сервис Ajax Cloud. Он за доли секунды передает команды, владеет актуальной информацией о состоянии каждого устройства и благодаря постоянным пингам сервера уже через 1 минуту знает про изоляцию объекта.

БЕСПРОВОДНЫЕ УСТРОЙСТВА И ДАТЧИКИ

Ajax Systems имеет большой арсенал беспроводных датчиков для мгновенного определения открытия дверей и окон, разбития стекла, движения в помещениях, дыма, угарного газа и роста температуры, а также протечек воды. Отдельная линейка обеспечивает безопасность придомовых участков. Датчики Ajax имеют режим игнорирования животных, функцию самодиагностики и работают до 7 лет от предустановленных батарей.

САМЫЙ ВЫСОКИЙ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ УРОВЕНЬ НАДЕЖНОСТИ

Устройства Ajax соответствуют требованиям международного стандарта EN 50131-1:2006. Они прошли тестирование в

независимых аккредитованных лабораториях и получили самый высокий для беспроводных систем второй уровень надежности.

Сегодня Ajax – самая титулованная беспроводная система безопасности в Европе. Ajax признана «Лучшим инновационным продуктом» на Securika MIPS и «Охранная система года» на Intersec. Во Франции система получила награду «Безопасность и противопожарные риски» на Les Trophées Exoprotection.

ПРЕИМУЩЕСТВА СИСТЕМЫ AJAX ДЛЯ КОММЕРЧЕСКИХ ОБЪЕКТОВ

Система безопасности Ajax широко используется для охраны крупного и среднего бизнеса. Рассмотрим несколько характерных примеров.

В РОССИИ

Онлайн-магазин построил централизованную защиту более 400 точек выдачи товара на базе системы Ajax. На каждой точке был установлен базовый комплект оборудования: централь Hub, комбинированный датчик движения и разбития стекла CombiProtect, датчик открытия двери DoorProtect, сенсорная клавиатура KeyPad, видеокамера Hikvision.

В САУДОВСКОЙ АРАВИИ

Перед владельцами крупной сети аптек стояла задача защитить 70 отделений по всей стране. Внедрить систему безопасности хотели без ремонта и в максимально короткие сроки. Внутренняя служба безопасности решила установить беспроводные датчики Ajax. Каждая аптека была оборудована следующим комплектом: централь Hub, клавиатура KeyPad, датчики движения MotionProtect Plus – в зале и на складе, датчики открытия двери DoorProtect Plus, двумя видеокамерами Dahua.

В УКРАИНЕ

Сеть супермаркетов электроники применила расширенный комплект системы Ajax, включающий датчики, сирены, брелоки с тревожной кнопкой. А также интегрировала видеорегистраторы.

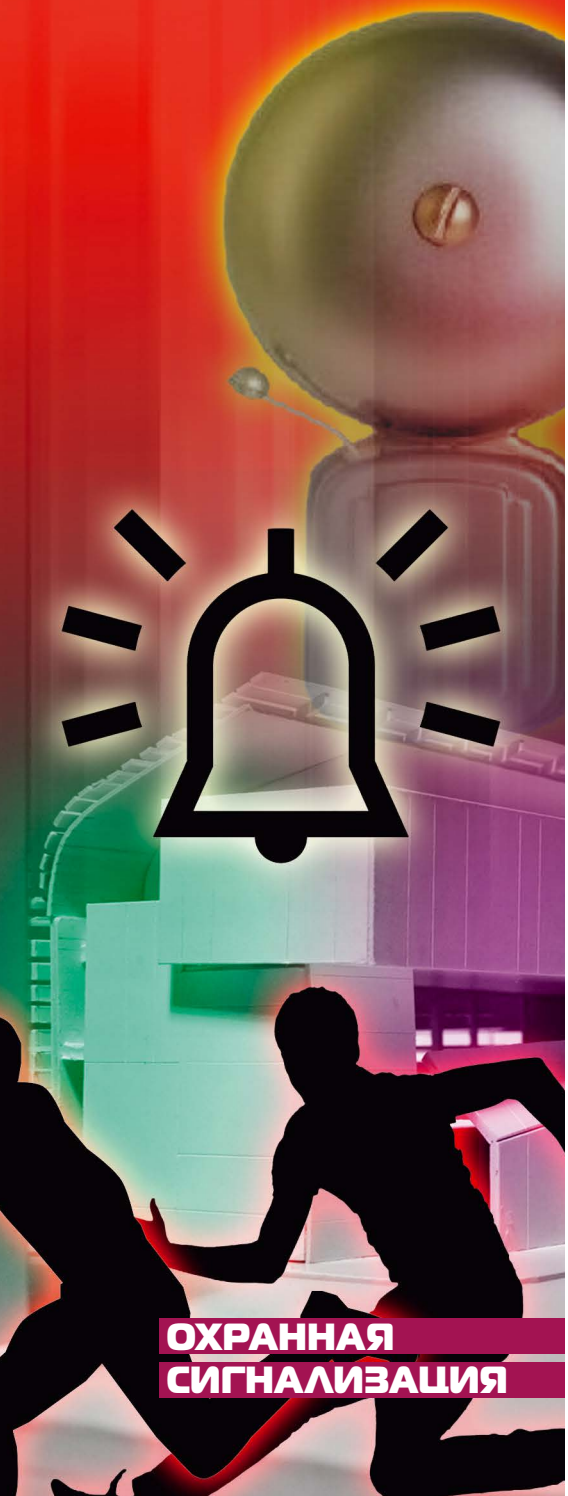
Внутренние службы безопасности компаний используют приложения Ajax для просмотра потоков с видеокамер, контроля состояния устройств и администрирования каждого объекта. Кроме того, системы безопасности подключены к ПЦН местных охранных компаний.

AJAX

ООО «Аджакс Системс»
Москва, ул. Рочдельская, д. 15, стр. 17–18, 3 этаж, офис 17
тел.: 8-800-500-41-05
e-mail: hello@ajax.systems
ajax.ru

«Операция Ы...» и охрана магазина сегодня

Копытова Ольга Андреевна
исполнительный директор Safe City 112



ОХРАННАЯ СИГНАЛИЗАЦИЯ

Физическая охрана дежурным сторожем – активной пенсионеркой или голодным студентом – прекрасно зафиксирована в классике советского кинематографа. Конечно, сегодняшний охранник – это совсем другой уровень. Благодаря закону «О частной охранной деятельности...» наведен относительный порядок и со служебными обязанностями, и с обучением, и с внешним видом. Но, тем не менее, в данной статье мы ставим вопрос о том, что сам тип физической охраны тоже скоро станет историей, как минимум на уровне частных коммерческих компаний. И предпосылки здесь две: экономическая и техническая.

Возьмем, к примеру, небольшой магазин «шаговой доступности» площадью около 100 м^2. Два вопроса: как правильно считать потраченные деньги и как современные технологии меняют алгоритмы и стоимость охраны такого объекта. Сразу оговоримся, что рассмотрим как объекты с 24-часовым графиком работы, так и закрываемые на ночь.

Вернемся к легендарному фильму. Первое, о чем нужно напомнить, – современный охранник, услуги которого предлагают многочисленные агентства, это, прежде всего, человек без ружья, даже без заряженного солью. И связывать и «грузить в саночки» он никого не имеет право по определению. Максимум, что он может, – пригласить подозреваемого в краже дождаться приезда вызванной им полиции или просто вызвать полицию, если есть подозрение на угрозу грабежа магазина. И даже эти нехитрые обязанности никак невозможно полноценно выполнить без пультовой охраны (частной или вневедомственной). Кто пробовал дозвониться по 02, поймет, что без тревожной кнопки, передающей сигнал за секунды, и приезда наряда в течение 10–15 минут, как это в большинстве случаев предусмотрено договором, – не обойтись. Что же остается, кроме психологического фактора для хозяина магазина. Ему кажется, что наличие физической охраны что-то ему гарантирует, и за это он готов платить около 100 тыс. рублей в месяц (при трехсменной работе). Очень условно можно причислить дежурного охранника к профессиональной охране, обычно это человек, имеющий невысокий класс лицензии, т.е. прошедший только устный инструктаж, а не полноценное обучение. Что качественно отличает его от профессиональной группы реагирования, выезжающей по тревоге.

Немного остановимся на упомянутых гарантиях и еще раз вернемся к героям любимого фильма. Несмотря на комедийный жанр, мы иногда всерьез сравниваем этих ответственных и смелых охранников в тулупах с современными охранниками в идеальной форме и с непроницаемыми лицами. Уверены ли мы, что эти люди готовы броситься с риском для своего здоровья на грабителей, не растеряются ли в экстремальной ситуации. И статистика частных охранных агентств неутешительна – в более чем 90% случаев тревожная кнопка используется уже по факту грабежа, когда злоумышленники уже скрылись. И опять вернемся к кинематографу – ограбление-то было, когда все украли заранее. Охранник не только не повлияет на внутренние хищения, но еще может оказаться в сговоре с персоналом, а значит, следить нужно и за ним. И еще одна немаловажная деталь – охранник не имеет материальной заинтересованности в процветании торговли. Более того, его служебные обязанности по досмотру покупателей, бдительное наблюдение никак не улучшают атмосферу в магазине, а значит, и комфорт посетителей. Можно как угодно долго перечислять негативные составляющие так называемого человеческого фактора, говорящие о «закате» физической охраны в магазине. Но что же является альтернативой?

Как уже упоминалось выше, без тревожной кнопки не обойтись. А значит, в охрану магазина входит оснащение охранной сигнализацией. Самые бюджетные современные охранные панели уже построены не на одном шлейфе сигнализации. Имеет смысл предусмотреть и полноценную охранную сигнализацию всего магазина. В случае круглосуточной работы это кажется не актуальным. Но не забывайте о сейфовых комнатах, складе с ценными товарами, кабинете директо-

ра – в этих помещениях персонал находится только днем, впрочем, и днем сейфы лучше ставить под охрану. Если же мы говорим о магазине, который нужно ставить под охрану ночью, то комплект охранной сигнализации может выглядеть следующим образом:

- контрольная панель и комплект оборудования для передачи сигнала на пульт централизованного наблюдения;
- охранные извещатели на окнах и витринах;
- охранные извещатели на входных (разгрузочных) зонах, помещениях с ценностями, желательно и на двери сейфа;
- охранные извещатели (объемные) во всех помещениях, складах и торговом зале;
- тревожная кнопка (возможно, несколько).

Логика пользования помещениями у всех магазинов разная, разные права доступа у сотрудников, разные алгоритмы постановки и снятия с охраны магазина. Например, постановку на охрану всего магазина осуществляет дежурный продавец, а помещения с ценностями – администратор, а складом заведует отдельный персонал и т.д. Гибкость системы обеспечит организация максимального количества разделов/зон охраны, и это в большинстве случаев никак не повлияет на стоимость системы. Организация разделов повысит информативность, значит, группа реагирования сразу по получению тревожного сигнала уже может разработать план пресечения преступления. Кроме того, отдельный раздел в сейфовой комнате дает возможность использовать пассивные методы охраны: дымовые завесы, сирены, световые шокеры и т.п. Использование этих систем из-за ложных срабатываний практически невозможно в автоматическом режиме запуска. Но удаленное включение с пульта охраны безопасно и эффективно, особенно, если объект еще оснащен системой видеомониторинга.

И еще раз вернемся к тревожной кнопке. Эффективность ее использования зависит от работы персонала. Охранники обучены пресекать реальные преступления, следовательно, в лучшем случае она будет нажата уже в момент очевидного грабежа. Но, как упоминалось ранее, реальная ситуация редко складывается идеально. Времени на реагирование может не хватить, охранник – растеряться. К тому же его зона ответственности входная, за кассой, а преступление может совершаться и в других помещениях. Не нужно забывать, что договор с охранным агентством предусматривает вызов группы реагирования именно для предотвращения грабежа и воровства. А значит, вызов на основании любых подозрительных действий посетителей не может оцениваться как ложный. Правильно обученный персонал магазина гораздо эффективнее в определении угроз, и вполне логично доверить тревожную кнопку именно им. Это еще один аргумент о неэффективности физической охраны посредством дежурного охранника.

Перейдем к системе видеонаблюдения. Она стала уже обязательным элементом, поскольку призвана решать множество административных и бизнес-задач даже самого небольшого магазина. Прибавим к этому обязательное требование в рамках антитеррористической защиты – магазины причислены к объектам с массовым пребыванием людей по критерию – более 50 человек на объекте. А значит, требования по установке видеокамер и 30-дневному хранению информации уже ложатся материальным грузом на владельца магазина. Предположим, что камеры и так используются для работы магазина, и это не является дополнительными затратами. Архив можно хранить в облаке, что значительно удешевляет стоимость системы за счет экономии на видеорегистраторах с большими системами хранения. Но организация полноценной системы видеонаблюдения для охранных целей на объекте – это уже серьезные затраты. Требуется предусмотреть хотя бы минимальный набор функций видеоаналитики, организовать хотя бы небольшой архив с интеллектуальным поиском для оперативного разбора ситуаций. И самое главное, предусмотреть локальное рабочее место оператора видеонаблюдения. Здесь и прямые расходы на оборудование, и выделение дефицитной площади – стоимость услуг такого охранника уже значительно выше. И кстати, это не заменяет работу охранника в зале. Следовательно, двойные расходы на зарплату.

Прежде чем перейти к достоинствам использования системы удаленного видеомониторинга, поделимся еще одним решением, позволяющим удалить охранника из магазина.

Все мы уже привыкли к табличкам «ведется видеонаблюдение». И эта привычка сыграла злую шутку – их уже никто не замечает. Насколько правильнее прямо при входе, на месте скучающего охранника, повесить видеомонитор с выводом на экран изображений видеокамер торгового зала. Практика внедрения показывает, что это дает снижение попыток воровства в несколько раз, а потратить единоразово нужно не более месячной зарплаты одного охранника. Уже есть примеры замены охранников именно таким решением.

Что же может добавить к охране магазина система удаленного видеомониторинга. Если на пульте централизованной охраны, кроме реагирования на тревожные сообщения, ведется постоянное наблюдение за объектом, это не только повышает надежность и эффективность реагирования, но и дает возможность использования пассивных методов охраны, о которых упоминалось выше. Никакой, даже самый добросовестный и обученный, охранник магазина не сможет, да и не уполномочен пресечь серьезное, вооруженное ограбление. Не может защитить сотрудников и посетителей. Тем более на дежурстве он один. Видеомониторинг поможет группе реагирования правильно оценить ситуацию, сделать все возможное для защиты людей. Оперативное прибытие группы, локализация ее действий по информации от видео, если и не задержит похитителей, то не даст им достаточно времени для нанесения серьезного ущерба. И конечно же, видеоинформация вместе с осмотром объекта повышает шансы найти злоумыш-

ленников «по горячим следам» и вернуть похищенные ценности.

Пульт видеонаблюдения охранного агентства – это очень мощная система. Интеллектуальные функции системы обычно самые современные, как по формированию сигналов тревог, так и по поиску информации в архиве для разбора ситуаций. Небольшой магазин, скорее всего, не сможет позволить себе такую технику. Кроме того важен фактор независимости – хозяин магазина защищен от сокрытия нарушений своими сотрудниками, все на виду. По отзывам заказчиков, пользующихся такими услугами, дисциплина на объекте повышается практически в день внедрения системы, а недобросовестные сотрудники предпочитают уволиться.

Сделаем первый вывод. Современные технические средства позволяют не только полностью заменить дежурного охранника в магазине, но и перевести охрану магазина на другой уровень безопасности. Вместо субъективного ощущения можно получить реальную и профессиональную защиту: постоянное наблюдение, фиксацию всех нештатных событий, оперативное прибытие на место преступления профессиональной группы реагирования (а при необходимости и нескольких).

Разобрав организационно-технические особенности организации охраны магазина без охранника, перейдем к экономической части. Позволим себе небольшой сравнительный анализ.

Если охрана магазина осуществляется силами дежурного охранника, то оплата его услуг при трехсменном режиме составит около 1 200 000 руб. в год. Если же дополнительно заказчик организует собственное рабочее место видеонаблюдения, то эти затраты увеличиваются вдвое. Плюс вложения на оснащение самого рабочего места – не менее 70 000 рублей. И не забываем об аргументах в пользу необходимости тревожной кнопки и, как следствие, системы сигнализации и оплаты услуг пультовой охраны. Этот расчет не совсем корректен, поскольку в рамках антитеррористической защиты все равно придется потратиться на систему видеонаблюдения.

Рассмотрим вариант решения задачи техническими средствами с привлечением централизованной охраны. Полноценная система охраны, описанная выше, для магазина площадью около 100 м^2 обойдется владельцу единоразово примерно в 100 000 руб., а установка видеокамер, облачного хранения и вывод информации на два объектовых монитора – 200 000 руб. Очевидно, что зарплата охранника «отбивается» менее чем через 3 месяца. Услуги централизованной охраны составляют примерно 5000 руб. в месяц, а совместно с удаленным видеомониторингом (с учетом затрат на связь) до 10 000 руб. в месяц. И в сумму услуг включены выезды профессиональных групп реагирования. Не забываем, что компания, осуществляющая централизованную охрану, заинтересована в бесперебойной работе систем безопасности объекта. Это означает, что с владельца снимаются вопросы обслуживания.

Не потребуется доставать калькулятор, чтобы сделать вывод: оснащение магазина системой безопасности с выводом информации на пульт централизованного наблюдения и выездом группы реагирования – самый экономичный и эффективный способ защиты объекта.

Конечно, обаятельный сторож из любимого кинофильма убеждал нас в необходимости специального сотрудника для охраны магазина. Но его эффективность, по сравнению с деятельностью профессионалов централизованной охраны вкупе с возможностями охранной техники, не очевидна. Подробное изучение функций современных технических средств откроет перед заказчиком не только новые грани безопасности, но и дополнительные возможности по организации бизнеса. Но торговля есть торговля. Начните с расчета вложений и текущих затрат, и вывод сделайте сами.

ЭФФЕКТИВНЫЕ ОПЦИИ ОХРАННОЙ СИГНАЛИЗАЦИИ

Мониторинговый центр «Safe City 112» предоставляет полный комплекс охранного мониторинга для объектов различного назначения. Для этих целей организованы пульты централизованной охраны, обеспечивающие как прием сигнала от тревожных кнопок и систем охранной сигнализации, так и развернутое удаленное круглосуточное видеонаблюдение. При возникновении экстренных ситуаций операторы связываются с клиентом для уточнения обстоятельств и при необходимости вызывают оперативные службы или группы быстрого реагирования. Для обеспечения безопасности клиентов специалисты центра подбирают и устанавливают на объекте технические средства, которые прошли проверку на надежность и отвечают индивидуальным требованиям клиентов. При неполадках с аппаратурой нужно лишь сообщить оператору мониторингового центра и ждать устранения проблемы

Многие системы охранной сигнализации приобретают новые качества при подключении объекта на пульт централизованного наблюдения. По практике работы компании особое внимание нужно уделить выбору и установке тревожной кнопки, поскольку ее функции достаточно широки и гибко настраиваемые.

Прежде всего, это вызов сотрудниками объекта, на котором произошла экстренная ситуация. Но можно оснастить и автомобиль (личный или коммерческий) и через наш пульт централизованной охраны простым нажатием кнопки вызвать ГИБДД или эвакуатор при ДТП. Встроенный GPS-навигатор передаст на пульт местонахождение угнанного автомобиля, и сотрудники нашей компании организуют розыск и возврат транспортного средства.

На этапе разработки находится проект «социальной кнопки». Данное устройство предназначено для тяжелобольных людей, инвалидов, одиноких пенсионеров. Ее планируют сделать двух типов: стационарную (для лежачих больных) и портативную. При ухудшении состояния здоровья, для вызова социального такси, при чрезвычайной ситуации, а также по консультационным вопросам клиент нажимает кнопку на своем устройстве и операторы мониторингового центра принимают необходимые меры.

Большой опыт охраны магазинов, автозаправок, кафе и тому подобных малых коммерческих объектов, на которых не предусмотрены серьезные, обученные службы безопасности, подсказал необходимость установки еще одного типа систем для предотвращения краж.

Генеральным директором компании «Safe City 112» Дмитрием Олеговичем Копытовым совместно с техническим департаментом группы компаний «Энерголайн» был разработан комплект КПО-1, который направлен на предотвращение краж материальных ценностей и пассивную защиту сейфовых комнат на охраняемых объектах клиентов. Речь идет о задымлении помещения в случае несанкционированного проникновения. Эффект этого метода защиты в том, что в зоне поражения становится некомфортно находиться. КПО-1 – это новый подход и ответ на все замечания по использованию подобных систем, накопленные за все время их эксплуатации.

В состав комплекта входят: контрольная панель с управляемым реле, сирена и дымовые шашки. На *рисунке 1* приведена схема подключения. Требуется источник питания 12 В, и есть возможность подключения от действующей охранной сигнализации. При активизации КПО-1 можно предусмотреть также автоматический сигнал тревоги на пульт централизованного наблюдения, сотрудники которого направят на объект группу реагирования для возможного захвата временно деморализованных нарушителей.

Случаи ложного срабатывания и соответствующие последствия, если система установлена в помещениях, где находится персонал, можно исключить за счет отмены автоматической сработки. Есть различные варианты активации КПО-1 в ручном режиме. Это можно осуществить самими сотрудниками объекта, с пульта централизованной охраны по сигналу тревоги и/или по решению оператора удаленного видеонаблюдения. Для управления предусмотрен сигнал включения с любого желаемого устройства – звонком с телефона на номер, присвоенный контрольной панели. Такое решение позволяет гибко настроить работу системы под любые требования клиента.

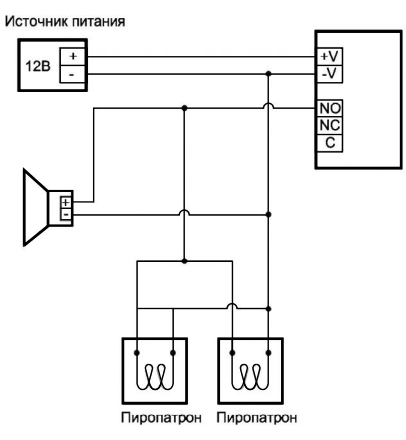


Рис. 1. *Схема подключения КПО-1*

Комплект прост в монтаже и эксплуатации. Используемые пиропатроны рассчитаны для небольшого объема. Для замены пиропатрона не требуется вызывать специалиста, по желанию это может произвести сам клиент. И стоимость самого пиропатрона незначительна.

Еще одна важная деталь. После срабатывания системы (истинного или ложного) не требуется уборка помещения, незначительный запах пороха быстро выветривается.

По сравнению с использованием для подобных решений генератора тумана, КПО-1 не имеет ограничений по температуре помещений, а значит, может быть установлен на неотапливаемых складах, погрузочных зонах, различных охраняемых инженерных помещениях и т.п. И стоимость заправки значительно ниже, чем у систем с использованием генератора тумана (генератор тумана – 100 000 руб., пакет с жидкостью для заправки генератора – от 8000 руб.).

КПО-1 – это эффективное и надежное решение, доступное по цене для любых клиентов «Safe City 112». Также систему можно приобрести в качестве готового комплекта. Стоимость комплекта КПО-1 составляет около 10 000–15 000 руб. Сам пиропатрон – 1500 руб.

Для объектов, находящихся под централизованной охраной «Safe City 112», могут быть предусмотрены многие индивидуальные опции. Возможности мониторингового центра универсальны, а значит, решение задач клиентов будет обеспечено на 100%.

SAFECITY 112

ООО «Сэйф Сити 112»
тел.: (812) 402-88-88
тел.: (903) 092-11-12
e-mail: info@safecity112.ru
www.safecity112.ru

SYNOLOGY: И ЭТО ВСЕ О NAS

Компания Synology предлагает стратегию многофункциональности NAS-устройств, позволяющую решить задачи по организации IT-инфраструктуры, стоящие перед современным офисом. Такой подход приветствуется рачительным средним и малым бизнесом. Тем более, что политика компании Synology позволяет наращивать мощность IT-структуры с ростом потребностей, а не приобретать аппаратно-программные продукты на вырост.

Сердцем системы, построенной на серверах Synology, является операционная система **Synology DiskStation Manager** (DSM). Для работы с дополнительными сервисами и функциями используется Центр пакетов, устанавливаемых при необходимости программных модулей. Официальный каталог насчитывает свыше ста приложений, большая часть из которых бесплатна.

Пакет **Synology Drive** позволяет создать собственное облако из вашего NAS-сервера с сохранением политики прав доступа. Изменения, внесенные в файл на одном из устройств, будут автоматически внесены в соответствующие файлы и папки на других устройствах при подключении к сети. Доступно создание папок, управление файлами, установка тэгов, защита файлов паролем, а также совместный доступ к документам.

Ни одна компания не может обойтись без функции резервного копирования, и возможность сравнительно недорогого и быстрого восстановления информации востребована бизнесом. Для решения этой задачи в DSM реализован целый набор приложений.

Пакет **Active Backup for for Business** (ABB) – это централизованное решение по созданию резервных копий серверов и рабочих станций семейства Windows. При использовании клиентского ПО Active Backup for Business Agent Synology может резервировать целиком образ системы с данными. А вот для резервирования виртуальных машин на VMware установка Agent не требуется. Пакет **Hyper Backup** позволяет делать резервные копии с NAS Synology между разделами на другой NAS Synology, внешние носители и облачные среды или собственное облако Synology C2.

В качестве дополнительной защиты данных будет полезна технология для мгновенного восстановления, которую реализовывает приложение **Snapshot Replication**.

Приложение **Virtual Machine Manager** (VMM) позволяет создавать свои виртуальные машины (серверы) или несколько виртуальных машин, включая Windows, Linux и Virtual DSM на Synology NAS. Кроме того, VMM является решением для восстановления резервных копий, сделанных ABB, что позволяет обеспечить непрерывность работы служб и гибкое управление ресурсами.

Конфиденциальность и надежность деловой переписки реализуется в DSM посредством программного пакета **MailPlus Server**. Компания получает собственный почтовый сервер и веб-клиент для эффективной работы с электронной почтой, позволяющий упорядочивать сообщения, проверять корпоративные адресные книги, а также совместно с деловыми партнерами использовать почтовые ящики.

Системы видеонаблюдения являются неотъемлемой частью безопасного ведения бизнеса. На рынке безопасности нет единого мнения о предпочтительном варианте сервера для системы видеонаблюдения. С недавнего времени к участию в спорах сторонников DAS- и NAS-серверов присоединяются производители видеокамер, прямо указывающие в спецификациях: «Поддержка записи на сетевой накопитель (NAS)». Система видеонаблюдения **Surveillance Station** актуальна для малых (системы видеонаблюдения до 16 камер), средних (от 16 до 100 камер) и крупных (до 5000 камер) предприятий. Приложение поддерживает более 7000 IP-камер от 120 вендоров. Видеокамеры производства Axis, Bosch, Dahua, Hikvision и Amcrest интегрируются в систему видеонаблюдения Synology посредством API (application programming interface). Surveillance Station предоставляется в Центре пакетов Synology бесплатно (подключение двух видеокамер) и поддерживается на всех устройствах Synology. Новые устройства добавляются в систему путем приобретения лицензий.

Приложение позволяет просматривать трансляцию с нескольких IP-камер в режиме реального времени, воспроизводить записи, работать с пакетами настроек камер. Приложение совместимо с основными браузерами (IE, Firefox и Safari), операционными системами (Windows® и Mac®), а для мобильных устройств (iOS и Android™) разработано приложение DS CAM и LiveCam. Мобильные устройства поддерживают просмотр видео с 6 камер одновременно, при установке бесплатного мобильного клиента Synology – до 12.

Реализованная на NAS-серверах Synology функция «Правило действия», делает возможным автоматическое реагирование на конкретные события. Программно определяются: обнаружение движения, отсутствующий объект, посторонний объект – в заранее определенной зоне; загораживание камеры; расфокусировка камеры; пребывание объекта дольше назначенного времени в зоне активности. Фиксация системой наступления одного или нескольких событий запускает сценарий реагирования, например:

- если злоумышленник повредит одну из видеокамер, предустановленный режим патрулирования объекта с помощью PTZ-камер позволит запустить панорамирование на ближайшей камере или отслеживание объектов в данной зоне;
- если в системе видеонаблюдения задействованы камеры с поддержкой цифрового ввода/вывода, то через интерфейс Surveillance Station возможно задействовать внешние свето-звуковые устройства.

Объединение NAS-серверов Synology с сетевыми контроллерами ввода/вывода создает интегрированную систему безопасности на единой платформе. Управление физическим доступом позволяет открывать и блокировать двери, осуществлять наблюдение за точками доступа. Приложение Surveillance Station реализует опцию «Журналы доступа к подключенным дверям»: поиск записей осуществляется по источнику, двери, состоянию, временному промежутку и ключевым словам. Записи сопровождаются видео, сделанными сопряженной с контроллером камерой.

Объем журнальной публикации не позволяет хотя бы кратко описать более 100 приложений, разработанных компанией Synology, но одно невозможно оставить без внимания – собственная русскоязычная служба поддержки, функционирующая с 09:00 до 20:00 часов в течение рабочей недели. Специалисты Synology консультируют, а при необходимости производят удаленное подключение и отлаживают работу сервера совместно с IT-службой заказчика.

Расширенная версия статьи «Synology: И это все о NAS» размещена в разделе «Статьи AVTORITET.NET»

Synology®

Synology Inc
www.synology.com
Русскоязычная техподдержка:
тел.: (499) 704-4539 для Москвы
тел.: (804) 333-9601 для регионов России
(звонок бесплатный)
www.synology.su

РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБЪЕКТОВ ОБЩЕОБРАЗОВАТЕЛЬНОЙ СФЕРЫ

КОМПЛЕКСНЫЕ СИСТЕМЫ

Шепелев Алексей Викторович
полковник полиции, начальник отдела научно-технической информации ФКУ НИЦ «Охрана» Росгвардии,
Кузнецова Елена Николаевна
старший научный сотрудник ФКУ НИЦ «Охрана» Росгвардии,
Метелева Наталья Георгиевна
научный сотрудник ФКУ НИЦ «Охрана» Росгвардии

Обеспечение безопасности общеобразовательных учреждений в последние годы стало особенно актуально. Следует учитывать современные вероятные угрозы, такие как вооруженное нападение, возможность захвата заложников и другие. Только за 2017–2018 годы зафиксировано не менее 15 случаев нападения или использования холодного и огнестрельного оружия в российских школах, в результате которых учащимся, педагогам, сотрудникам полиции были причинены тяжкий вред здоровью или действия, повлекшие смерть человека.

Безопасные условия обучения, охрану учеников и работников во время их пребывания в учебном заведении обязано обеспечивать образовательное учреждение в соответствии с п. 8 статьи 41 и п. 6 статьи 28 федерального закона № 273-ФЗ «Об образовании» от 29.12.2012.

Организационные, инженерно-технические, правовые и другие мероприятия по антитеррористической защищенности указанных объектов закреплены постановлением Правительства РФ № 1235 от 7.10.2017 *«Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации и формы паспорта безопасности этих объектов (территорий)»*, а также федеральным законом от 30.12.2009 № 384-ФЗ *«Технический регламент о безопасности зданий и сооружений»*.

В соответствии с этим постановлением правообладателю объекта предоставляются широкие возможности самостоятельного выбора варианта оборудования инженерно-техническими средствами охраны. Параметры объектов по площади, конфигурации, прилегающей территории, дополнительным постройкам, а также условиям финансирования настолько различаются, что для организации их защиты в каждом конкретном случае требуется индивидуальный подход. В одном случае такая система будет слишком дорогой, в другом – не обеспечит требуемого уровня безопасности, в третьем – системе достаточно зафиксировать только факт проникновения нарушителя, в четвертом – на объектах необходима идентификация личности и т.д. В то же время, многие вопросы организационного и структурного построения систем безопасности в определенной степени являются общими и вполне применимыми для целого ряда объектов. В любом случае система обеспечения безопасности объекта должна строиться по принципу «разумной достаточности».

При построении системы безопасности необходимо исходить из специфики объекта – с одной стороны, нужно организовать беспрепятственный доступ детей и работников в образовательное учреждение в определенное время суток, а с другой – максимально ограничить возможность проникновения на объект посторонних лиц. Поэтому основными составляющими должны быть:

- охранно-тревожная сигнализация;
- система контроля управления доступом;
- система видеонаблюдения.

Безопасность объекта оптимально реализовывать на базе интегрированных систем безопасности, в которых на одной аппаратной платформе объединены указанные подсистемы.

На каждую подсистему разрабатывается свой рабочий проект, который содержит пояснительную записку и графическую часть.

Рассмотрим типовой рабочий проект системы охранно-тревожной сигнализации общеобразовательного учреждения (школа). В состав проекта входит пояснительная записка, которая содержит общую часть, характеристики объекта, технические решения и графическую часть с планом объекта.

ОБЩАЯ ЧАСТЬ

Содержит свод нормативных и нормативно-технических документов на соответствие разработке данного проекта, а именно:

1. Постановление Правительства РФ от 18.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию».

2. СП 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования».

3. ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации».

4. Р 78.36.039-2014 Технические средства систем безопасности объектов.

5. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения.

6. Р 78.36.032-2013 «Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1. Методические рекомендации».

7. Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации».

8. Р 78.36.028-2012 Рекомендации «Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов».

9. К 78.36.001-2014 Классификатор условных обозначений на технические средства систем передачи извещений.

ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

Согласно рекомендациям Р 78.36.032-2013, общеобразовательные учреждения являются объектами с массовым пребыванием граждан, на которых охрана общественного порядка и материальных ценностей обеспечивается постами физической охраны и выводом тревожной сигнализации на ПЦО подразделений вневедомственной охраны, и относятся к категории А3.

В общем виде архитектурно-типологическая структура здания общеобразовательного учреждения имеет две основные обособленные группы – учебную и общешкольную. Специфичная организация архитектурных решений школ требует продуманных решений по обеспечению их безопасности.

Для установления требований противокриминальной защиты необходимо проводить обследование – оценку состояния защиты объекта комиссией по антитеррористической защищенности. В состав комиссии входят представители организации правообладателя, сотрудники объекта, а также представители территориального органа безопасности и сотрудники вневедомственной охраны Росгвардии, обладающие необходимыми навыками в данной сфере.

В ходе обследования комиссия исследует:

- расположение объекта на местности;
- занимаемую площадь;
- конфигурацию периметра;
- критические элементы, в отношении которых могут быть реализованы противоправные действия и вероятные способы проникновения (открывание, взлом или пролом, другие способы);
- инфраструктуру физической охраны (внутриобъектовый и пропускной режимы).

Пример объекта: *Защите средствами охранно-тревожной сигнализации подлежит двухэтажное здание общеобразовательного учреждения (школа), высота потолка в помещениях 3 м, высота потолка в спортзале 6 м. Территория школы огорожена декоративным металлическим ограждением на ленточном железобетонном фундаменте. Высота ограждения 2,5 м. Физическая охрана здания осуществляется круглосуточно. Центральная входная дверь и дверь запасного выхода открываются наружу и соответствуют 2 степени защиты объекта от проникновения (двери, соответствующие 1 классу защиты от взлома по ГОСТ Р 51072-05). Ключи от замков двери запасного выхода размещаются в специально выделенном помещении (в помещении охраны), в шкафу, исключающем доступ к нему посторонних лиц. Остальные двери в здании школы соответствуют 1 классу защиты (минимально необходимая степень защиты объекта от проникновения. Двери деревянные внутренние со сплошным или мелкопустотным заполнением полотен по ГОСТ 6629-88, ГОСТ 14624-84, ГОСТ 24698-81. Толщина полотна менее 40 мм).*

Окна здания соответствуют конструкции 1 класса защиты (минимально необходимая степень защиты объекта от проникновения). Окна с обычным стеклом, дополнительно оклеенным защитной пленкой, обеспечивающей класс устойчивости остекления А1 по ГОСТ Р 51136-08. Оконный проем помещения охраны соответствует конструкции 2 класса защиты (средняя степень защиты объекта от проникновения). Решетки на окнах отсутствуют.

Все защищаемые помещения в здании отапливаемые, в помещениях предусмотрена естественная приточно-вытяжная вентиляция.

На этажах здания расположены административные помещения, учебные классы и кабинеты, санузлы и служебные помещения.

Лифт в здании не предусмотрен. Вертикальная связь между этажами осуществляется по лестнице. Чердачные и подвальные помещения отсутствуют.

Электроснабжение – централизованное от городской сети 380/220 В.

Стены и перекрытия в здании соответствуют 2 классу защиты (средняя степень защиты от проникновения, сплошные железобетонные перекрытия толщиной 120 мм и 160 мм из легких бетонов).

Охрана располагается на первом этаже возле центрального входа.

В помещении директора располагается металлический шкаф (сейф).

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Охранно-тревожной сигнализацией оборудуются все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери), через которые возможно несанкционированное проникновение в помещения объекта.

Обязательным требованием для всех образовательных учреждений является установка тревожной сигнализации с выводом в дежурную часть вневедомственной охраны для оперативной передачи сообщения о противоправных действи-

ях. Это позволит в кратчайшие сроки принять необходимые меры по пресечению правонарушения.

В состав данного раздела должны входить следующие подразделы.

НАЗНАЧЕНИЕ И ФУНКЦИИ СИСТЕМЫ

Система охранно-тревожной сигнализации предназначена для обеспечения защиты людей и материальных ценностей, находящихся в защищаемом здании.

Система охранно-тревожной сигнализации выполняет следующие функции:

- выявление (автоматически и персоналом) тревожных ситуаций, формирование сигналов тревоги, выдачу информации о наличии и месте возникновения тревожной ситуации на пульт управления;
- автоматический и полуавтоматический (по сигналам с пульта) контроль состояния элементов системы и ее составных частей.

СИСТЕМА ОХРАННОЙ СИГНАЛИЗАЦИИ (СОС) ЗДАНИЯ

Для построения СОС применены пульт контроля и управления охранно-пожарный, подключаемые к нему по RS-485 приборы приемно-контрольные (ППК) емкостью на двадцать шлейфов сигнализации.

Пульт контроля и управления охранно-пожарный (далее – пульт) предназначен для работы в составе систем охранной и пожарной сигнализации для контроля состояния и сбора информации, ведения протокола возникающих в системе событий, индикации тревог, управления постановкой на охрану, снятием с охраны, управления автоматикой. В системе пульт выполняет функцию центрального контроллера, собирающего информацию с ППК и управляющего ими автоматически или по командам оператора. ППК анализируют состояние шлейфов сигнализации (ШС), передают на пульт информацию о состоянии ШС и позволяют ставить на охрану/снимать с охраны ШС командами с пульта.

На первом этаже здания охранной сигнализацией блокируются:

- окна на открывание и разрушение;
- двери на открывание;
- входные двери в здание на открывание и пролом.
- кабинет директора (пом. 6) двумя рубежами охраны.

Первым рубежом охраны блокируется периметр помещения: двери и окна на открывание, окна на разбитие.

Вторым рубежом охраны блокируется объем помещения.

В кабинете директора блокируется металлический шкаф (сейф) на открывание и пролом.

На втором этаже здания охранной сигнализацией блокируются:

- двери на открывание;
- кабинеты и классы – объем помещений.

Для защиты помещений применены следующие виды извещателей охранной сигнализации:

- деревянные (пластиковые) двери блокируются на «открывание» извещателем охранным магнитоконтактным для установки на деревянные (пластиковые) двери;
- входные двери в здание блокируются на «открывание» извещателем охранным магнитоконтактным для установки на металлические двери и на «разрушение» извещателем охранным поверхностным оптико-электронным;
- окна первого этажа блокируются на «разрушение» (разбитие) извещателем охранным поверхностным звуковым;
- окна первого этажа блокируются на «открывание» извещателем охранным магнитоконтактным для установки на деревянные (пластиковые) окна;
- объем помещения блокируется извещателем охранным объемным оптико-электронным;
- металлический шкаф (сейф) блокируется извещателем охранным поверхностным, вибрационным.

СИСТЕМА ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ

Для подачи сигнала тревоги используются кнопки тревожной сигнализации (извещатель охранный ручной точечный электроконтактный) и извещатели охранные ручные радиоканальные (брелоки).

Стационарные кнопки тревожной сигнализации (КТС) установлены: в кабинете директора (пом. 6), в учительской и в помещении охраны.

Извещатели охранные ручные радиоканальные (брелоки) находятся у директора школы и у охранника. Извещатели охранные ручные радиоканальные (брелоки) подключаются через радиоприемник на ППК.

КТС размещены в местах, незаметных для посторонних.

ОРГАНИЗАЦИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ О СРАБАТЫВАНИИ СИГНАЛИЗАЦИИ

Вся информация о работе системы охранно-тревожной сигнализации выводится в помещение охраны на пульт контроля и управления охранно-пожарный.

На ПЦО ОВО выводятся обобщенный сигнал от КТС об отключении основного электропитания системы и, по согласованию с руководством школы, охранная сигнализация отдельных помещений.

СИСТЕМА ПЕРЕДАЧИ ИЗВЕЩЕНИЙ (СПИ)

Устройство оконечное объектовое (УОО) СПИ предназначено для организации централизованной охраны объектов в составе автоматизированной системы охранно-пожарной сигнализации. УОО осуществляет передачу на ПЦО ОВО извещений «взят/снят», «неисправность», «проникновение».

Способ передачи информации с УОО на ПЦО ОВО зависит от типа СПИ и может осуществляться по занятой или выделенной телефонной линии, радиоканалу, каналу GSM (GPRS) или Ethernet, по GPON (оптоволокну) либо другому проводному каналу связи.

Для исключения доступа посторонних лиц к УОО СПИ, разветвительным коробкам, другой установленной на объекте аппаратуре охраны должны приниматься меры по их маскировке или скрытой установке.

В ЗАКЛЮЧЕНИЕ

Хотелось бы отметить, что многие вопросы организационного и структурного построения систем безопасности в определенной степени являются общими и вполне применимыми для целого ряда объектов. В любом случае система обеспечения безопасности объекта должна строиться по принципу «разумной достаточности», и для ее построения рекомендуется применять технические средства охраны, включенные в Список технических средств безопасности, удовлетворяющих «Единым требованиям 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».

«Единые требования…» – сводный нормативный документ, в котором использованы современные требования национальных, межгосударственных и международных стандартов в области технических средств и систем охранной сигнализации, средств инженерно-технической укрепленности, безопасности и электромагнитной совместимости. Применение технических средств охраны, включенных в Список, обеспечивает высокую надежность централизованной охраны объектов, так как по всем изделиям согласованы технические условия с параметрами, соответствующими или превышающими требования стандартов, проведены техническая экспертиза и испытания, получены необходимые сертификаты, а также осуществляется постоянный контроль качества серийного производства и авторский надзор за вносимыми в них схемными, конструктивными и программными изменениями.

AXIS: VMS РАСТЕТ ВМЕСТЕ С БИЗНЕСОМ

Оснащение объекта системой видеонаблюдения является для ряда малых компаний законодательным требованием. Компания Axis Communications рассказывает о стратегии роста системы видеонаблюдения: как на каждом этапе развития бизнеса иметь достаточную, но не избыточную систему видеонаблюдения; как с ростом бизнеса наращивать систему эволюционным путем; как привлечь систему безопасности к решению бизнес-задач.

МАЛАЯ СИСТЕМА

Для компаний, которым требуются базовые функции видеонаблюдения для контроля своей территории, персонала и имущества, достаточно систем, рассчитанных на 16 и менее видеокамер на объект.

Начальным шагом становится выбор и добавление устройств в систему. **AXIS Site Designer** представляет собой приложение, объединяющее набор инструментов, позволяющих разработать всю систему. На первом этапе определяются параметры, которым должна удовлетворять камера. После выбора необходимых функций следует определить, на какой высоте камера будет установлена, в каком направлении будет повернута, какой угол и плотность пикселей для данной сцены требуется. Результатом применения Site Designer может стать автоматически сгенерированный список всех компонентов, необходимых для построения целостной системы видеонаблюдения, что позволит значительно сократить время разработки проекта. К сохраненному проекту можно возвращаться при любых изменениях и пополнении системы.

Бесплатное программное обеспечение **AXIS Companion** для управления видеонаблюдением включает в себя мобильные приложения для устройств с операционными системами iOS и Android. Технология безопасного удаленного доступа Axis Secure Remote Access обеспечивает доступ к живому видео или видеозаписям для удаленного пользователя, и для этого не требуется настраивать сеть или маршрутизатор. ПО имеет тесную интеграцию со всеми сетевыми камерами и видеокодерами Axis со встроенным ПО версии 5.50 и выше. AXIS Companion поддерживает все разрешения и частоты кадров камеры.

СРЕДНЯЯ СИСТЕМА

С расширением бизнеса требуется расширение системы видеонаблюдения: не только количественное, но и качественное.

Главным шагом на пути роста системы становится смена VMS. Миграция AXIS Companion в систему, поддерживающую до 100 камер на объект, **AXIS Camera Station** проста и сжата во времени: настраивает и запускает систему Мастер настройки с автоматическим обнаружением камер. В интерфейсе пользователя предусмотрены гибкие настройки просмотра видео в режиме реального времени, схемы объектов, широкие возможности настройки событий, управление сигналами тревоги и PTZ-управление. Быстрое расследование инцидентов и получение данных для экспорта реализуются за счет наглядной визуализации относительно временной шкалы и эффективного поиска по видеозаписям.

ОТ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ К СИСТЕМЕ БЕЗОПАСНОСТИ

AXIS Camera Station легко масштабируема, в нее одинаково легко добавляются дополнительные камеры в существующую систему и создаются новые группы камер. Это актуально, например, при увеличении числа производственных помещений компании или при появлении в существующей сети новых подразделений (например, сеть АЗС).

В AXIS Camera Station реализована возможность решения целого спектра задач из одного интерфейса. Этот подход позволяет превратить систему видеонаблюдения в многопрофильную систему безопасности. Для каждой задачи у Axis есть решение из оборудования и приложения.

Пакет приложений **AXIS Guard Suite** позволяет выявлять угрозы и информировать о них службу безопасности. Системы обнаружения движения, вторжения и подозрительных лиц уменьшают число ложных срабатываний системы. Эти аналитические приложения идеально подходят для видеонаблюдения в нерабочее время в магазинах, банках, офисах, учебных заведениях и т.д.

AXIS Entry Manager – IP-система управления доступом, управляющая учетными данными и графиками доступа для контроля тех, кто имеет доступ на территорию объекта. Это приложение решает не только проблемы охраны, но и экономические, в частности, интеграция с системами отопления, вентиляции и кондиционирования воздуха позволяет снижать коммунальные расходы, а также вести учет рабочего времени и посещаемости. Дверные контроллеры, видеодомофоны, считыватели карт Axis разработаны на основе открытых стандартов, и это означает, что заказчик не привязан к продукции одного производителя.

Надстройкой к этому приложению является **AXIS Visitor Access**, с помощью которого на небольших объектах можно легко организовать управление доступом посетителей с использованием QR-кодов в качестве пропусков. Оно в индивидуальном порядке пропускает посетителей на объект и позволяет перемещаться в пределах допустимых зон, одновременно давая возможность отслеживать, кто именно присутствует на объекте в заданный момент времени.

Приложение **AXIS License Plate Verifier**, установленное на совместимую камеру Axis, позволяет создать простую и недорогую систему автоматического управления доступом автомобилей на автостоянках и в других аналогичных местах.

Достаточно установить приложение видеоаналитики на совместимую камеру Axis, настроить камеру и подсоединить порт ввода/вывода камеры к реле, установленном на ограждении для автомобилей. После этого останется лишь ввести в аналитическое приложение список номеров автомобилей и правило действия, чтобы система начала работать.

Экономически выгодным является не только добавление дополнительного приложения к AXIS Camera Station, но и добавление оборудования: решения для контроля доступа легко подсоединить и питать по существующей IP-сети.

Краткий обзор средних и малых систем Axis призван дать общее представление о возможностях и преимуществах VMS. Подробная информация вкупе с практическими занятиями будет представлена на специализированном учебном курсе, первые группы которого начнут занятия в августе 2019 года.

Расширенная версия статьи «Axis: VMS растет вместе с бизнесом» размещена в разделе «Статьи AVTORITET.NET»

ООО «АКСИС КОММУНИКЕЙШНС»
125284, Москва, Ленинградский пр.,
д. 31 А, стр. 1, этаж 16
тел./факс: (495) 940-6682
www.axis.com

ПОЖАРНАЯ БЕЗОПАСНОСТЬ ШКОЛЫ. ПРОЕКТНОЕ РЕШЕНИЕ

Школы и другие детские образовательные учреждения – это объекты самого строгого контроля в области защиты жизни и здоровья детей. Система противопожарной защиты школы включает в себя пожарную сигнализацию, систему оповещения и управления эвакуацией, пожарную автоматику (управление техническими средствами противодымной защиты, автоматизацию противопожарного водопровода, автоматические установки пожаротушения). И при проектировании такой системы необходим комплексный подход с применением современных технологий.

Выделение денежных средств на капитальный ремонт или реконструкцию объектов бюджетной сферы жестко регламентировано и определяется в ходе открытых торгов. В результате госконтракт заключается с компанией, давшей минимальную цену. Поэтому школы зачастую оборудуются самыми дешевыми неадресными системами, применяется минимально возможный по нормам тип оповещения (без разбиения на зоны и невозможностью управления процессом эвакуации). Такие системы быстро оказываются неработоспособными. Так, например, неадресные пожарные извещатели не имеют системы самотестирования и не могут сообщить приемо-контрольному прибору о своей неисправности. Проблема усугубляется также и тем, что должностное лицо, ответственное за пожарную безопасность школы, – директор или его заместитель – редко обладают нужными знаниями для оценки качества смонтированной системы, принимаемой в эксплуатацию. Штрафные санкции за нарушения могут существенно превышать стоимость неадресной системы пожарной сигнализации. Следовательно, для школ необходимо применение адресно-аналоговых систем. Их преимущественные особенности: высокая скорость выявления места возгорания, низкая вероятность ложных срабатываний и повышенная «живучесть». Рассмотрим проектное решение системы противопожарной защиты для здания типовой школы (*рис. 1*).

В настоящее время большая часть школ размещается в типовых зданиях советского периода постройки, представляющих собой два корпуса, соединенных 2-этажным переходом. Такие типовые школы, как правило, имеют минимальный набор инженерных систем, отсутствуют лифты и системы дымоудаления. В последние годы они активно ремонтируются и оборудуются системами безопасности.

Система построена на оборудовании российского производства (ЮНИТЕСТ, Москва) – адресном приборе приемно-контрольном (АППК) ЮНИТРОНИК 496М.

Адресные устройства (адресные извещатели, метки, модули) подключаются к АППК по 2-проводной адресной линии по кольцевой схеме (защита от одиночных обрывов). Ответвления адресной линии подключаются через размыкатели линии РЛ-2 (защита от коротких замыканий – на схеме не показаны). Для удобства дежурного персонала к АППК по линии связи RS-485 подключены пульт светодиодной индикации и управления СДИ и персональный компьютер (ПК) с программным обеспечением (ПО) «Мониторинг». Выдача сигналов на пульт 01 – объектовую станцию (ОС) ПАК «Стрелец-Мониторинг» – реализована при помощи адаптер протокола Contact ID (CID).

Помещения классов, кабинеты, столовая оборудуются адресно-аналоговыми дымовыми пожарными извещателями с системой самотестирования ИП 212-108 МАКС. Особенности извещателя:

- Имеет режимы чувствительности «день/ночь». В режиме «день» чувствительность снижена в 2 раза в пределах допустимого диапазона. В режиме «день» при повышенном, но допустимом уровне задымленности передает извещение «ПРЕДУПРЕЖДЕНИЕ», которое автоматически снимается при восстановлении прозрачности среды.
- Передает значение уровня запыленности дымовой камеры и при превышении 80% подает извещение «ОБСЛУЖИВАНИЕ» на АПКП. Чистка извещателя производится только по необходимости, что сокращает расходы на обслуживание.

Помещения кухни, подсобные и складские помещения, учебные мастерские оборудуются адресно-аналоговыми тепловыми максимально-дифференциальными пожарными извещателями с системой самотестирования ИП 101-50 МАКС. Особенности извещателя:

- Температура срабатывания максимального канала устанавливается с АПКП.
- Передает измеренное значение температуры, а также подает извещение «ПОЖАР» («ВНИМАНИЕ»).

Технические помещения, помещения чердака и подвала оборудуются адресно-аналоговыми газовыми пожарными извещателями с системой самотестирования ИП 435-7 МАКС. Извещатели угарного газа (CO) способны обнаружить возникновение пожара на стадии тления – до появления дыма, пламени и повышения температуры. Они, в отличие от дымовых, практически не подвержены ложным срабатываниям, исправно работают в запыленных, влажных и загрязненных помещениях. В связи с тем, что газ распространяется не только с помощью конвекции, но и за счет диффузии, газовые извещатели работают эффективно при наличии физических барьеров, например, потолочных балок. Особенности извещателя:

- Передает измеренную величину концентрации CO, а также подает извещение «ПОЖАР» («ВНИМАНИЕ») с указанием своего адресного кода.

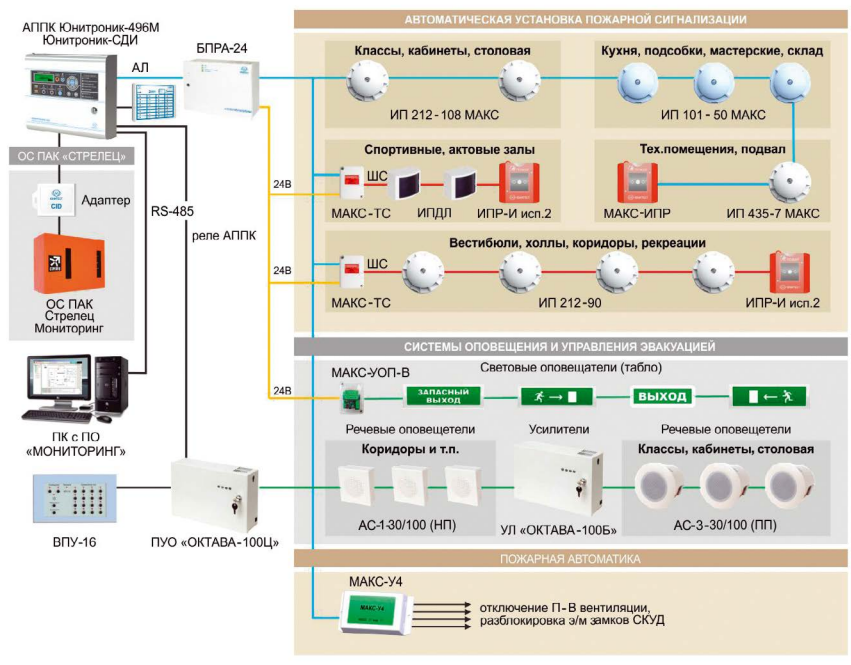


Рис.1. *Структурная схема адресно-аналоговой системы сигнализации и управления*

- Имеет режимы чувствительности «день/ночь».

Для вестибюлей, холлов, коридоров и рекреаций используются извещатели пожарные дымовые оптико-электронные ИП 212-90 «ОДИН ДОМА-2» с автоматическим контролем работоспособности. Извещатель передает извещение «НЕИСПРАВНОСТЬ/ЗАПЫЛЕННОСТЬ» на АПКП.

Извещатель с помощью встроенного светодиода обеспечивает индикацию состояний: «НОРМА»; «ВНИМАНИЕ/ПОЖАР»; «НЕИСПРАВНОСТЬ»; «ЗАПЫЛЕННОСТЬ».

Повышенная достоверность сигнала о пожаре для всех вышеперечисленных извещателей подтверждена сертификатом ВНИИПО МЧС России № ССРП-RU. ЧС13.Н.00307 от 27.08.2018.

На путях эвакуации у выходов из защищаемых помещений устанавливаются адресные ручные пожарные извещатели МАКС-ИПР и аналоговые ручные пожарные извещатели ИПР-И исп.2.

ИПР-И и ИП 212-90 включаются в 2-пороговые шлейфы сигнализации адресных меток МАКС-ТС.

Для помещений с высокими потолками и большими площадями (спортивные и актовый залы) устанавливаются извещатели пожарные дымовые линейные типа ИПДЛ. ИПДЛ также включаются в шлейфы меток МАКС-ТС.

Система речевого оповещения о пожаре и чрезвычайных ситуациях, управления эвакуацией, а также для трансляции информационных сообщений, музыкальных и иных программ «ОКТАВА-100» состоит из прибора управления оповещением «Октава-100Ц», усилителей линейных «Октава-100Б», пульта управления ВПУ-16 и речевых оповещателей АС. Связь между составными частями системы осуществляется по RS-485, что позволяет строить сложные структуры оповещения с линиями связи большой протяженности. Система обеспечивает от 1 до 16 зон речевого оповещения. Запуск оповещения о пожаре (4 зоны оповещения) производится посредством 4 программируемых реле АППК «Юнитроник 496М».

Управление световым оповещением (табло «Выход», «Направление движения») производится адресными модулями МАКС-УОП-В. Табло подключаются к модулю по древовидной схеме и не требуют установки дополнительных диодов и резисторов. Модуль обеспечивает контроль наличия напряжения питания, а также контролирует на обрыв и замыкание линию управления и внутренние цепи табло. В дежурном режиме табло горят, в режиме «Пожар» – мигают.

Отключение принудительной приточно-вытяжной вентиляции (П и В) и разблокировка электромагнитных замков системы контроля и управления доступа (СКУД) при пожаре осуществляется адресными модулями МАКС-У4. Модуль содержит 4 реле (переключающие контакты) для формирования 4 (с одним общим адресом) управляющих сигналов для устройств пожарной автоматики. Модуль контролирует наличие напряжения питания управляемых устройств 12–220 В и исправность цепи управления, включая внутреннюю цепь управляемого устройства.


Сертификат

17062702 27 июня 2017

Настоящим сертификатом удостоверяется, что

ООО «ТД «ЮНИТЕСТ»

является участником сессии производителей инновационной продукции в сфере гражданской обороны, предотвращения чрезвычайных ситуаций и обеспечения пожарной безопасности, прошедшей в ГБУ «Агентство инноваций Москвы» 27 июня 2017 года.

Продукция, представленная ООО «ТД «ЮНИТЕСТ», получила 11,9 баллов из 15 возможных по результатам оценки городскими заказчиками.

По итогам сессии производителей продукция рекомендована к внесению в Перечень инновационной, высокотехнологичной продукции и технологий.

Продукция: Охранно-пожарная адресно-аналоговая система сигнализации «Юнитроник 496М».

Агентство инноваций города Москвы

А.И.Парабучев
Генеральный директор

С.Б.Титов
Руководитель направления

Рис.2. *Сертификат Агентства инноваций Москвы*

В последнее десятилетие активно строятся школы нового типа, с планировками и инженерными системами, отвечающими самым современным требованиям. Такие здания имеют систему дымоудаления, бассейн, компьютерные классы, насыщенные электронным оборудованием. К современным школам часто присоединяют дошкольные учреждения. Для подобных объектов также целесообразно применение системы «Юнитроник 496М», обладающей оптимальным соотношением цена/качество. Дополнительный набор оборудования позволяет управлять и контролировать установки дымоудаления и пожаротушения. Например:

- МАКС-УРП – управление и контроль клапанов с реверсивным приводом;
- МАКС-У, МАКС-У исп.2, МАКС-У исп.4 – одно, два и четыре адресных реле для управления пожарной автоматикой;
- МАКС-УДП – адресные устройства дистанционного пуска (дымоудаление, насосы);
- ШУП – адресные шкафы управления вентиляторами;
- МАКС-КТМ – контроллер считывателя для системы автоматического модульного пожаротушения и ограничения доступа;
- МАКС-УОП – управление сиренами, табло и модулями пожаротушения;
- МАКС-ТК, МАКС-ТК исп.3 – охранно-контрольно-пожарная метка на 1 и 3 ШС;
- МАКС-СМК, МАКС-ДКД – адресный охранный извещатель и датчик контроля дверей зоны безопасности;
- МАКС-КДИ-01 – контроллер для объединения АППК по RS-485 (более 16000 адресов);
- ЮНИТРОНИК-АРМ – сертифицированное автоматизированное место оператора системы.

Внедрение современной системы безопасности «Юнитроник 496М» позволяет обеспечить снижение так называемой «стоимости владения». Бесплатное ПО, наличие «шаблонного» программирования, систем самотестирования, лазерного и аналоговых тестеров, штанги-съемника для извещателей и других инновационных технических решений существенно упрощают техническое обслуживание и соответственно – эксплуатационные расходы, что особенно актуально для бюджетных общеобразовательных учреждений. Система включена в перечень инновационной, высокотехнологичной продукции и технологий (*рис. 2*).

Однако не стоит забывать, что основой обеспечения пожарной безопасности в школах является совокупность технических средств и организационных мероприятий, причем регулярные учебные тревоги, обучение конкретным действиям при пожаре дают максимальный эффект. Персонал школы должен быть ознакомлен с действием основных элементов технических средств безопасности, уметь с ними обращаться. Задача же технических средств – максимально быстро обнаружить возгорание и инициировать эвакуацию.

ЮНИТЕСТ
ОХРАННО-ПОЖАРНЫЕ СИГНАЛИЗАЦИИ

ООО «ТОРГОВЫЙ ДОМ «ЮНИТЕСТ»
Москва, ул. 15-я Парковая, д. 46 Б
тел.: 8-800-775-7879, (495) 988-3884
e-mail: info@unitest.ru
www.unitest.ru

ОБЗОР ОБОРУДОВАНИЯ

ПРИБОРЫ ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННО-ПОЖАРНЫЕ

ППКОП 019-4-1 «КОРУНД 2/4-СИ» ИСП.04 ВЗРЫВОЗАЩИЩЕННЫЙ НА 4 ШЛЕЙФА

Взрывозащищенный прибор пожарной и охранной сигнализации с 4 гальванически развязанными шлейфами, с видом взрывозащиты «Искробезопасная электрическая цепь "i" , «[Exia]IIC».

Напряжение в шлейфах 9 – 13 В. Ток питания извещателей не более 0,6 мА.

Выходы прибора:

- 5 релейных выходов (коммутируемые напряжение/ток)12 – 250 В/0,1 – 4 А;
- 2 выхода питания (10,8 – 17 В) оповещателей с контролем целостности цепи;
- выход питания внешних потребителей (10,8 – 17 В);
- гальванически развязанный канал связи RS-485;
- мощность, потребляемая от сети переменного тока 220 В, не более 10 ВА;
- потребляемый ток от аккумуляторного резервного питания не более 0,2 А;
- диапазон рабочих температур от -30 до +50 °С

Прибор позволяет программировать функцию каждого ШС как охранный или пожарный

ППКОП АДРЕСНЫЙ ВЗРЫВОЗАЩИЩЕННЫЙ «РАКИТА»

Прибор с одним адресным шлейфом сигнализации.

Напряжение в шлейфе 16 – 23 В. Ток питания извещателей, не более 3 мА.

Максимальное количество адресных извещателей 16.

Прибор обеспечен набором:

- размыкателей короткого замыкания шлейфа сигнализации,
- искробезопасными барьерами с гальванической развязкой и без гальванической развязки для включения адресных искробезопасных извещателей,
- расширителем адреса для подключения безадресных извещателей.

Выходы прибора :

- 3 программируемых релейных выхода (коммутируемые напряжение/ток) 12 – 250 В/0,1 – 4 А;
- 2 выхода питания оповещателей (10,8 – 17 В) с контролем целостности цепи.

Питание прибора от двух вводов постоянного тока 12 – 24 В, ток потребления, не более 250 мА

Двухпроводная линия связи упрощает монтаж и обслуживание системы.

ППКОП «СИГНАЛ 2/4-СИ» ИСП.04/06 НА 4 ШЛЕЙФА

Прибор пожарной и охранной сигнализации на 4 шлейфа.

Напряжение в шлейфах 16 – 23 В. Ток питания извещателей по каждому шлейфу, не более 2,5 мА.

Выходы прибора :

- 4 релейных выхода по каждому шлейфу (коммутируемые напряжение/ток) 12 – 250 В/0,1 – 4 А;
- 2 релейных выхода общих сообщений: "НЕИСПРАВНОСТЬ", "ПОЖАР".
- 2 выхода питания (10,8 – 17 В) оповещателей с контролем целостности цепи;
- выход питания внешних потребителей (10,8 – 17 В);
- гальванически развязанный канал связи RS-485.

Прибор обеспечивает световую индикацию состояния прибора и встроенной аккумуляторной батареи, звуковое оповещение, трансляцию тревожных извещений на ПЦН, выдачу стартового импульса на приборы управления пуском систем пожаротушения, дымоудаления, оповещения.

Специнформатика-СИ

ООО «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «Специнформатика-СИ»
115230, Москва,
Каширское шоссе, д.1 корп.2
тел: (499) 611-1586, (499) 611-5085
e-mail: specinfo@specinfo.ru
www.specinfo.ru

Специнформатика-СИ

ООО «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «Специнформатика-СИ»
115230, Москва, Каширское шоссе,
д.1 корп.2
тел: (499) 611-1586, (499) 611-5085
e-mail: specinfo@specinfo.ru
www.specinfo.ru

Специнформатика-СИ

ООО «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «Специнформатика-СИ»
115230, Москва, Каширское шоссе,
д.1 корп.2
тел: (499) 611-1586, (499) 611-5085
e-mail: specinfo@specinfo.ru
www.specinfo.ru

ДЛЯ МАЛЫХ ОБЪЕКТОВ

ПРИБОРЫ ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННО-ПОЖАРНЫЕ

ВЕРСЕТ-GSM 02

«ВЕРСЕТ–GSM 02» – прибор нового поколения: особо компактный корпус (110x105x40 мм), встроенный литиевый аккумулятор, работа с двумя SIM–картами, работа с Android-приложением.

Прибор передает информацию о состоянии объекта в виде SMS–сообщений на телефоны пользователей и на пультовую станцию мониторинга «ВЕТТА–50 GSM». Управляется с телефонов пользователей специальными SMS–сообщениями и с прибора с помощью электронных ключей и кодонаборных клавиатур серии «ПОРТАЛ».

Настройка прибора выполняется быстро и удобно с помощью компьютерной программы, поставляемой с прибором.

При тревоге прибор выдает звуковые и световые сигналы на оповещатели, подключенные к прибору.

Пожарные и охранные извещатели подключаются с помощью универсальных проводных шлейфов сигнализации.

Приборы обеспечивают сервисные функции, такие, как получение баланса счета СИМ-карты прибора, получение информации о состоянии охраны.

Для передачи прибором сообщений, ему может быть задано до 8 телефонных номеров. Сообщения прибора разделены на 8 групп. При настройке прибора выбираются группы сообщений, которые будут передаваться на телефоны пользователей.

Прибор оснащен внешним источником питания, который обеспечивает работу прибора от сети 110 – 240 В.

СИБИРСКИЙ АРСЕНАЛ

ООО НПО «СИБИРСКИЙ АРСЕНАЛ»
630073, Новосибирск,
микрорайон Горский, 8 А
тел.: (383) 240-8540
e-mail: info@arsenalnpo.ru
www.arsenal-sib.ru

ВЕРСЕТ–GSM 03 ВМ, ВЕРСЕТ–GSM 06 ВМ, ВЕРСЕТ–GSM 09 ВМ

Являются универсальными многофункциональными приборами для обеспечения безопасности на объектах. Приборы имеют все необходимые средства для того, чтобы организоват охрану от проникновения посторонних лиц в охраняемое помещение, пожарную охрану, но и контроль доступа в помещение (проход в помещение на основе электронных ключей, проксимити карт, паролей), работу с технологическими датчиками и управление оборудованием, контроль температуры в помещениях и другие важные функции безопасности.

Приборы могут передавать информацию о состоянии контролируемого объекта по GSM сети на телефоны пользователей, получать с телефонов команды управления, работать совместно с пультовой станцией мониторинга «ВЕТТА–50 GSM» для обеспечения централизованной охраны.

Приборы информируют о состоянии охраняемых объектов путем передачи речевых сообщений и/или отправки SMS–сообщений на телефоны сотовой связи, передачей речевых сообщений на телефоны фиксированной проводной связи, передачи специальных кодированных SMS сообщений на станцию мониторинга «ВЕТТА–50 GSM».

СИБИРСКИЙ АРСЕНАЛ

ООО НПО «СИБИРСКИЙ АРСЕНАЛ»
630073, Новосибирск,
микрорайон Горский, 8 А
тел.: (383) 240-8540
e-mail: info@arsenalnpo.ru
www.arsenal-sib.ru

ППКОПУ 01121-24-1 МИНИТРОНИК 8 (НА 4 ШС)

Предназначен для защиты помещений от несанкционированных проникновений и возгораний. Комфортное отображение информационных данных за счет наличия индикаторов неисправностей. Создания сети из приборов без применения дополнительного оборудования. Упрощенный механизм управления 2 клавишами либо электронными ключами. Не требует программирования. Архивация событий. Любые сложных варианты организации сигнализации. Упрощенный монтаж и сервисное обслуживание. Расширение до 8 ШС установкой дополнительной платы индикации.

Краткие характеристики:

- питание прибора от блока резервированного питания U=12 В;
- число выходов управления ОК (300 мА) и реле (до 5 А, до 220 В) – по 3;
- параметры длины пожарного ШС – до 2 км, охранного ШС – до 2,5 км;
- число датчиков на один ШС – до 20;
- число электронных ключей типа «Touch Memory» – 74;
- возможность удаления выносных считывателей – до 300 м;
- срок службы не менее – 10 лет.

ЮНИТЕСТ
ОХРАННО-ПОЖАРНЫЕ СИГНАЛИЗАЦИИ

ООО «ТОРГОВЫЙ ДОМ «ЮНИТЕСТ»
Москва, ул. 15-я Парковая, д. 46 Б
тел.: 8-800-775-7879, (495) 988-3884
e-mail: info@unitest.ru
www.unitest.ru

ОБЗОР ОБОРУДОВАНИЯ

ПРИБОРЫ ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННО-ПОЖАРНЫЕ

GSM-СИГНАЛИЗАЦИЯ ИПРО-6

Надежное решение для управления безопасностью и климатом вашего дома с помощью телефона.

Использует GSM и 433,92 мГц протоколы связи.

Возможность подключения до 110 проводных и беспроводных датчиков:

- движения;
- задымления;
- утечки газа;
- протечки воды;
- температуры;
- открытия/закрытия дверей и окон.

В совокупности с исполнительными устройствами, позволяет строить системы практически любой сложности с позонным контролем и управлением.

Может работать с 2 проводными и 6 беспроводными датчиками температуры. По контролю температуры - 2 режима. Настраиваемое оповещение хозяина при снижении температуры ниже установленной. А также управление котлом с мобильного телефона. При подключении беспроводных датчиков, каждому можно задать имя, что обеспечивает адресность. Вы будете точно знать какой датчик сработал. В приборе есть 2 силовых реле на 220В х 10 А к которым можно подключать силовые устройства и управлять ими. Также для удобства можно подключать до 16 беспроводных реле, радиоканальных розеток и управлять электроустройствами с телефона, без прокладки проводов от прибора до исполнительных устройств. Реализована техническая поддержка. Не дорогой прибор с хорошим функционалом.

ИПРО

ООО «ИПРо»(Инженерно-производственное объединение)
г. Рязань, ул. Зубковой, д. 8 А
тел. (4912)77-79-41; 8(804)333-90-80
e-mail: zakaz@ipro-gsm.ru
www.ipro-gsm.ru

ППКОП ВЭРС-ПК2 ТРИО-М ВЕРСИЯ 3.2

Предназначен для организации в офисах, квартирах, коттеджах, дачах, гаражах и других объектах пожарной сигнализации; охраны от проникновения; выдачи сигналов на технологическое оборудование; автоматического информирования пользователей по каналам GSM-голос, GSM-SMS, ГТС; автоматической передачи информации на мобильное приложение (платформы Android и iOS).

Технические характеристики:

- Исполнение от 2 до 24 ШС.
- Три выхода управления внешними оповещателями с током нагрузки до 1 А.
- Поддержка двух SIM-карт.
- Максимальное количество номеров телефонов до 72 (GSM-голос – 24, GSM SMS – 24, ГТС – 24).
- Возможность присваивать номер телефона пользователя к одному или нескольким ШС.
- Конфигурирование с помощью: кнопок прибора и сотового телефона, USB и персонального компьютера, Bluetooth и смартфона.
- Дистанционное управление или управление по расписанию: шлейфами сигнализации, реле, запрос баланса.
- Возможность подключения внешнего микрофона и трех термодатчиков.
- Задание пользовательских текстов SMS.
- Передача информации о ФИО владельца ключа ТМ при постановке/снятии ШС.
- Дистанционная установка времени.

ВЭРС

ООО «МПП ВЭРС»
630041 г. Новосибирск,
ул. 2-я Станционная, 30
тел.: (383) 304-8-204 многоканальный
тех. поддержка: 8-800-250-21-29
www.verspk.ru

ППКОП ВЭРС-ПК4 LAN ВЕРСИЯ 3.2

Прибор предназначен для работы в составе системы IP-ОПС ВЭРС-LAN. Система позволяет собирать, хранить информацию о состоянии множества приборов а также ими удаленно управлять и конфигурировать их с помощью ПО ВЭРС-LAN и персонального компьютера. Удаленный доступ к приборам через облачный сервер через персональный компьютер/смартфон на платформе Android или iOS. ПО ВЭРС – возможность работы с планами объектов для большей информативности и удобства обслуживания. Количество приборов в системе не ограничено.

Технические характеристики:

- Количество ШС от 2 до 24.
- Три выхода управления внешними оповещателями с током нагрузки 1 А.
- три реле ПЦН («Пожар», «Тревога», «Неисправность»).
- Магистраль RS-485 для подключения внешних блоков, расширяющих функционал прибора: ВЭРС-БМК (внешняя клавиатура); ВЭРС-БК (блок управления внешними оповещателям); ВЭРС-БРУ (внешний блок силовых реле).
- Управление кнопками и ключами ТМ до 250 шт.
- Исполнение со встроенным регистратором событий (ВЭРС-ПК-РС).
- Конфигурирование около сорока параметров.
- Исполнение в пластмассовом и металлическом корпусе.

ВЭРС

ООО «МПП ВЭРС»
630041 г. Новосибирск,
ул. 2-я Станционная, 30
тел.: (383) 304-8-204 многоканальный
тех. поддержка: 8-800-250-21-29
www.verspk.ru

ДЛЯ МАЛЫХ ОБЪЕКТОВ

ПРИБОРЫ ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННЫЕ

AJAX
HUB PLUS

Основой системы безопасности Ajax является интеллектуальная централь Ajax Hub Plus с расширенными коммуникационными возможностями.

Она контролирует работу до 150 охранных устройств Ajax и моментально оповещает о тревогах пользователей и охранную компанию, используя push-уведомления, SMS -сообщения и звонки. Оснащена четырьмя штатными каналами связи (Wi-Fi, Ethernet и две SIM-карты 2G/3G) для обеспечения максимально надежной коммуникации с охраняемым объектом.

Hub Plus может обеспечить комплексную безопасность большого объекта: загородного дома, магазина, офиса, производства, контролируя 150 датчиков, 50 камер видеонаблюдения и 25 групп охраны.

- Дальность связи с датчиками: до 2000 м на открытом пространстве.
- Двухсторонний радиопротокол: Jeweller (868,0 868,6 МГц или 868,7 – 869,2 МГц), с AES шифрованием.
- Каналы связи: Wi-Fi 2,4 ГГц, Ethernet, 2 слота Micro-SIM, сети 2G, 3G
- Максимальное количество пользователей: 50.
- Максимальное количество подключенных устройств: 100.
- Отклик датчиков проверяется пингами с периодом 12 – 300 секунд.
- Защита: от глушения, от перехвата, от подлога.
- Встроенный резервный аккумулятор: до 15 ч автономной работы.
- Программное обеспечение: обновляется бесплатно, автоматически.

ООО «Аджакс Системс»
г. Москва, ул. Рочдельская, д. 15,
стр. 17–18, 3-й этаж, офис 17
тел.: 8-800-500-41-05
e-mail: hello@ajax.systems
ajax.ru

ПКПО
НОРД GSM AIR

Компактная беспроводная панель с клавиатурой на корпусе: для постановки и снятия с охраны не нужны дополнительные устройства. К панели подключаются до 31 беспроводного устройства: охранные датчики, температурный и технологические датчики, реле и ретрансляторы. Предусмотрены два проводных шлейфа для датчиков и два дискретных выхода для проводной сирены и светового оповещателя.

В комплекте внешний блок питания 220 В, АКБ типоразмера 18650 и встроенная GSM-антенна. На плате встроенная GSM-антенна, разъем для выносной GSM-антенны и слот на две SIM-карты. Кнопки клавиатуры с подсветкой и звуковым подтверждением нажатия. Габариты – 150 х 96 х 33 мм.

Норд Air доступны все преимущества экосистемы Си-Норда – удаленное программирование, обновление прошивки через веб-интерфейс, в том числе массовое обновление сразу нескольких приборов. К панели подключаются устройства автоматизации, позволяющие управлять электрооборудованием на объекте через мобильное приложение. Панель позволяет поделить объект на 32 раздела, настроить управление для 32 пользователей. Дополнительно можно подключить 32 ТМ- или RFID-ключа.

Система защищена от взлома – при попытке вскрыть или разбить панель, на пульте появится тревожное событие «Вероятная тревога».

Панель работает со всеми типами беспроводного оборудования Си-Норда. Специально для Норд Air выпущены экономичные датчики ИК-Мини и СМК-Мини в малогабаритных корпусах.

ООО «НТКФ «Си-Норд»
190020, Санкт-Петербург,
наб. Обводного канала,
199 – 201, корпус 13 К
тел.: (812) 747-81-48
e-mail: sales@cnord.ru
cnord.ru

ПКПО
НОРД GSM MINI

Компактная проводная панель с клавиатурой на корпусе: для постановки и снятия с охраны не нужны дополнительные устройства. Подключаются 4 проводных охранных шлейфа или дискретных выхода с возможностью увеличения до 16 за счет внешнего расширителя.

В комплекте внешний блок питания 220 В, АКБ типоразмера 18650. На плате встроенная GSM-антенна, разъем для выносной GSM-антенны и слот на две SIM-карты.

Корпус из пластика, силиконовые кнопки клавиатуры с подсветкой и звуковым подтверждением нажатия. Габариты – 150 х 96 х 33 мм.

Для панели Норд Mini доступны все преимущества экосистемы Си-Норда – удаленное программирование, обновление прошивки через веб-интерфейс, в том числе массовое обновление сразу нескольких приборов, управление взятием/снятием и технологическими датчиками через мобильное приложение. Панель позволяет поделить объект на 32 раздела, настроить управление для 32 пользователей. Также дополнительно можно подключить 32 ТМ-или RFID-ключа.

Система защищена от взлома – если злоумышленник попробует вскрыть или разбить панель, на пульте появится тревожное событие «Вероятная тревога».

ООО «НТКФ «Си-Норд»
190020, Санкт-Петербург,
наб. Обводного канала,
199 – 201, корпус 13 К
тел.: (812) 747-81-48
e-mail: sales@cnord.ru
cnord.ru

СЕРИЯ ПРИБОРОВ «ВЕРСЕТ-GSM» ДЛЯ БЕЗОПАСНОСТИ МАЛЫХ ОБЪЕКТОВ

GSM-сигнализация – это комплекс оборудования, который передает тревожные сигналы по каналу мобильной связи, то есть GSM-сети. Такое оборудование может использоваться при организации охраны коттеджного поселка, группы офисных помещений или мини-магазинов, складских и производственных строений, гаражных комплексов.
Компания ООО «ВЕРСЕТ» разработала линейку беспроводного оборудования, обладающую всеми необходимыми параметрами для обеспечения безопасности этих объектов: ППКОП «ВЕРСЕТ-GSM 02», «ВЕРСЕТ-GSM 03 ВМ», «ВЕРСЕТ-GSM 06 ВМ», «ВЕРСЕТ-GSM 09 ВМ», адресный радиоканальный прибор «ВС-ПК ВЕКТОР-АР GSM-100» и станцию мониторинга «ВЕТТА-50 GSM».

ППКОП «ВЕРСЕТ-GSM 02»

«ВЕРСЕТ–GSM 02» - прибор нового поколения, характеризующийся особо компактным корпусом (110х105х40 мм) и встроенным литиевым аккумулятором, комфортной работой с Android-приложением. Цена прибора существенно ниже по сравнению с аналогичными по функционалу приборами. Вместе с тем «ВЕРСЕТ–GSM 02» является полноценным приемно-контрольным охранно-пожарным прибором, что подтверждается сертификатом соответствия требованиям технического регламента о требованиях пожарной безопасности.

К прибору подключаются охранные и пожарные извещатели с помощью двух универсальных проводных шлейфов сигнализации. Передача информации о состоянии контролируемого объекта и тревожных сообщений от прибора передается в виде SMS-сообщений на телефоны пользователей и на пультовую станцию мониторинга «ВЕТТА-50 GSM».

В случае возникновения тревожных ситуаций прибор также выдает звуковые и световые сигналы на оповещатели, подключенные к прибору.

Настройка ППКОП «ВЕРСЕТ-GSM 02» выполняется с помощью компьютерной программы, поставляемой с прибором. Для передачи сообщений может быть задано до 8 телефонных номеров, включая номера пользователей и номера станции мониторинга «ВЕТТА-50 GSM». Сообщения разделены на 8 групп. При настройке прибора можно выбрать определенные группы сообщений, которые будут передаваться на телефоны пользователей.

Управление ППКОП «ВЕРСЕТ-GSM 02» осуществляется с телефонов пользователей специальными SMS-сообщениями и непосредственно с самого прибора с помощью электронных ключей и кодонаборных клавиатур серии «ПОРТАЛ».

Прибор оснащен внешним источником питания, который обеспечивает его работу от сети с диапазоном напряжения 110–240 В. В качестве резервного источника питания используется размещенный внутри прибора литиевый аккумулятор. Источник питания прибора обеспечивает заряд аккумулятора в автоматическом режиме.

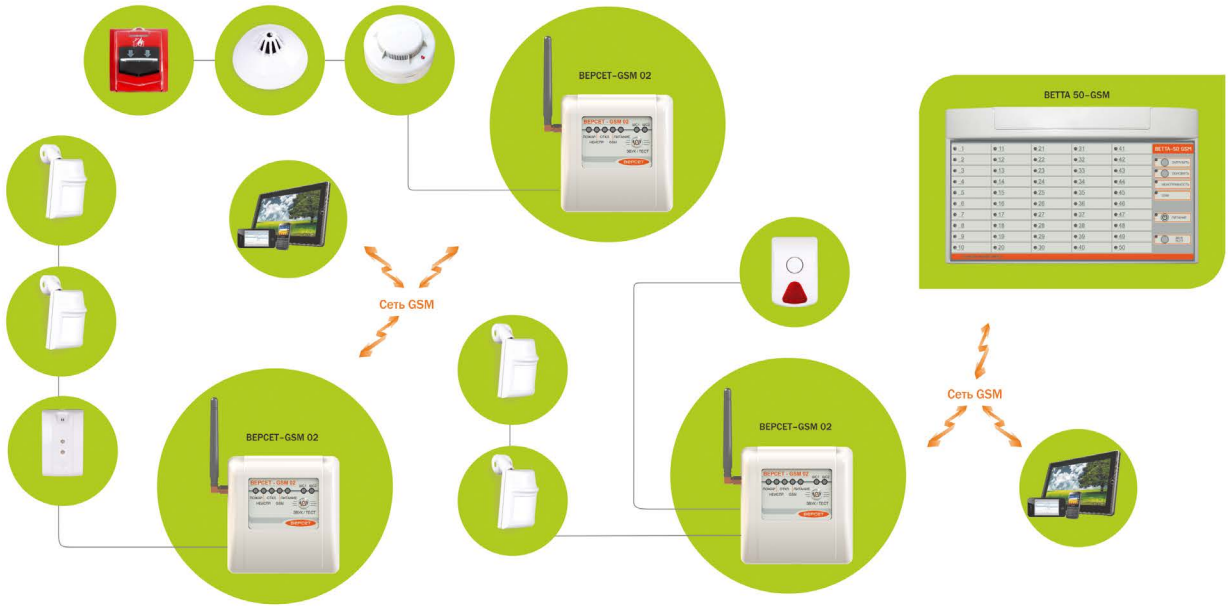
Кроме этого ППКОП «ВЕРСЕТ-GSM 02» имеет дополнительные сервисы, например такой, как получение на телефон пользователей баланса счета SIM-карты прибора.

ПК «ВЕКТОР-АР GSM-100»

Адресный радиоканальный прибор «ВС-ПК ВЕКТОР-АР GSM-100» обеспечивает эффективную защиту объектов от пожара и несанкционированного проникновения. Может работать совместно с радиоканальными извещателями, оповещателями и радиобрелками производства «ВЕРСЕТ».

Передача информации о состоянии контролируемого объекта, тревожных сообщений от прибора передается в виде SMS-сообщений на телефоны пользователей. Кроме этого ПК «ВС-ПК ВЕКТОР-АР GSM-100» осуществляет температурный контроль и передачу этой информации пользователю. Функция измерения температуры производится по трем каналам, что существенно расширяет возможности прибора, превращая его в универсального «помощника по дому».

Управление ПК «ВЕКТОР-АР GSM-100» можно осуществлять дистанционно с помощью команд с мобильного телефона:



ставить и снимать объект или одну его зону с охраны, делать различные запросы о состоянии объекта.

Помимо управления с телефона, прибор принимает команды с радиоканальных брелков, ключей ТМ, а также с помощью кодонаборных панелей – универсальных считывателей серии «ПОРТАЛ».

На корпусе прибора отображаются извещения «ПОЖАР» и «ТРЕВОГА», состояние охранных зон (поставлен/снят), информация о неисправности прибора. Эти данные могут передаваться с помощью реле на ПЦН. ПК «ВЕКТОР-АР GSM-100» имеет возможность передачи информации по GSM-каналу на станцию мониторинга «BETTA-50 GSM», что открывает возможность коллективной охраны группы объектов (дачного поселка, гаражного общества, квартир в подъезде и многого другого).

ППКОП «ВЕРСЕТ-GSM 03 ВМ», «ВЕРСЕТ-GSM 06 ВМ», «ВЕРСЕТ-GSM 09 ВМ»

Приборы приемно-контрольные охранно-пожарные являются универсальными многофункциональными приборами для обеспечения безопасности на объектах. В отличие от ППКОП «ВЕРСЕТ-GSM 02», кроме охранно-пожарных функций приборы данной серии имеют ряд дополнительных функций: работу с технологическими датчиками и управление оборудованием, контроль температуры в помещениях и другие важные функции безопасности. Кроме этого прибор осуществляет функцию контроллера. Это позволяет организовать на объекте контроль доступа в помещения. Проход в помещение осуществляется с помощью электронных ключей, проксимити-карт, паролей.

Приборы серии «ВЕРСЕТ-GSM...ВМ» осуществляют передачу информации о состоянии контролируемого объекта по GSM-сети на телефоны пользователей и могут получать с телефонов команды управления, работать совместно с пультовой станцией мониторинга «BETTA-50 GSM» для обеспечения централизованной охраны. Информация о состоянии объекта может передаваться в виде речевых сообщений и/или отправки SMS-сообщений. Передача речевых сообщений происходит на телефоны фиксированной проводной связи, передача специальных кодированных SMS-сообщений на станцию мониторинга «BETTA-50 GSM».

СТАНЦИЯ МОНИТОРИНГА «BETTA-50 GSM»

Станция мониторинга – мини пультовая система «BETTA–50 GSM» предназначена для организации простой, быстро разворачиваемой системы охраны объектов, охраняемых с помощью приборов серий «ВС-ПК ВЕКТОР-АР GSM-100», «ВЕРСЕТ-GSM», «ВЕРСЕТ-ДОМ», сигнализаторов серии «Express GSM». Все эти устройства имеют режим работы со станцией мониторинга «BETTA-50 GSM».

Принцип работы станции мониторинга: «BETTA-50 GSM» получает по GSM-каналу информацию в виде SMS-сообщений о состоянии объектов от объектовых приборов и отображает эти данные на световых индикаторах. Одному индикатору соответствует один прибор. Станция может контролировать состояние до 50 приборов.

Закрепление за станцией объектовых приборов и задание параметров работы станции выполняется с помощью SMS-сообщений. Те же действия могут быть реализованы с помощью компьютерной программы «КОНФИГУРАТОР». Станция с помощью этой программы сохраняет события в специальном журнале, который можно просмотреть по необходимости.

В ЗАКЛЮЧЕНИЕ

Преимуществом оборудования компании «ВЕРСЕТ» является его возможность отправлять информацию об объекте не только на телефоны пользователей, но и на общий пульт – станцию мониторинга «BETTA-50 GSM», что в свою очередь позволяет оперативно отслеживать состояние объектов как владельцам, так и организации, осуществляющей централизованную охрану. А возможность управления приборами при помощи SMS-сообщений (для прибора «ВЕРСЕТ-GSM 02» и с помощью приложения для мобильных устройств) дает возможность оперативно реагировать на нестандартные ситуации.

Еще одно преимущество оборудования компании «ВЕРСЕТ»: при использовании GSM-сети нет ограничения по дальности установки объектовых приборов от станции мониторинга «BETTA-50 GSM».

СИБИРСКИЙ АРСЕНАЛ

ООО НПО «СИБИРСКИЙ АРСЕНАЛ»
630073, Новосибирск,
микрорайон Горский, 8 А
тел.: (383) 240-8540
e-mail: info@arsenalnpo.ru
www.arsenal-sib.ru

ВОПРОСЫ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ И ПАРАМЕТРОВ РАДИОТРАКТА ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Зайцев Александр Вадимович
научный редактор журнала «Алгоритм безопасности»

НОРМЫ

ЧТО ТАКОЕ ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ?

Беспроводные системы пожарной сигнализации появились на российском рынке более 15 лет назад. Их преимущества перед проводными неоспоримы. Это и экономия на монтаже, и быстрота установки и модернизации, и исключение работ, нарушающих интерьер. Казалось бы, они должны были уже давно завоевать рынок. Особенно, это касается объектов малого и среднего бизнеса, жилищной сферы, временных некапитальных построек и много другого. Но – не произошло. И основным препятствием, на настоящий момент, является наличие серьезных сомнений у заказчиков в надежности их работы в реальных условиях. В области же пожарной безопасности надежность является ключевым и обязательным критерием. И многие заявления производителей остаются только на бумаге, неподтвержденные какими-то конкретными показателями инструментальной проверки. По моему мнению, основная проблема в том, что в области пожарной безопасности не решены вопросы контроля степени защищенности по электромагнитной совместимости (ЭМС) техническими средствами, проходящими сертификацию, а следовательно, данная техническая характеристика носит декларативный характер. Но сейчас ситуация на европейском рынке меняется, желательно, чтобы она изменилась и у нас.

Не буду скрывать, я тоже, как и многие специалисты, долгое время в своей практической работе старался обходить стороной вопросы, касающиеся электромагнитной совместимости (ЭМС). С одной стороны, они первоначально мне даже казались не настолько актуальными, чтобы ими интересоваться, с другой стороны, я тогда даже не представлял себе, как их можно и нужно решать при разработке и конструировании технических средств.

Что подразумевается под вопросом электромагнитной совместимости? Термин уж больно сложен для поверхностного понимания, особенно для людей, далеких от разработки и конструирования электронных систем. Приведу для пояснения парочку примеров из жизни моего старенького телевизора, который когда-то жил вместе со мною.

Почему-то вдруг по утрам примерно в одно и то же время на экране телевизора вместо нормальной картинки появлялась масса черно-белых тонких полос по диагонали на весь экран, а вместо речи диктора жужжал какой-то моторчик. Оказывается, у одного моего пожилого соседа была любимая бритва «Харьков» доисторических времен, а в ее сетевой вилке был выкушен пробитый искрогасящий конденсатор. Высокочастотная наведенная помеха распространялась по сети электропитания и воздействовала на телевизоры всего дома. Кто виноват, бритва или слабая защищенность телевизора от этого вида помех? А сколько проблем до-

ставляли и даже сейчас доставляют люминесцентные светильники производства нашего восточного соседа.

При частичном повреждении телевизионного кабеля примерно такая же помеха может попасть в телевизор, но другим путем – через его антенный вход. Это уже второй тип помех.

Синтетический палас или линолеум в квартире – вроде ничего страшного. Там походили, тут походили. После чего стоит прикоснуться к этому любимому телевизору, как между ним и вами проскакивает искра. Статика. Но эта статика может вывести из строя, как минимум, большую часть органов управления, после чего этот телевизор придется нести в ателье ремонта. И это тоже ЭМС.

А ведь когда-то производились ламповые телевизоры, которые после очередного ремонта невозможно было даже разместить в одной комнате, они мешали друг другу нормально работать. Т.е. они не только были чувствительны к внешним электромагнитным помехам, так еще и сами создавали эти помехи другим.

Вот и пришлось во всем мире вводить жесткие нормы как на излучение электромагнитных помех, так и на защищенность от них.

Сейчас в нашей стране действует порядка 200 как национальных, так и межгосударственных стандартов в области ЭМС. Немного существует областей технического регулирования, в которых есть такое глубокое и широкое нормирование.

Для того, чтобы можно было охарактеризовать уровень излучения электромагнитных помех от того или иного оборудования или в тех или иных помещениях, было введено такое понятие, как степень жесткости. Чем выше уровень помех, тем выше эта степень. В свою очередь, оборудование, на которое оно могло влиять, стало характеризоваться степенью защищенности по ЭМС.

Кстати, именно заниженная степень защищенности по ЭМС у технических средств пожарной сигнализации по отношению к имеющейся на объекте степени жесткости является наиболее частой причиной ее ложных срабатываний. Об этом и о том, как решаются эти проблемы за рубежом, на страницах данного издания уже было размещено достаточное количества статей.

При большом желании, можно практически полностью исключить излучение всяких помех от электроинструмента, всякого рода светильников, бытовых электроприборов и т.п. Но беспроводные радиоканальные системы управления и сигнализации по определению должны и излучать электромагнитные сигналы, и соответственно их принимать, при этом, на их работу не должны влиять как другие источники электромагнитных помех, так и они не должны мешать нормальному функционированию других систем, в т.ч. и беспроводных. А вот это уже почти на грани фантастики. Для одновременной работы всех беспроводных систем должны применяться достаточно жесткие меры по обеспечению электромагнитной совместимости между ними.

БЕСПРОВОДНЫЕ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Как я уже упомянул в самом начале, вот уже почти пятнадцать лет на нашем отечественном рынке присутствуют беспроводные системы пожарной сигнализации. За это время у нас в стране появилось более десятка производителей, поставляющих эти системы.

Чем отличаются отечественные беспроводные системы пожарной сигнализации между собою, по каким техническим параметрам их можно сравнить?

А можно ли сравнивать наши отечественные системы с зарубежными аналогами?

Ни на один из этих двух вопросов ответить пока не представляется возможным. Нет никаких объективных данных у отечественных систем. Максимум, что пишут в эксплуатационной документации, дальность действия у кого-то – 300 м на открытом интервале, а кто-то заявляет более 1000 м. Чем это объясняется, и почему такая разница, даже специалисту не всегда понятно. А какой был рельеф трассы между устройствами при проведении этих экспериментов, какова подстилающая поверхность, на какой высоте были размещены приемопередатчики? А в течение какого периода времени проверялась эта радиолиния, сколько попыток понадобилось для передачи одного пакета данных? И таких условий проведения экспериментов – масса.

Но нас интересуют и возможности работы этих систем не только в чистом поле, а в окружении других источников электромагнитного излучения. На одном и том же объекте могут одновременно использоваться как беспроводные система охранной сигнализации, так и пожарной. А под окнами дети будут управлять своими танками и вездеходами. И это все на фоне объектовой системы Wi-Fi.

Чтобы что-то сравнивать, нужно иметь инструментально полученные данные о всех составляющих энергетического потенциала радиоинтервала, в том числе, и имеющихся методов снижения необходимого запаса на быстрые и медленные затухания сигнала, чтобы достигнуть требуемой устойчивости работы, «чистоты» и стабильности параметров излучаемого сигнала, защищенности приемного тракта не только по радиоканальной части, но в тракте цифровой обработки принимаемых сигналов.

В действующем национальном стандарте ГОСТ Р 53325-2012 «Техника пожарная. Технические средства пожарной автоматики», также как и в его предшественнике редакции от 2009 года, какие-либо требования к беспроводным устройствам по их характеристикам радиотракта полностью отсутствуют.

СИСТЕМА ЕВРОПЕЙСКОГО НОРМИРОВАНИЯ ЭМС В ЗАРУБЕЖНЫХ СПС

В отличие от нашей страны в европейской системе стандартизации в 2008 году смогли принять так необходимый для этого документ. Это EN 54-25 «Fire detection and fire alarm systems – Part 25: Components using radio links» («Системы пожарной сигнализации. Часть 25. Компоненты, использующие радиосвязь»).

В нем появились некоторые параметры, по которым уже можно было судить о пригодности тех или иных систем к практическому использованию. К ним относятся:

- Устойчивость к ослаблению сигнала с учетом методов снижения резерва ослабления.
- Рабочие характеристики ресивера:
  a) избирательность по соседнему каналу;
  b) блокировка и снижение чувствительности при уходе частоты радиопередачи от рабочей частоты;
  c) подавление ложных сигналов.
- Доступность радиолиний в двух или более технически схожих системах, представленных одним производителем.
- Доступность радиолиний при наличии других пользователей полосы частот, т. е. совместимость с другими пользователями полосы частот для многоканальных и одноканальных компонентов.
- Не была забыта и электромагнитная совместимость (ЭМС) и испытания на устойчивость (при эксплуатации). Испытания на устойчивость к ЭМС регламентировалось проводить согласно EN 50130-4 (очень хороший и важный стандарт). В них входили:
  a) электростатический разряд;
  b) излучение электромагнитного поля;
  c) помехи, вызываемые электромагнитными полями;
  d) помехи от быстрых переходных процессов;
  e) медленные всплески высокой энергии;
  f) питание от сети с изменением напряжения;
  g) питание от сети с падением напряжения и короткими перерывами.

И все эти испытания в указанном объеме проводилось вплоть до начала 2018 года. Но в Европе уже давно зрели перемены. В редакции EN 54-25 от

2008 года уже была ссылка на EN 300 220-1 V 1.3.1:2000, «Electromagnetic compatibility and Radio spectrum Matters (ERM) – Short range devices – Radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW – Part 1: Technical characteristics and test methods» («Электромагнитная совместимость и радиочастотный спектр (ERM) – Устройства ближнего радиуса действия – радиооборудование, используемое в диапазоне частот от 25 МГц до 1000 МГц с уровнями мощности до 500 МВт – Часть 1: Технические характеристики и методы испытаний»). Но даже в редакции от 2008 года в этом документе требований было не так уж много. Всего на нескольких страничках приведены особенности радиоканала в режиме «прежде чем включить передачу, послушай», который у нас называется множественным доступом с контролем несущей (МДКН), и два вида широкополосной модуляции.

Вся беда заключается в том, что всякие беспроводные системы управления, передачи и т.п. за эти годы просто заполонили весь мир. Особенно в этом преуспели производители одной очень большой страны на Востоке. А в отсутствии всяких на это стандартов у них там никто и не задумывался, чем этот неуправляемый процесс в итоге может закончиться.

Дистанционное открывание автомобиля или гаражных ворот. Управление шторами в доме или детский луноход. Управление домашней автоматикой и прочими устройствами для малоподвижных групп населения. Электронная няня у ребенка, и тут же компоненты или охранной, или пожарной сигнализации. Я уже не буду упоминать десятки и даже сотни модификаций радиостанций Walkie-Talkie, многие из которых можно купить в магазинах детских товаров.

Настало время от игрушек и систем сигнализации для дома, для семьи перейти к жесткому нормированию параметров компонентов всех этих беспроводных систем.

И в 2018 году в Евросоюзе для всех радиоустройств ближнего действия стала обязательной новая редакция европейского стандарта от 2017 года – ETSI EN 300 220-1 V3.1.1 (2017-02) «Short Range Devices (SRD) operating in the frequency range 25 MHz to 1000 MHz; Part 1: Technical characteristics and methods of measurement» («Приборы ближнего действия (SDR), работающие в диапазоне частот от 25 МГц до 1000 МГц; Часть 1: Технические характеристики и методы измерений»).

И этот документ уже не на 14 страничках, как его предыдущая редакция, а на 74-х. Все стало очень серьезно, и теперь с радиоканалом так просто не «забалуешь».

ЧТО ТАКОЕ ETSI EN 300 220-1 V3.1.1 (2017-02)?

Этот стандарт нельзя в полной мере отнести к стандартам по ЭМС. Это стандартизация основных параметров для находящихся в обращении беспроводных средств, независимо от использования диапазона частот (лицензируемый или нелицензируемый). И этими испытаниями занимаются совсем другие аккредитованные испытательные лаборатории, нежели чем ТС охранной или пожарной безопасности.

С момента вступления в силу этого стандарта, прежде чем подать на сертификацию беспроводную систему пожарной сигнализации по EN 54-25, сначала надо получить документы соответствия данному стандарту, наравне с производителями или поставщиками других беспроводных устройств и систем, а уже потом и общие параметры систем проверять по назначению.

Какие параметры подлежат проверке на соответствие стандарту ETSI EN 300 220-1 V3.1.1. Вот неполный перечень подлежащих проверке параметров:

- номинальная рабочая частота передающего устройства и занимаемая полоса;
- эффективная излучаемая мощность;
- максимальная эффективная спектральная плотность излучаемой мощности;
- стабильность рабочей частоты передающего устройства;
- суммарный уровень внеполосных излучений передающего устройства;
- излучение передающего устройства по соседнего частотному каналу;
- изменение параметров передающего устройства в условиях пониженного напряжения;
- работа адаптивного регулятора излучаемой мощности;
- чувствительность приемного тракта;
- селективность приемного устройства по соседнему каналу;
- насыщение приемника по соседнему каналу;
- работоспособность при высоком уровне принимаемого сигнала;
- корректность при выхода на связь в режиме «прежде чем включить передачу, послушай» (МДКН);
- корректность при выходе на связь в режиме «прежде чем включить передачу, послушай» (МДКН) по временным интервалам;
- адаптивная перестройка частоты;
- двухнаправленная проверка функционирования.

Измерили параметры, сравнили с требованиями национальных стандартов или требований, и после этого можно идти в свою целевую испытательную лабораторию по назначению прибора.

Радиочастотный спектр во всем мире является точно таким же национальным достоянием, как воздух или вода. Все имеют право этим достоянием пользоваться, но никто не имеет право наносить ущерб другим. Поэтому радиочастотный спектр и все, что его использует, подлежит регулированию, даже приборы ближнего радиуса действия (SDR).

Почему один производитель выпускает беспроводные устройства для диапазона 433 МГц с выходной мощностью не более 10 мВт, как то требует положение ГКРЧ, а другой производитель ставит перемычку, сняв которую, уже можно вместо положенных 10 мВт получить все 100 мВт в нарушении действующих требований. Только делается это немного хитрее. С завода устройство уходит с установленной перемычкой, но в руководстве по эксплуатации пользователю предлагается самому, в случае необходимости, ее снять. Вроде ответственность перекладывается на пользователя, но нарушителем здесь является однозначно производитель, который создал все условия для нарушения и подтолкнул на это пользователя.

И вот это все должно однозначно пресекаться.

ОТЕЧЕСТВЕННОЕ НОРМИРОВАНИЕ ЭМС ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ

Решением Комиссии Таможенного союза от 09.12.2011 № 879 был утвержден перечень стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента Таможенного союза «Электромагнитная совместимость технических средств» (ТР ТС 020/2011).

В данном перечне, помимо всего прочего, был стандарт Республики Беларусь СТБ EN 300 220-1-2011 (ETSI EN 300 220-1: 2008, NEQ) «Электромагнитная совместимость и радиоспектр. Устройства радиосвязи малого радиуса действия (SRD). Радиооборудование в полосе частот от 25 до 1000 МГц с уровнем мощности до 500 мВт. Часть 1. Технические характеристики и методы измерения».

Этот стандарт является полным аналогом европейского варианта и уже упоминался здесь в связи с наличием его в СТБ EN 54-25:2008.

Но в перечне еще был национальный стандарт ГОСТ Р 52459.3-2009 (ЕН 301 489-3-2002) «Совместимость технических средств электромагнитная. Технические средства радиосвязи. Часть 3. Частные требования к устройствам малого радиуса действия, работающим на частотах от 9 кГц до 40 ГГц» (MOD).

И таких частей с частными или особыми требованиями существует сейчас порядка 32-х для различных источников радиоизлучения.

Еще недавно этот стандарт базировался на требованиях национального

стандарта ГОСТ Р 52459.1-2009 (ЕН 301 489-1-2008) «Совместимость технических средств электромагнитная. Технические средства радиосвязи. Часть 1. Общие технические требования и методы испытаний» (MOD). Но с 01.01.2014 его заменил межгосударственный стандарт ГОСТ 32134.1-2013 (EN 301 489-1:2008) «Совместимость технических средств электромагнитная. Технические средства радиосвязи. Часть 1. Общие технические требования и методы испытаний» (MOD).

Часть стандартов серии ГОСТ Р 52459 после переработки постепенно переходит в межгосударственные стандарты серии ГОСТ 32134.

Таким образом, с 2011 года для устройств радиосвязи малого радиуса действия можно было руководствоваться или переводным стандартом СТБ EN 300 220-1-2011, или национальным стандартом ГОСТ Р 52459.3-2009.

Но решением коллегии Евразийская экономической комиссии от 03.02.2015 № 8, стандарт СТБ EN 300 220-1-2011 (ETSI EN 300 220-1: 2008, NEQ) был исключен.

Теперь в новом перечне присутствуют только ГОСТ 32134.1-2013 (EN 301 489-1:2008) и опирающийся на него ГОСТ Р 52459.3-2009 (ЕН 301 489-3–2002).

Почему так произошло, история умалчивает.

Как видно, все эти стандарты являются некими модификациями европейских стандартов серии EN301 489 от 2008 года. В то же время в Европе уже давно действуют другие, более жесткие варианты этих стандартов:

- ETSI EN 301 489-1 V2.1.1:2017-02;
- ETSI EN 301 489-3 V2.1.1:2017-03.

И вот тут стоит обратить внимание на даты версий европейского стандарта EN 301 489-3-2002, который у нас в обрезанном и модифицированном виде взят за основу, и ныне действующего в европейской системе стандарта ETSI EN 301 489-3-2017. Разница между ними составляет всего 15 лет. Именно в этот промежуток времени беспроводные системы быстро развивались и завоевывали рынок. Только наши специалисты по стандартизации этого как-то не заметили.

А следовательно, не учтены новые версии стандартов серий EN 301 489 и европейский стандарт для приборов ближнего радиуса действия (SDR) нового поколения ETSI EN 300 220-1. В итоге оказались между стульями, т.е. на полу. А ситуация с беспроводными системами может в любой момент выйти из под контроля, и в стране возникнет «беспроводный» хаос.

Время простеньких беспроводных устройств для дома, для семьи уже прошло, с ними давно все ясно. Но уже вовсю создаются и применяются серьезные беспроводные системы. И складывается такое впечатление, что у нас в стране до сих пор мало кто понимает: в современном мире к всем этим системам должны быть уже совсем другие требования, а пользователи должны быть уверены, что эти устройства и системы готовы без каких-либо проблем решить стоящие перед ними задачи. И это возможно только путем инструментальной проверки на основании современных стандартов. А пока приходится верить на слово производителям, но мы все знаем, чем обычно это заканчивается.

«ЮМИРС» 25 ЛЕТ!

В этом году ЗАО «ЮМИРС» – разработчик и производитель технических средств охраны периметра, отмечает свой серебряный юбилей – 25-летие.

Компания уверенно идет вперед, постоянно совершенствуя свое производство и повышая качество продукции, внедряя новейшие технологии охраны периметра. Продукция ЗАО «ЮМИРС» хорошо известна в России и далеко за ее пределами, отмечена многочисленными наградами, дипломами и грамотами.

Торжественная часть по случаю юбилея прошла на аэродроме «Сосновка». Выбор места не случаен, президент компании Клюев Андрей Валентинович увлекается экстремальными видами спорта. В 2017 году экспедиция ЗАО «ЮМИРС» под его руководством проходила в Приэльбрусье, члены экспедиции поднялись на высоту 4500 метров над уровнем моря. В этом году на аэродроме 14 сотрудников совершили прыжки с парашютом и 10 полетов на планерах.

Поздравить руководство компании и сотрудников приехали представители администрации г. Пенза – заместитель Председателя Пензенской области Беспалов В.Н., министр промышленности, транспорта и инновационной политики Пензенской области Торгашин М.Н., член Правления «Российского союза промышленников и предпринимателей», председатель совета директоров ЦеСИС Шаповал О.Л.

На торжественной церемонии присутствовали представители компаний-партнеров.

СИСТЕМА ЭКСТРЕННОЙ ДВУСТОРОННЕЙ ГОЛОСОВОЙ СВЯЗИ «ЯНА»

Система обратной связи зон пожарного оповещения с помещением пожарного поста-диспетчерской.

ООО «НПП «ОМЕГА САУНД», продолжая развивать направление объектовых систем экстренной связи, разработала новую систему двусторонней связи «ЯНА» для небольших бюджетных объектов.

НАЗНАЧЕНИЕ СИСТЕМЫ

Двунаправленная полудуплексная система голосовой (речевой) экстренной связи (СГС) серии «ЯНА» позволяет выполнять следующие требования федеральных законов и нормативных актов:

- обеспечивает обратную связь с зонами пожарного оповещения для систем оповещения и управления эвакуацией в СОУЭ 4–5 типов согласно СП 3.13130.2009;
- обеспечивает двустороннюю речевую связь безопасных зон с дежурным персоналом (диспетчером) и организацию связи для людей с ограниченными физическими возможностями (МГН) согласно СП 59.13330.2016.

СГС «ЯНА» ПРЕДНАЗНАЧЕНА ДЛЯ ИСПОЛЬЗОВАНИЯ

Администрацией здания на начальном этапе эвакуации. СГС «ЯНА» позволяет диспетчеру получать оперативную информацию о месте возгорания, распространении ОФП, процессе эвакуации и передавать управляющие команды лицам, ответственным за эвакуацию в зонах пожарного оповещения;

Пожарными и другим ответственным персоналом в процессе эвакуации во время чрезвычайных ситуаций в высотных зданиях или на больших территориальных объектах, где работа радиосвязных средств не может гарантироваться из-за влияния строительных конструкций и интерференции радиоволн.

Пожарными после завершения эвакуации. Пожарные могут продолжать использовать систему после завершения эвакуации, для координирования своих действий в процессе тушения пожара.

Маломобильными группами населения (МГН), которые не могут эвакуироваться самостоятельно. Люди, укрывшиеся в зонах безопасности и ожидающие помощи, должны иметь возможность связаться с персоналом, отвечающим за эвакуацию, для идентификации своего местонахождения и получения инструкций о дальнейших действиях. В соответствие с СП 59.13330.2016, СГС «ЯНА» позволяет осуществлять вызов и двустороннюю голосовую связь с дежурным персоналом. Абонентские устройства обладают повышенной громкостью, а надписи на лицевых панелях продублированы тактильным шрифтом Брайля.

ОСОБЕННОСТИ СИСТЕМЫ

- Двунаправленная полудуплексная система голосовой связи. Для разговора с диспетчером абоненту не требуется нажатие и удержание кнопки.
- Максимальное количество абонентов в системе – 32.
- Автоматическая самодиагностика и контроль исправности компонентов системы, межблочных соединений и линий связи с абонентскими устройствами позволяют существенно упростить процедуру технического обслуживания.
- Вывод информации о состоянии системы на пульт диспетчера и во внешние цепи мониторинга.

РАСПРЕДЕЛЕННАЯ СТРУКТУРА СГС «ЯНА»

Кабельные линии СГС «ЯНА» проектируются в основе радиальной топологии «линия»/«звезда». Технологии связи пульта диспетчера с блоками коммутации, в комбинации с топологией подключения линий абонентских устройств, обеспечивают масштабную экономию кабеля и не требуют специального помещения для размещения стойки с центральной аппаратурой.

Максимальное удаление от пульта диспетчера до абонента составляет 1500 м.

СОСТАВ СИСТЕМЫ

В состав системы входят три основных компонента: пульт диспетчера, блок коммутации и абонентское устройство. Для удовлетворения требований заказчика, функциональных возможностей, конструктивного исполнения и дизайна, каждый из компонентов имеет несколько модификаций. Применяемые инженерные решения в конструкции корпуса пульта диспетчера обеспечивают настенную и настольную установку. Абонентские устройства имеют металлический вандалозащищенный корпус для настенного накладного или врезного монтажа. Степень защиты оболочки абонентских устройств – IP54. По отдельному заказу защита оболочки может быть поднята до IP65.

Система двусторонней полудуплексной голосовой связи «ЯНА» разработана и производится в России, на научно-производственном предприятии «ОМЕГА САУНД» в Санкт-Петербурге.

ООО «ОМЕГА САУНД»
197022, Санкт-Петербург,
Каменноостровский пр., д. 57-2 Н
тел.: (812) 346-0790,
факс: (812) 346-0789
e-mail: info@omegasound.ru
www.omegasound.ru

БКП380/Р — НОВОЕ УСТРОЙСТВО ДЛЯ КОНТРОЛЯ ИСПРАВНОСТИ СИЛОВЫХ ЛИНИЙ СВЯЗИ СПЗ

В основе большинства проектов пожарной защиты зданий и сооружений заложены исполнительные устройства, основным элементом которых являются электродвигатели. В данной статье речь пойдет именно о контроле исправности реверсивных электроприводов типовых задвижек системы пожаротушения и других устройств, основой которых является мощный трехфазный электродвигатель 220/380 В. Проблема заключается в том, что на этапе проектирования функциям контроля исправности линий связи с электродвигателем, исправности катушек пускателей, а также самого двигателя и концевых выключателей уделяется недостаточно внимания. Как следствие, надежность системы пожарной защиты падает. Одной из причин этого является недоступность такой возможности из-за отсутствия готовых решений. Для решения данной задачи группой компаний «Гефест» было разработано устройство БКП380/Р.

Блок контроля и пуска БКП380/Р предназначен для контроля исправности линий связи и состояния удаленного исходно выключенного трехфазного электродвигателя 220/380 В, направление вращения которого задается коммутацией фаз сети. Обмотки двигателя могут быть соединены треугольником или звездой без нейтрального провода. БКП380/Р не осуществляет самостоятельное управление двигателем. Команду на запуск двигателя он принимает от переключающихся контактов стороннего ППУ.

Устройство выполнено в компактном пластиковом корпусе со степенью защиты IP30, конструктивные особенности которого позволяют легко осуществлять монтаж как на DIN-рейке 35 мм, так и на другой поверхности саморезами. Рекомендуется осуществлять монтаж в электротехническом шкафу на DIN-рейку. Устройство является дополнительным компонентом (работает в составе ППУ «Гефест» или другого ППУ), его легко можно подключить к уже имеющимся системам противопожарной защиты. Монтаж следует осуществлять в соответствии с проектной документацией.

БКП380/Р имеет встроенную индикацию, возможность подключения внешней индикации, а также информационные выходы. Устройство осуществляет контроль наличия трех фаз, состояние каждой из них отображается зеленым цветом на индикаторах L1, L2, L3. При монтаже в шкафу устройство позволяет разместить на двери шкафа лампы индикации (220 В) состояний контролируемого устройства («Открыто», «Закрыто», «Неисправность», «Автоматика»), а также элементы управления, такие как переключатель режима (ручной/автоматический), кнопки ручного перевода привода в положение «Открыто»/«Закрыто», кнопки «Стоп» и «Сброс». Информационные выходы представляют собой сухой контакт для передачи состояний на пожарный пост. В дежурном режиме контакты информационных выходов для передачи состояний «Открыто» и «Неисправность» замкнуты, контакты для состояний «Закрыто» и «Пуск» разомкнуты.

ДЕЖУРНЫЙ РЕЖИМ

Основным режимом работы БКП380/Р является дежурный режим. Устройство находится в дежурном режиме при условии включенного режима «Автоматический» и отсутствии каких-либо неисправностей. В данном режиме привод находится в крайнем состоянии (разомкнут концевой выключатель), которое условно считается положением «Открыто» (положения «Открыто» и «Закрыто» для БКП380/Р равнозначны).

Блок контроля и пуска БПК380/Р

Устройством осуществляется контроль на обрыв проводов:

- От пускателей до двигателя, а также самих обмоток двигателя. Рекомендуется подключать контрольные цепи БКП380/Р именно к выходным клеммам пускателя для исключения неконтролируемых участков внутри шкафа.
- Замкнутых контактов концевых и моментных выключателей привода.
- Исходно разомкнутых контактов моментных выключателей привода.
- Цепей катушек пускателей открытия и закрытия.

Контроль перечисленных выше цепей осуществляется непрерывно с момента ввода устройства в эксплуатацию, благодаря этому при возникновении внештатной ситуации будет немедленно сформирован сигнал «Неисправность» для информирования дежурного персонала. Важно отметить, что контроль обмоток электродвигателя осуществляется малым током 1,2 мА, при напряжении не более 15 В. За счет контроля низким напряжением, даже случайное касание оголенных контактов электродвигателя в дежурном режиме будет безопасно для жизни человека. Длина проводов до привода не влияет на функции контроля.

РЕЖИМ «ПУСК»

Устройство переходит в режим «Пуск» по команде от стороннего ППУ при переключении контактов пускового реле.

В режиме «Пуск»:

- включается пускатель закрытия, начинается движение привода;
- включается встроенный индикатор состояния «Пуск» и замыкаются контакты информационного выхода «Пуск»;
- по замыканию концевого выключателя положения «Открыто» выключается встроенный индикатор состояния «Открыто», снимается напряжение с внешней индикаторной лампы состояния «Открыто» и размыкаются контакты информационного выхода «Открыто».

По достижении приводом крайнего положения «Закрыто» (по размыканию концевого выключателя положения «Закрыто»):

- двигатель останавливается;
- включается встроенный индикатор состояния «Закрыто», подается напряжение на внешнюю индикаторную лампу состояния «Закрыто», на информационном выходе «Закрыто» замыкаются контакты.

В случае необходимости остановки электродвигателя во время движения, можно воспользоваться внешней кнопкой «Стоп», это позволит остановить двигатель в нужный момент.

РУЧНОЙ РЕЖИМ

Помимо автоматического режима, БКП380/Р можно перевести в ручной режим переключателем выбора режима автоматики. В данном режиме отключается автоматика и пуск двигателя от стороннего ППУ невозможен, двигателем можно управлять только вручную внешними кнопками «Открыто», «Закрыто» и «Стоп». При переходе в данный режим формируется сигнал «Неисправность» на встроенных и внешних индикаторах, осуществляется информирование дежурного персонала на пожарном посту о нештатной работе системы (размыкание контактов информационного выхода «Неисправность»).

БЛОКИРОВКА ПУСКА

В случае необходимости, например, для проведения регламентных работ, обслуживающий персонал может полностью заблокировать пуск двигателя. Блокировка включается установкой переключателя выбора режима работы устройства в среднее положение или путем установки перемычки (тумблера) на соответствующие клеммы устройства. Также к клеммам «Блокировка пуска» можно подключить кнопку «Стоп», в зависимости от требований объекта. Стоит обратить внимание, что при включенной блокировке пуска БКП380/Р формируется сигнал «Неисправность», благодаря этому исключена вероятность, что обслуживающий персонал забудет перевести устройство в дежурный режим, так как на пожарный пост будет сформирован сигнал «Неисправность» и дежурный персонал будет своевременно проинформирован.

РЕЖИМ «НЕИСПРАВНОСТЬ»

В режиме «Неисправность» становится невозможно автоматическое движение двигателя в любом направлении.

Устройство переходит в режим «Неисправность» при возникновении хотя бы одной из следующих ситуаций:

- отсутствие напряжения хотя бы в одной из фаз сети;
- подача напряжения одновременно на катушки пускателей «Открыто» и «Закрыто» в результате неверной коммутации или в ручном режиме;
- при обрыве в цепи подключения замкнутых моментных и концевых выключателей;
- при обрыве в цепи подключения разомкнутых моментных выключателей, используемых для индикации;
- в дежурном режиме выявлен обрыв подводящего провода от выходных контактов пускателя до обмоток двигателя, самих обмоток или цепей катушек пускателей;
- заклинивание двигателя в начальном положении (нет замыкания концевого выключателя положения «Открыто» по команде «Пуск» в течении 4 секунд) или заклинивание двигателя в процессе движения (нет размыкания концевого выключателя положения «Закрыто» по истечении 64 секунд);
- включение ручного режима или блокировки пуска.

Режим «Неисправность» является самоблокирующимся, таким образом выйти из него можно только по команде «Сброс». При переходе в режим «Неисправность» осуществляется индикация состояния на встроенном и внешнем индикаторах, формирование обобщенного сигнала «Неисправность» на пожарный пост, благодаря чему дежурный персонал будет своевременно осведомлен о неполадках в системе пожарной защиты. Далее персонал, осуществляющий обслуживание системы, при помощи детальной индикации на самом устройстве БКП380/Р сможет с легкостью установить, чем именно вызвана данная неполадка в системе.

БКП380/Р соответствует требованиям ГОСТ Р 53325-2012 и обеспечивает функции автоматического контроля:

- на обрыв линии от пускателя до обмоток двигателя, а также самих обмоток двигателя;
- на обрыв замкнутых контактов концевых и моментных выключателей электродвигателя и разомкнутых контактов моментных выключателей электродвигателя;
- наличия напряжения в каждой из трех фаз сети питания на входе пускателя.

ВЫВОД

Таким образом БКП380/Р представляет собой простое в эксплуатации устройство с информативной индикацией, которое полностью решает проблему контроля исправности линий связи и самого реверсивного привода с трехфазным электродвигателем в системах противопожарной защиты. В качестве элементной базы устройства используются только качественные комплектующие, что гарантирует долговечность и надежность работы устройства в период эксплуатации.

ГРУППА КОМПАНИЙ «ГЕФЕСТ»
Санкт-Петербург,
Сердобольская ул., д.65 А
тел.: (812) 600-6911
www.gefest-spb.ru

АСПИРАЦИЯ. ЧАСТЬ 1
ОПЫТЫ С ХЛОПКОМ

Неплохов Игорь Геннадьевич
к.т.н., технический директор ООО «Пожтехника»

Аспирационные пожарные извещатели в настоящее время широко используются для защиты атриумов, складов, центров обработки данных, информационно-вычислительных центров, и т.д. В общем случае их чувствительность на несколько порядков выше точечных дымовых извещателей (ИПДОТ). Однако эффективность обнаружения малых концентраций дыма различных очагов в значительной степени зависит от типа измерителя оптической плотности среды. В своде правил СП 5.13130 [1] п. 13.1.1 есть рекомендация: «Выбор типа точечного дымового пожарного извещателя рекомендуется производить в соответствии с его чувствительностью к различным типам дымов». В большей мере это требование относится к аспирационным пожарным извещателям, которые в ГОСТ Р 53325-2012 [2] по чувствительности разделены на классы А, В и С. Однако, как правило, информация по чувствительности аспирационных извещателей дается в общем виде, без дифференциации по типам очагов и по размерам частиц дыма. Кроме того, нет полной ясности относительно степени «старения» дыма в трубе аспирационного извещателя длиной порядка 100 м и более.

ОБОРУДОВАНИЕ

Значительное влияние на чувствительность точечных дымовых пожарных извещателей оказывает величина аэродинамического сопротивления дымозахода. Поэтому их испытания по стандартным тестовым очагам ТП-2–ТП-5 проводятся в помещении площадью 70 м^2, на расстоянии 3 м от очага [2]. Если в дымовом канале, с принудительным воздушным потоком, ИПДОТ срабатывает при удельной оптической плотности порядка 2,5 %/м (0,11 дБ/м), то на тестовых очагах при низких скоростях воздушных потоков сработка при в 10 раз большем задымлении, порядка 20 %/м (1 дБ/м), считается хорошим результатом. У аспирационных извещателей проблема аэродинамического сопротивления отсутствует, так как производится принудительный отбор проб воздуха через отверстия в трубе при использовании аспиратора. Следовательно, для определения эффективности различных измерителей оптической плотности аспирационных извещателей огневые испытания можно проводить без использования специальных помещений. Для оценки работы аспирационного извещателя в реальных условиях большее значение имеет наличие трубы и ее длина. Считается, что дым вблизи очага состоит из частиц меньшего размера, по сравнению с дымом на большом расстоянии от очага. Со временем частицы дыма сталкиваются друг с другом, слипаются и увеличивается их размер. Если за время транспортировки по трубе частицы дыма успевают «состариться», то реакция аспирационного извещателя на дым, поступающий в начало трубы и в конец трубы, должна быть различной. Исходя из данных предпосылок, в экспериментах будут использоваться трубы различной длины с формированием очагов минимальных размеров вблизи одного воздухозаборного отверстия в трубе, преимущественно вблизи отверстия в заглушке трубы.

В первой части опытов используется труба длиной порядка 100 м, состоящая из четырех горизонтальных участков примерно по 24 м с восемью поворотами на 90° (*рис. 1*). В трубе имеются 16 воздухозаборных отверстий диаметром Ø3 мм, расположенных на расстоянии 6 м друг от друга и на расстоянии 3 м от поворотов. В заглушке имеется отверстие диаметром Ø6 мм. Очаг располагается вблизи отверстия в заглушке, через остальные отверстия в трубе поступает чистый воздух.

Для данной конфигурации трубы при обеспечении аспиратором разрежения порядка 350 Па аэродинамический расчет определяет суммарную величину воздушного потока около 65 л/мин., время транспортировки порядка 86 с (класс В), величина воздушного потока через отверстие в заглушке примерно

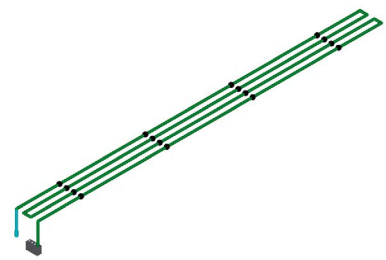


Рис. 1. *Конфигурация трубы аспирационного извещателя. Точками обозначены отверстия в трубе*

6,6 л/мин., что составляет 10,1% суммарного воздушного потока. Соответственно дым, поступающий через отверстие в заглушке, разбавляется чистым воздухом через остальные отверстия в трубе примерно в 10 раз. При увеличении разрежения до 760 Па, по расчету суммарная величина воздушного потока возрастает до 97 л/мин. Воздушный поток через отверстие в заглушке увеличивается до 10,8 л/мин., что составляет 11,1% суммарного воздушного потока. При этом расчетное время транспортировки сокращается до 59 с (класс А). Вычисленные значения немного отличаются от полученных экспериментально, поскольку при расчете в структуре трубы не были учтены дополнительные вставки отрезков труб, в которых были просверлены отверстия, за счет этого реально труба имеет большую длину и в 2 раза большее количество муфт, что повышает турбулентность воздушного потока.

ТЕСТОВЫЕ ОЧАГИ

Один из стандартных тестов по ГОСТ Р 53325-2012 для дымовых извещателей – тление хлопковых фитилей со свечением. При тлении хлопка отсутствует этап развития очага, тление фитиля происходит линейно во времени, что удобно при проведении опытов. Кроме того, наблюдается достаточно хорошая стабильность дымовыделения хлопкового фитиля, что позволяет проводить сравнение результатов экспериментальных исследований, проведенных в разное время с измерителями оптической плотности разного типа. Используется свечной хлопковый фитиль, который состоит из 10 ниток (*рис. 2*), что позволяет формировать различные концентрации дыма. Удельная оптическая плотность дыма при тлении фитиля, по сравнению с тлением одной нитки увеличивается примерно в 4 раза, а не в 10 раз, как, казалось бы, должно было быть на первый взгляд. Нитки в фитиле плотно скручены, за счет чего скорость тления снижается примерно в 2,5 раза, по сравнению со скоростью тления одной нитки. В результате чего, в единицу времени фитиль из 10 ниток образует примерно в 4 раза больше дыма по сравнению с одной ниткой.

Для поступления дыма только в отверстие заглушки трубы и для исключения распространения дыма в помещении, хлопковый фитиль помещается в коробку размером 255 х 95 х 95 мм с открытой нижней стенкой (*рис. 3*). Заглушка трубы с воздухозаборным отверстием диаметром Ø6 мм соединена с верхней стенкой коробки (*рис. 4*). Таким образом, при тлении фитиля или нитки, весь дым поднимается в верхнюю часть коробки и затягивается в трубу.

Благодаря достаточно большому сечению коробки воздушный поток, поступающий в отверстие в заглушке, практически не оказывает влияния на режим тления фитиля и не отличается от тления в свободном пространстве. Для изменения режима тления фитиля он помещается в металлическую трубку с внутренним диаметром Ø10 мм длиной 90 мм (*рис. 5*), в которой формируется воздушный поток со скоростью около 2,5 м/с. Увеличение притока кислорода к очагу вызывает повышение его температуры, о чем говорит увеличение яркости свечения фитиля. Соответственно изменяется структура дыма, предположительно при этом выделяются частицы дыма меньшего размера. Так же за счет воздушного потока примерно на 20% повышается скорость тления фитиля и, соответственно, увеличивается дымовыделение.

После определения основных закономерностей при тлении хлопкового фитиля в различных режимах, с образованием частиц дыма различного диаметра и трубами различной длины, планируется исследование широкого спектра очагов: перегрев кабеля различной длины, резисторов, тление брусков дерева и ДСП, тление ПВХ кабель-каналов и труб из полиэтилена, поролона, паласа, линолеума и т.д. В отличие от тления хлопкового фитиля при нагреве различных материалов на электоплитке режим тления и характеристики дыма изменяются в процессе развития очага при изменении температуры нагрева. Что создает дополнительные сложности при проведении экспериментов.

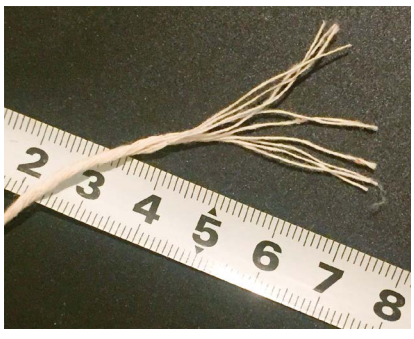


Рис. 2. *Хлопковый фитиль свит из 10 ниток*

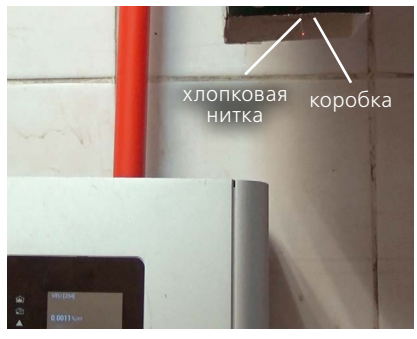


Рис. 3. *Тление хлопковой нитки в коробке*

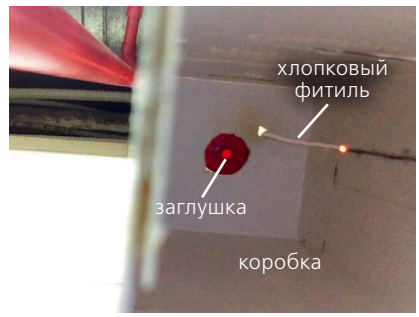


Рис. 4. *Тление хлопкового фитиля в коробке (вид снизу)*

Рис. 5. *Тление хлопкового фитиля в трубке Ø10 мм*

СЕРИЯ ОПЫТОВ 1

Первая серия опытов проводится с использованием измерителя удельной оптической плотности среды с коротковолновым лазером, с длиной волны не более 460 нм (0,46 мкн).. На *рисунке 6* приведен график изменения удельной оптической плотности при тлении одной хлопковой нитки. Несмотря на то, что при тлении хлопка развития очага нет, т.е. с начала до конца тления нитки в трубу через отверстие в заглушке поступает постоянное количество дыма, на выходе трубы наблюдается не скачкообразное, а плавное нарастание концентрации дыма. Происходит это из-за того, что скорость воздушного потока в сечении трубы не постоянная. В трубе аспирационного извещателя, так же как в воздуховодах, воздушный поток, проходящий по центру, имеет максимальную скорость, а ближе к стенкам скорость снижается. Соответственно, дым в трубе «растягивается», сначала в аспирационный извещатель поступает тонкая струйка дыма, протянутая аспиратором по центру трубы. Затем постепенно подтягиваются слои дыма, двигающиеся с меньшими скоростями вблизи стенок трубы, и происходит плавное увеличение концентрации дыма. Одновременно из-за движения дыма с различными скоростями происходит перемешивание дыма по всей длине трубы, в результате чего значительно снижается эффект «клубления» дыма, который всегда присутствует при развитии стандартных тестовых очагов в помещении.

Концентрация дыма в дежурном режиме до начала испытаний была на уровне 0,0012–0,0015 %/м, первые признаки

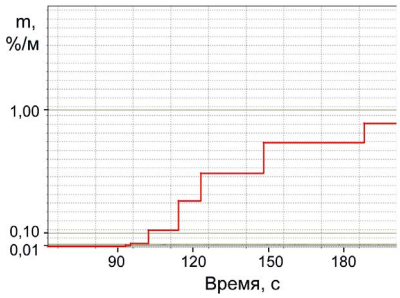


Рис. 6. *Оптическая плотность дыма при тлении хлопковой нитки*

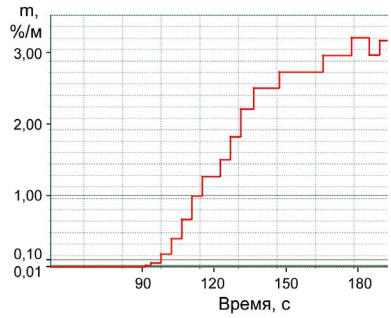


Рис. 7. *Оптическая плотность дыма при тлении хлопкового фитиля*

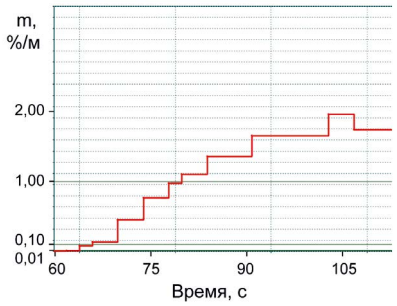


Рис. 8. *Оптическая плотность дыма при тлении хлопкового фитиля с повышенной мощностью аспиратора*

дыма на уровне 0,0058 %/м появляются через 90 с от размещения тлеющей нитки в коробке, время транспортировки до сработки порога «Внимание» на уровне 0,01 %/м равно 93 с. Через 60 с после появления дыма удельная оптическая плотность достигает уровня 0,8 %/м.

На *рисунке 7* приведен график изменения удельной оптической плотности во времени при тлении хлопкового фитиля. Концентрация дыма в дежурном режиме до начала испытаний была на уровне 0,0013–0,0017 %/м. Здесь также наблюдается плавное нарастание концентрации дыма, первые признаки дыма на уровне 0,0062 %/м появляются через 90 с, время транспортировки до сработки порога «Внимание» на уровне 0,01 %/м равно 91 с. Примерно через 60 с после появления дыма удельная оптическая плотность достигает уровня 2,8 %/м, что в 3,5 раза больше по сравнению с тлением нитки.

Ниже приведены результаты испытаний с тлением хлопкового фитиля (*рис. 8*)

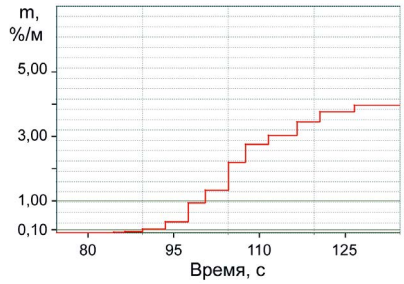


Рис. 9. *Оптическая плотность дыма при тлении хлопкового фитиля в трубке*

при увеличении разрежения аспиратора до 760 Па. Это позволяет реально сократить время транспортировки до 64 с. Расчетная величина воздушного потока через отверстие в заглушке увеличивается до 10,8 л/мин. Измеренный воздушный поток аспиратора повышается в 1,4 раза, с 66,4 л/мин. до 94,6 л/мин. При этом скорость тления фитиля остается прежней, и прохождение большего воздушного потока через отверстие в заглушке приводит к пропорциональному снижению концентрации дыма.

На *рисунке 9* приведен график изменения удельной оптической плотности при тлении хлопкового фитиля в трубке с внутренним диаметром Ø10 мм при разрежении аспиратора 350 Па. Первые признаки дыма на уровне 0,0075 %/м появляются через 80 с, время транспортировки до сработки порога «Внимание» на уровне 0,01 %/м равно 86 с.

Можно отметить повышение измеренной величины концентрации дыма примерно до 3,9 %/м, что почти в 1,4 раза больше по сравнению с тлением хлопкового фитиля в коробке. Это объясняется увеличением скорости тления фитиля и, соответственно, выделением большего объема дыма при наличии воздушного потока в трубке порядка 2,5 м/с. Необходимо отметить, что в случае использования измерителя с синим лазером, с длиной волны не более 460 нм, воздействие дыма с частицами меньшего размера не приводит к снижению чувствительности.

СЕРИЯ ОПЫТОВ 2

Вторая серия опытов проводилась с измерителем оптической плотности среды, выполненным на базе точечного дымового пожарного извещателя со свето- и фотодиодами инфракрасного диапазона. Кроме того, имеется полупроводниковый сенсор монооксида углерода CO, что позволяет определить соотношение аэрозолей и газов при движении дыма по трубе аспирационного извещателя. Длина трубы, количество отверстий и диаметры отверстий остаются без изменений.

На *рисунке 10* приведен график изменения оптической плотности и концентрации CO при тлении одной хлопковой

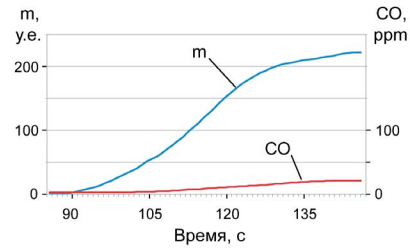


Рис. 10. *Оптическая плотность дыма и концентрация CO при тлении хлопковой нитки*

нитки в коробке. Как и в первом опыте, наблюдается исключительно плавное нарастание концентрации дыма и монооксида углерода на выходе трубы длиной 100 м. Отсутствие дискретизации объясняется значительно меньшим дискретом измерений, порядка 1 с. Концентрация дыма в дежурном режиме до начала испытаний равна 0 условных единиц, концентрация монооксида углерода на уровне 3,3–3,5 ppm. Первые признаки появления дыма, на уровне 2–4 условных единиц, наблюдаются примерно через 90 с от размещения тлеющей нитки в коробке. Время транспортировки по уровню вероятности пожара 10% около 97 с, а минимальные изменения концентрации CO, до 4 – 5 ppm, появляются только через 105 – 107 с, т.е. с задержкой на 15 – 17 с относительно появления дыма (*рис. 10*). Совершенно очевидно, что продукты тления хлопка со свечением в виде твердых частиц, аэрозолей и газов поступают в трубу аспирационного извещателя одновременно. При движении в трубе дым «растягивается», и минимальные концентрации эти составляющих одновременно достигают измерителя оптической плотности и измерителя концентрации CO. Однако за счет более низкого фона и большей чувствительности измерителя оптической плотности изменения концентрации дыма фиксируются значительно раньше. Таким образом, мультикритериальные возможности при совместной обработке этих двух факторов могут быть реализованы только при значительных концентрациях дыма.

На *рисунке 11* приведен график изменения оптической плотности и концентрации CO при тлении хлопкового фитиля в

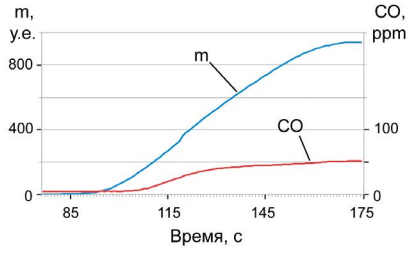


Рис. 11. *Оптическая плотность дыма и концентрация CO при тлении хлопкового фитиля*

коробке. Концентрация дыма в дежурном режиме на уровне 0 – 1 условных единиц, концентрация монооксида углерода 4,2 – 4,7 ppm. Первые признаки появления дыма, на уровне 3 – 5 условных единиц, наблюдаются примерно на 5 с раньше по сравнению с предыдущим тестом за счет большей концентрации дыма в отверстии в заглушке. Время транспортировки по уровню 10% около 93 с. Уровни концентрации CO порядка 5–7 ppm появляются только через 101–105 с, т.е. с задержкой на 16–20 с относительно появления дыма (*рис. 11*). К этому времени оптическая плотность дыма увеличивается до 92–143 условных единиц. Через 175 с рост концентрации дыма прекращается, достигнув оптической плотности, равной 943 условным единицам, и концентрации CO, равной 51,6 ppm.

Увеличить мощность данного аспиратора не представляется возможным ввиду технических ограничений, по этой причине в отличие от опыта 1 сразу переходим к тлению фитиля в трубке.

На *рисунке 12* приведен график изменения удельной оптической плотности и концентрации CO при тлении хлопкового фитиля в трубке с внутренним диаметром Ø10 мм. Концентрация дыма в дежурном режиме до начала испытаний равна 0 условных единиц, концентрация монооксида углерода на уровне 2,4 – 2,6 ppm. Первые признаки появления дыма, на уровне 3–5 условных единиц, наблюдаются примерно через 96 с от начала теста, что объясняется значительно более низким уровнем измеренной оптической плотности. Время транспортировки по уровню 10% около 102 с. Концентрация CO возрастает до 5 – 7 ppm через 108 с, т.е. с задержкой на 12 с относительно появления дыма (*рис. 12*), к этому времени оптическая плотность дыма увеличивается до 48 – 52 условных единиц.

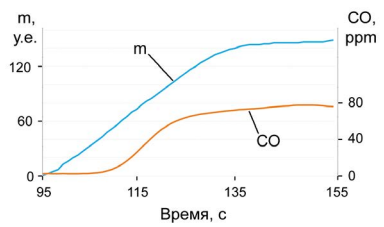


Рис. 12. *Оптическая плотность и концентрация CO при тлении хлопкового фитиля в трубке*

Примерно через 150 с от начала теста, или через 45 с от появления первых признаков дыма, рост оптической плотности и концентрации CO замедляется, достигнув уровней 147 условных единиц и 77,7 ppm соответственно. По сравнению с тлением фитиля в коробке концентрация CO увеличилась примерно в 1,5 раза, что может быть объяснено более интенсивным тлением хлопка. Но при этом измеренная оптическая плотность снизилась более чем в 6 раз, несмотря на повышение интенсивности тления фитиля. Этот эффект требует более тщательного рассмотрения в дальнейшем. Вероятно, здесь наблюдается резкое падение чувствительности оптико-электронного измерителя инфракрасного диапазона с длиной волны порядка 950 нм (0,95 мкн) по дымам с размерами частиц менее 0,5 – 1 мкн. При сравнении чувствительности точечных дымовых извещателей различных диапазонов отмечалось, что на частицах дыма диаметром менее 0,2 мкн интенсивность рассеяния инфракрасного света в 15 раз ниже интенсивности рассеяния синего света [3].

В следующих частях статьи будут изложены результаты проведения аналогичных опытов с хлопком при использовании измерителей оптической плотности других типов. Также будет развиваться тема с различными режимами тления хлопкового фитиля, при различных скоростях воздушных потоков, с трубками различного диаметра. Для исключения из рассмотрения эффекта «старения» дыма в трубах длиной 50 – 100 м с временем транспортировки 60–120 с будет проведено сравнение с результатами испытаний с длиной трубы порядка 7 м, с временем транспортировки около 10 с.

ПРЕДВАРИТЕЛЬНЫЕ ВЫВОДЫ

1. Дым в трубе аспирационного извещателя «растягивается». При скачкообразном повышении оптической плотности среды на входе трубы, на входе трубы наблюдается постепенное увеличение концентрации дыма. Время нарастания концентрации дыма сравнимо с временем транспортировки дыма.

2. Время транспортировки проб воздуха по трубе аспирационного извещателя сокращается при повышении чувствительности измерителя оптической плотности среды и при воздействии большей концентрации дыма.

3. При прохождении дыма через трубу аспирационного извещателя происходит перемешивание объемов дыма, поступающих в трубу в различные интервалы времени, что снижает до минимума эффект «клубления» дыма.

4. Высокая чувствительность измерителя оптической плотности среды в аспирационном извещателе определяет задержку обнаружения изменения концентрации монооксида углерода при тлении хлопка на 15 – 20 с, что значительно снижает эффективность использования мультикритериальных алгоритмов.

5. Тление хлопкового фитиля при разных скоростях воздушного потока обеспечивает формирование дымов с различными диаметрами частиц, что позволяет проводить сравнение эффективности измерителей оптической плотности различного типа.

ЛИТЕРАТУРА

1. Свод правил СП 5.13130 «Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования».

2. ГОСТ Р 53325-2012 «Техника пожарная. Технические средства пожарной автоматики. Общие технические требования. Методы испытаний».

3. Неплохов Игорь. Развитие дымовых извещателей // Грани безопасности. 2008. № 5 (53).

НОВОСТИ

- Axis Communications объявила о том, что самые популярные линейки камер компании для транспортной сферы получили сертификат ФКУ НПО «СТиС» МВД России. Сертификация регламентирует список продукции, которая соответствует требованиям и стандартам качества Постановления Правительства Российской Федерации № 969 от 26.09.2016 по обеспечению транспортной безопасности. Продукты серий Axis M11, M20, P12, P14, Q16, M30, M31, P31, P33, P39, получившие сертификацию, способны решить все задачи с которыми сталкиваются службы безопасности на государственных и коммерческих объектах транспортной инфраструктуры. Большой спектр технологий видеоаналитики дает возможность настроить камеры в зависимости от задачи: от фиксации номера автомобиля при пересечении им пешеходного перехода на красный свет и до распознавания лиц в больших залах аэропортов.

О НЕКОТОРЫХ ВОПРОСАХ НОРМАТИВНОЙ БАЗЫ ОХРАНЫ ЧАСТЬ 2

О ТЕРМИНОЛОГИЧЕСКОЙ НЕРАЗБЕРИХЕ ИЛИ О ПРИНЦИПИАЛЬНО РАЗНОМ ПОНИМАНИИ ИСБ

Петрушков Сергей Васильевич
к.т.н., полковник милиции в отставке,
старший научный сотрудник ФКУ НИЦ «ОХРАНА»

Продолжение статьи, первая часть которой была опубликована в №2-2018 журнала «Алгоритм безопасности».

В Росстандарте в рамках общероссийского классификатора стандартов ОКС 13.310 «**Защита от преступлений**...» работают сразу два технических комитета:

- ТК 234 «Системы тревожной сигнализации и противокриминальной защиты», созданный 06.05.1999. Секретариат – ФКУ «НИЦ «Охрана» Росгвардии;
- ТК 439 «Средства автоматизации и системы управления», созданный 18.09.2000. Секретариат – Международная ассоциация «Системсервис».

При этом ТК 439 был создан на год позже. По факту эти комитеты работают не очень согласованно, что привело к появлению сходных по названию, но принципиально отличающихся по своей сути стандартов. Остановимся на этом поподробнее.

ТК 234 ГОСТ Р 57674-2017 «ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ. ОБЩИЕ ПОЛОЖЕНИЯ»

Главная претензия автора (Зайцев А.В. Алгоритм безопасности. 2018. № 4) к этому документу заключается в том, что, по его мнению, ни одну из базовых систем, используемых во вневедомственной охране, нельзя отнести к системам безопасности. А коль скоро это так, то и сам термин «интегрированная система безопасности» охраной используется неправомерно. Попробуем и мы разобраться с принадлежностью этих базовых систем.

Системы охранной сигнализации (СОС) выполняют охранную функцию. С этим можно согласиться, но с одной оговоркой, о которой ниже.

Системы тревожной сигнализации (СТС) автор тоже относит к охранным с весьма неожиданной аргументацией:

«Очень часто имеет место отнесение СТС к системам безопасности. Но это неверное и ошибочное суждение. В первую очередь тревожными кнопками оборудуют всевозможные кассы. И если кассир добровольно согласится отдать при угрозе ограбления имеющиеся у него в наличии денежные средства, то ни у кого и в мыслях не будет его ни бить, ни убивать. Если нужно защитить эти денежные средства, то необходимо использовать технические средства инженерной укрепленности, в банках на этот счет имеется огромный опыт. Т.е. СТС, так же как и другие, относится к охранным системам».

Но, во-первых, даже если кассир согласится добровольно отдать деньги, то это отнюдь не будет означать, что угроза его жизни и здоровью автоматически миновала. Кому-то может не понравиться оставшийся в живых свидетель. Так что **тревожная** сигнализация о нападении будет у кассира совсем не лишней.

Во-вторых, тревожную сигнализацию не следует подменять технической укрепленностью. Это разные вещи, призванные взаимно дополнять друг друга.

В-третьих, кнопки тревожной сигнализации наиболее массово устанавливаются вневедомственной охраной отнюдь не в банках, у которых зачастую имеются свои службы безопасности, а прежде всего в школах, детских садах, поликлиниках, больницах и т.п. И именно в целях **обеспечения безопасности** больших и маленьких наших граждан от террористических, экстремистских и прочих противоправных действий. И используются эти

кнопки человеком в случае опасности, грозящей ему или окружающим.

Так что СТС, безусловно, относится именно к системам безопасности.

Но и это еще не все. На самом деле и СОС, и СТС – это одна и та же система. Разница лишь в том, как будут запрограммированы шлейфы сигнализации (ШС) и какое в ШС будет установлено оборудование. От охранных ШС сигнал тревоги на пульте будет интерпретирован как «несанкционированное проникновение». А от тревожного ШС как «нападение» и с наивысшим приоритетом из-за прямой угрозы жизни или здоровью (**безопасности!**) граждан.

С моей точки зрения следовало бы объединить СОС и СТС под общим названием **система тревожной сигнализации**. Де-факто это нашло отражение и в названии технического комитета ТК 234. Не знаю, кому и зачем пришла в голову мысль разделить эти понятия. Только из-за «тревожных кнопок»?

Системы контроля и управления доступом (СКУД) автор также относит к охранным, но с еще более странной аргументацией:

«До внедрения СКУД с древних времен существовало ограничение доступа в те или иные помещения с помощью замков и ключей к ним. Одна «бабка-ключница» чего стоит, а ведь она носила ключи от мест хранения съестных припасов, и ни о какой такой безопасности и слыхом не слышала. Тоже охранная функция».

То есть ограничение доступа является охранной функцией потому, что «бабка-ключница» не имела представления о безопасности?! Да очень даже имела бабка об этом представление, хотя в те времена могла и не знать такого слова. И именно с этой целью «закрома родины» на ключ и запирала. От греха подальше! А вот для **охраны** этих «закромов» у входа ставили стрельца-охранника. И о принципиальном отличии этих понятий как процессов мы еще поговорим в третьей части этой статьи.

И главное предназначение СКУД – ограничение доступа в **неохраняемые** помещения. Поэтому СКУД – это прежде всего повышение уровня безопасности и контроля находящихся в помещении людей, а также хранения информации, ноу-хау, коммерческих тайн и т.п.

Я готов согласиться с тем, что современные СКУД могут выдать на диспетчерский пульт сигнал тревоги в случае взлома входной двери. Если, конечно, дверь оборудована соответствующим датчиком. Но предназначение этого датчика для СКУД состоит прежде всего в том, что, во-первых, он подтверждает открытие двери в помещение после разрешения прохода туда. А, во-вторых, он фиксирует факт закрытия двери после того, как проход состоялся. Поэтому выдача сигнала тревоги в случае взлома двери является всего лишь дополнительным технологическим бонусом, который нельзя рассматривать в качестве полноценной охранной функции по крайней мере по двум причинам:

- в этом случае обеспечивается защита только одного рубежа охраны без учета всех остальных, а они, как правило, тоже имеются;
- взлом входной двери в рабочее время на глазах у изумленной публики (а как правило именно в это время помещения не находятся под охраной) представляется весьма странным и маловероятным событием. Тем более, что в это время и в самих помещениях с большой долей вероятности тоже могут находиться люди.

Тем не менее я с удовольствием поддержу довод о том, что эта функция повышает **уровень безопасности** находящихся в помещении людей.

Системы охранные телевизионные (СОТ). Здесь в технических умах тоже царит некоторая неразбериха. И я разделяю мнение автора, но только высказанное не в этот раз и по другому поводу.

Под заголовком СОТ с точки зрения классификации процессов взаимодействия «человек-машина» собраны как минимум три разных класса систем:

а) **охранное телевидение**, где камера по сути является оптическим пассивным охранным извещателем (новый термин?), который выдаст сигнал тревоги на пульт для последующего реагирования в случае изменения исходной условно статической картинки (или какой-то заранее выделенной ее части);

б) **видеонаблюдение (видеомониторинг)**, где сигналы с камер поступают на мониторы диспетчеров, наблюдающих за обстановкой на территории (объекте), и записываются на соответствующие носители данных. При этом системы с видеоаналитикой на борту тоже могут настраиваться на выдачу сигналов тревоги по заранее заданным условиям;

в) **видеорегистрация** (по сути «черный ящик»), где картинка с камеры только записывается в видеорегистратор для последующего «разбора полетов» в случае необходимости.

Здесь сначала надо навести порядок с классификацией и только затем определяться с принадлежностью. Но очевидно, что видеонаблюдение (видеомониторинг) и видеорегистрация применяется не столько для охраны, сколько для фиксации текущих событий. Что же касается охранного телевидения, то в настоящее время оно используется при обеспечении безопасности прежде всего особо важных, режимных объектов и объектов, подлежащих обязательной охране. Недешевы пока еще нынче «оптические пассивные охранные извещатели».

В итоге я возьму на себя смелость утверждать, что использование термина «интегрированные системы безопасности» в ГОСТ Р 57674-2017 от ТК 234 не противоречит ни науке, ни здравому смыслу. И в целом многое из того, что написано в этом ГОСТе, ближе моему видению подходов к построению систем безопасности. И из всех рассматриваемых здесь ГОСТов за него и проголосую. Хотя там есть еще, над чем поработать.

ТК 439

И все-таки разработчики из ТК 234, видимо не вполне доверяя широте собственного кругозора, допустили ошибку, написав: «Состав ИСБ может быть дополнен иными системами обеспечения безопасности по ГОСТ Р 53195.1».

Приведенная фраза позволяет предположить, что в документе по указанной ссылке вопросы безопасности раскрыты более широко. Это подметил и внимательный автор, заодно указавший, кому принадлежит эта заслуга:

«Стандарт был разработан Всемирной академией наук комплексной безопасности в составе технического комитета по стандартизации ТК 439 «Средства автоматизации и системы управления» при поддержке технического комитета по стандартизации ТК 465 «Строительство» и в поддержку закона о безопасности зданий и сооружений». При этом, «эти оба технических комитета находятся на достаточно большом удалении от ФКУ «НИЦ «Охрана» Росгвардии и их ТК 234».

По всей вероятности ТК 234 что-то где-то не дорабатывает? Тогда и я решил посмотреть на проблему безопасности зданий и сооружений повнимательнее. А начать решил с основы – закона 384-ФЗ, в поддержку которого и был создан ГОСТ Р 53195.1-2008.

ЗАКОН № 384-ФЗ ОТ 30.12.2009 «ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ О БЕЗОПАСНОСТИ ЗДАНИЙ И СООРУЖЕНИЙ»

В соответствии с п. 6 статьи 3 закон устанавливает «минимально необходимые требования к зданиям и сооружениям (в том числе к входящим в их состав сетям инженерно-технического обеспечения и системам инженерно-технического обеспечения)». И касается это требований по механической и пожарной безопасности; безопасности при опасных природных процессах и явлениях и/или техногенных воздействиях; безопасных для здоровья человека условий проживания и пребывания в зданиях и сооружениях; безопасности для пользователей зданиями и сооружениями; доступности зданий и сооружений для инвалидов и других групп населения с ограниченными возможностями пере-

движения; энергетической эффективности зданий и сооружений; безопасного уровня воздействия зданий и сооружений на окружающую среду.

Про безопасность самих зданий имеется статья 11 «Требования безопасности для пользователей зданиями и сооружениями»:

«Здание или сооружение должно быть спроектировано и построено, а территория, необходимая для использования здания или сооружения, должна быть благоустроена таким образом, чтобы в процессе эксплуатации здания или сооружения **не возникало угрозы наступления несчастных случаев и нанесения травм людям** – пользователям зданиями и сооружениями в результате скольжения, падения, столкновения, ожога, поражения электрическим током, а также вследствие взрыва».

А о системах инженерно-технического обеспечения указано в п. 21 статьи 2 (обратите внимание, где безопасность, а где остальное, это еще понадобится!):

«**Система инженерно-технического обеспечения** – одна из систем здания или сооружения, предназначенная для выполнения функций водоснабжения, канализации, отопления, вентиляции, кондиционирования воздуха, газоснабжения, электроснабжения, связи, информатизации, диспетчеризации, мусороудаления, вертикального транспорта (лифты, эскалаторы) **или функций обеспечения безопасности**».

О функциях обеспечения «криминальной» безопасности (практически вскользь, в свое время по настоянию НИЦ «Охрана») упоминается в п. 13 статьи 30:

«Для обеспечения защиты от несанкционированного вторжения в здания и сооружения необходимо соблюдение следующих требований:

1) в зданиях с большим количеством посетителей (зрителей), а также в зданиях образовательных, медицинских, банковских организаций, на объектах транспортной инфраструктуры должны быть предусмотрены меры, направленные на уменьшение возможности криминальных проявлений и их последствий;

2) в предусмотренных законодательством Российской Федерации случаях в зданиях и сооружениях должны быть устроены системы телевизионного наблюдения, системы сигнализации и другие системы, направленные на обеспечение защиты от угроз террористического характера и несанкционированного вторжения».

Таким образом, главное предназначение закона заключается в формировании минимальных требований, необходимых для **эксплуатационной безопасности** зданий и сооружений.

А при чем тогда здесь ТК 439? По всей вероятности его подкомитет ПК/3 «Комплексные системы безопасности» рассматривает эксплуатационную безопасность зданий и сооружений в качестве неотъемлемой части своей сферы деятельности. Хотя мне думается, что понятия «комплексные системы безопасности (КСБ)» и «комплексная безопасность» при всей фонетической схожести отнюдь не синонимичны между собой. Но к этому я вернусь чуть позже.

Теперь непосредственно о выпущенных этим техническим комитетом документах.

ГОСТ Р 53195.1-2008 «Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения».

Основой для создания стандарта явились международный стандарт МЭК 61508 и российский ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». Но силами технического комитета ТК439 в приложении к «зданиям и сооружениям».

О чем же рассматриваемый стандарт? В переводе на русский о функциональной безопасности не просто систем, а **систем, связанных с безопасностью зданий и сооружений**. И коль скоро он создавался в поддержку 384-ФЗ, то логично было бы предположить, что речь должна идти о функциональной безопасности таких систем, которые, в соответствии с упомянутым ранее п. 6 статьи 3 закона, обеспечивают должный уровень всех перечисленных в той же статье закона видов безопасности.

При этом под **функциональной безопасностью** указанных систем логично было бы понимать часть общей безопасности, отвечающую за **правильную работу** систем или отдельных их компонентов в соответствии с заложенными в них алгоритмами функционирования (в том числе и в ответ на входные воздействия) и обеспечивающую отсутствие неприемлемого риска здоровью людей, их собственности или окружающей среде.

Однако на деле все оказалось не так просто.

Основополагающие определения в рассматриваемом документе звучат таким образом:

«3.37 **связанная с безопасностью система [подсистема]; СБС (safety-related system)**: Система [подсистема], реализующая функцию или функции безопасности, необходимые для достижения и поддержания безопасного состояния управляемого оборудования своими силами или совместно с другими связанными с безопасностью системами или внешними средствами уменьшения риска».

«3.38 **связанная с безопасностью зданий и сооружений система [подсистема]; СБЗС-система [подсистема]**: Связанная с безопасностью система [подсистема], установленная в зданиях и сооружениях, взаимодействующая с системами или подсистемами этих объектов, с их составляющими и средой».

«3.42 **функциональная безопасность (functional safety)**: Часть безопасности, относящаяся к управляемому оборудованию и системе управления управляемым оборудованием связанной с безопасностью здания или сооружения системы при выполнении функции безопасности».

В свою очередь:

«3.43 **функция безопасности (safety function)**: Функция, выполняемая связанной с безопасностью системой для достижения или поддержания безопасного состояния управляемого оборудования при определенном опасном событии».

Итак, **СБС** – это система, реализующая **функцию безопасности**, необходимую для достижения и поддержания безопасного состояния управляемого оборудования. А **функция безопасности**, в свою очередь, – это функция, выполняемая **СБС** для достижения или поддержания безопасного состояния этого же самого управляемого оборудования. Просто и убедительно!

С **СБЗС-системой** вообще никаких проблем. Это та же СБС, но только уже установленная в здании.

И на вершине всего находится **функциональная безопасность**, ради которой ГОСТ и создавался. В рассматриваемом документе она является некоей частью безопасности, относящейся к управляемому оборудованию и к системе управления управляемым оборудованием **СБЗС-системы** при выполнении (вероятно посредством системы управления управляемым оборудованием) функции, обеспечивающей достижение или поддержание безопасного состояния этого самого управляемого оборудования при определенном опасном событии.

А что же скрывается под этим таинственным термином «управляемое оборудование»? Молчит ГОСТ, не дает ответа… Дает лишь определение «системы управления управляемым оборудованием», которая призвана им управлять.

Сказать по правде, я как ни старался, но так до конца и не понял смысла всего написанного. Вместо этого возникла только пара вопросов. С одной стороны почему такое понятие, как **функциональная безопасность** является принадлежностью лишь систем, связанных с безопасностью? А с другой – в такой трактовке может оно и к лучшему?

В самом же ГОСТ удивило большое количество новых терминов, перешедших к нам из международных стандартов. Например, такого:

«3.5 **вторжение (intrusion)**: Несанкционированное проникновение на охраняемую или контролируемую территорию, зону или объект».

Зачем это понадобилось делать, не ясно. Ведь по-русски «вторжение» – это хоть и несанкционированное, но прежде всего насильственное проникновение. Что в корне меняет весь смысл (и замысел!) проникновения тайного.

Тем не менее, всех этот ГОСТ устроил, в том числе и своими развернутыми приложениями, которые, судя по всему, и следовало бы считать образцовым результатом комплексного подхода к обеспечению безопасности. По этому поводу автор пишет:

«И вот в Приложении А к этому ГОСТ в пункте А.2 «Системы обеспечения безопасности» можно найти большое множество составляющих, реально влияющих на безопасность зданий и сооружений по отношению к людям. Многие будут удивлены, но в безопасность зданий и сооружений на одном из первых мест входит безотказная работа систем канализации или мониторинг целостности строительных конструкций».

Признаться, я тоже был удивлен этим утверждением и не поленился заглянуть в раздел А.2. Однако среди систем обеспечения безопасности никакой канализации не обнаружил! А обнаружилась она в разделе А.1 «Инженерные системы». Поэтому спешу всех успокоить – согласно и 384-ФЗ, и ГОСТ Р 53195.1-2008 система канализации на безопасность зданий и сооружений не влияет. В соответствии со статьей 19 закона «Требования к обеспечению выполнения санитарно-эпидемиологических требований» она просто должна быть предусмотрена. И это правильно – не «на двор» же людям бегать! Что же касается безопасности самих граждан, то все, что я слышал по этому поводу, так это истории о том, как люди тонули в выгребных ямах уличных сортиров.

Теперь непосредственно о Приложении А, состоящем из двух частей.

Если в законе (п. 21 статьи 2) перечислено четырнадцать систем обеспечения жизнедеятельности зданий и сооружений, то в приложении **А.1 Инженерные системы** их уже порядка пятидесяти!

А в разделе **А.2 Системы обеспечения безопасности** таких систем я насчитал порядка тридцати, включая даже экзотику в виде «контроля уровня жидкостей в емкостях и бассейнах». Впрочем, логика в этом тоже есть – нырять и плавать в бассейне без воды действительно опасно для здоровья.

Там же дополнительно отдельной строкой прописаны как ИСБ (при объединении **двух или более** систем или подсистем обеспечения безопасности), так и КСБ (система безопасности, одновременно выполняющая **несколько функций безопасности**, снижающих риски, обусловленные несколькими видами и/или источниками опасностей). А структурированная кабельная сеть (в силу неких сомнений или для убедительности?) вообще упоминается в обоих разделах сразу!

И в течение всего времени, потраченного на изучение этого ГОСТ с его Приложениями, я не мог отделаться от ощущения, что их наполнение производилось по принципу «цыганские ученые где-то разузнали...». На мой взгляд, авторы поместили туда все, о чем когда-либо и где-либо хоть что-нибудь слышали.

Поэтому я и посчитал ошибкой разработчиков из ТК 234 ссылку на этот ГОСТ с точки зрения расширения номенклатуры подсистем в составе ИСБ.

Попутно я попытался разобраться и с тем, как ГОСТ Р 53195.1-2008 обеспечивает упомянутую ранее поддержку закона 384-ФЗ. Однако изучив Постановление Правительства РФ от 26.12.2014 № 1521 «Об утверждении перечня национальных стандартов и сводов правил (частей таких стандартов и сводов правил), в результате применения которых на обязательной основе обеспечивается соблюдение требований Федерального закона «Технический регламент о безопасности зданий и сооружений», я не обнаружил никаких сведений об упоминании ГОСТ Р 53195.1-2008. Видимо по мнению Правительства РФ закон № 384-ФЗ в такой поддержке не нуждается.

ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»

Вероятно осознав, что в ГОСТ Р 53195.1-2008 терминологические отличия для базовых понятий ИСБ и КСБ оказались на уровне арифметики туземного племени (один – система, два – ИСБ, несколько – КСБ), разработчики буквально через год подошли к решению задачи гораздо основательнее. И выпустили новый документ, в котором дана расширенная формулировка этих терминов:

«3.16 **система безопасности интегрированная**: Разрабатываемая специализированная сложная техническая система, объединяющая (интегрирующая) на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных целевые функциональные технические подсистемы и технические средства, предназначенные для комплексной защиты объекта от нормированных угроз различной природы возникновения и характера проявления.

3.17 **система безопасности комплексная**: Проектируемая для конкретного объекта специализированная сложная организационно-техническая открытая (допускающая последующее расширение структуры и функций) система, состоящая из алгоритмически объединенных (интегрированных) целевых функционально самостоятельных технических подсистем и технических средств, предназначенных для комплексной защиты объекта от нормированных угроз различной природы возникновения и характера проявления...

5.1.3 Структурно КСБ объектов представляют собой алгоритмически упорядоченные и взаимосвязанные совокупности централизованно управляемых функционально самостоятельных технических подсистем конкретного целевого назначения, а также средств инженерного обеспечения объектов и занимаемой ими территории, сетей технических средств иного назначения, используемых на объектах (например, локальных компьютерных сетей).

6.1.1 ИСБ представляют собой сложные программируемые многофункциональные составные изделия, изготавливаемые предприятием-изготовителем по нормативной документации, утвержденной в установленном порядке (например, по ТУ или по стандарту организации (СТО)».

И что же из всего этого терминологического хитросплетения следует?

А следует из этого то, что ИСБ разрабатывается и поставляется от предприятия-изготовителя, а КСБ проектируется под конкретный объект.

Отличия между ИСБ и КСБ вроде бы есть. В **ИСБ** входят технические подсистемы и средства «на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных **целевые функциональные**», а вот в **КСБ** – «алгоритмически объединенные (интегрированные)(!!) **целевые функционально самостоятельные**». Однако практически сразу же из п. 6.2.1 мы узнаем, что: «В общем случае состав технических подсистем ИСБ на основе функциональных блоков аналогичен составу технических подсистем КСБ, приведенных в п. 5.2».

А не означает ли это, что КСБ тоже может делаться на заводе и состоять из «целевых функциональных технических подсистем»? А подсистемы в ИСБ, в свою очередь, тоже могут быть не только «алгоритмически объединенными (интегрированными)(!!)», но и «целевыми функционально самостоятельными»?

А может КСБ на заводе не делается, потому что этого никому и не надо?

А что же по поводу этого самого проектирования под объект говорит Постановление Правительства Российской Федерации от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию»? А там определено двенадцать разделов, но про КСБ ничего и нигде не написано. Имеется отдельный раздел 9 «Мероприятия по обеспечению пожарной безопасности» (п. 26). О безопасности имеются разрозненные сведения в разделе 5 «Сведения об инженерном оборудовании…»: охранное теленаблюдение и СКУД для объектов производственного назначения; досмотровая техника для больших зданий (более 50 человек в одном помещении одновременно); СОС, СКУД, видеонаблюдение и оповещение для Метрополитена. Пожалуй и все.

А каким же образом по мнению Правительства Российской Федерации должна обеспечиваться **комплексная безопасность** объекта от угроз различного типа? А для этих целей в соответствии с п. 26 раздела 9 Постановления должны быть прописаны **сценарии взаимодействия** систем безопасности с технологическими, инженерными и другими системами. А реализация этих сценариев – в соответствующих разделах проекта.

И что мы имеем в итоге? А в итоге по утвержденным правилам должны проектироваться системы безопасности «криминальной» и пожарной. Должны проектироваться системы инженерно-технического обеспечения. Должны быть прописаны сценарии взаимодействия между ними на случай возникновения чрезвычайных обстоятельств и угроз различного типа. А вот сами КСБ проектироваться не обязаны. Просто потому, что их нет. И по закону нет! И по Постановлению Правительства нет! И получается в итоге как в забавной детской песенке – подкомитет ПК/3 «Комплексные системы безопасности» есть, а самих КСБ нет.

На самом деле в этом гораздо больше логики, чем может показаться на первый взгляд.

Дело в том, что основным предназначением систем безопасности является раннее обнаружение угроз с последующим реагированием на них. И об этом мы еще поговорим в третьей части статьи. А вот штатная работа инженерных систем, напротив, заключается совсем в другом. Их предназначение – в организации и поддержке процессов жизнеобеспечения зданий и сооружений в процессе их эксплуатации. Возникновение же на объекте угроз различного характера является для инженерных систем ситуацией **нештатной**! В результате чего они переводятся в **аварийный** режим работы в соответствии с заранее подготовленными сценариями.

Например, при пожаре кабина лифта не открывая дверей должна направиться вниз на основной этаж, имеющий непосредственный выход на улицу. Там она должна остановиться и стоять с открытыми дверями. А в случае, например, землетрясения та же самая кабина должна остановиться на ближайшем этаже и тоже стоять с открытыми дверями. Ну и так далее.

Поэтому при столь различных целях и задачах, организационно-правовая и техническая структура диспетчеризации и управления системами кардинально отличается. И общего у них гораздо меньше, чем отличий.

Разумеется, понятие безопасности для инженерных систем тоже существует, но только с точки зрения обеспечения их безопасного функционирования для жизни и здоровья человека. В соответствии с 384-ФЗ.

А вот разработчики ГОСТ Р 53704-2009 этот закон (п. 21 статьи 2) нарушили, включив в состав КСБ электроосвещение, электропитание, канализацию (поторопился я успокоить читателя – есть оказывается такая угроза безопасности человечеству!), газоснабжение, водоснабжение и поддержание микроклимата.

Правда, когда читаешь соответствующие разделы ГОСТ, посвященные отдельным подсистемам, то начинаешь понимать, что речь вроде бы идет не о них самих, а о процессах мониторинга и контроля за ними. Однако от этого не становится легче, поскольку эти самые процессы мониторинга, по мнению разработчиков ГОСТа, заключаются в следующем:

«При мониторинге сетей и сооружений водо-, газоснабжения, канализации и поддержания микроклимата в помещениях (отопление, вентиляция, кондиционирование), а также официально разрешенных к применению на объекте электробытовых приборов постоянного использования проверяется их исполнение, техническое состояние и наличие соответствующих документов, подтверждающих их электрическую, санитарно-гигиеническую и пожарную безопасность, а также **обеспечение условий** для контроля рабочих и потребительских характеристик и параметров в пределах действующих норм безопасности».

Каким образом все это должны реализовывать специалисты по разработке проектной документации на ту же КСБ, мне не вполне непонятно.

К слову сказать, среди моих многочисленных знакомых проектировщиков я не знаю ни одного, кто в своей работе руководствовался бы ГОСТ Р 53704-2009.

Базовыми документами проектантов по их мнению являются:

- упомянутое Постановление Правительства Российской Федерации от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- ГОСТ Р 21.1101-2013. Национальный стандарт Российской Федерации. Система проектной документации для строительства. Основные требования к проектной и рабочей документации.

Резюмируя написанное, могу сказать одно. С моей точки зрения, отмеченная терминологическая неразбериха вкупе с нарушением действующего законодательства, указывают на наличие серьезных внутренних противоречий в самой сути понятия «комплексные системы безопасности».

ВЫВОДЫ

На этой оптимистической ноте мы подошли к главному вопросу автора: «Тогда какой стандарт по ИСБ, из приведенных, самый правильный, какие требования нужно предъявлять к этой ИСБ, какую и кому она должна обеспечить безопасность? Как и где потом доказывать у кого больше прав?»

С формальной точки зрения оба стандарта являются официально действующими. Поэтому формально оба правы. Ну а дальше время само все расставит по своим местам.

О своих предпочтениях я уже высказался, а о своем видении путей решения проблемы выскажусь в третьей части этой статьи.

Автор же со всей очевидностью отдает пальму первенства документам, созданным в ТК 439. Со своей позицией он определился еще в 2013 году и озвучил ее в статье «Где находится последний рубеж комплексной системы безопасности?» (Алгоритм безопасности. 2013. № 1):

«И слава богу, что наконец-таки термин «система безопасности комплексная» нашла своего правообладателя» (имелся в виду ТК 439).

В этой связи позволю себе задать лишь один встречный вопрос – а на основании какого правоустанавливающего документа права на термин(!) «система безопасности комплексная» принадлежат техническому комитету ТК 439? Из-за соответствующего названия его подкомитета ПК/3?

Хотя, признаюсь, я бы и не пытался этого оспаривать.

Вывод из наболевшего у меня один – общими усилиями, отбросив лишние амбиции и с привлечением всех заинтересованных сторон навести порядок в собственном доме. Иначе за нас это сделают другие.

Полная версия трех частей статьи будет опубликована в разделе статьи на www.avtoritet.net