атель – компания Grotech с 1993 года

СИСТЕМЫ БЕЗОПАСНОСТИ

циалистов

S&S

февраль – март 2020 № 1 (151)

★ ЖУРНАЛ СИСТЕМЫ БЕЗОПАСНОСТИ ★ ЖУРНАЛ СИСТЕМЫ БЕЗОПАСНОСТИ

25 ЛЕТ

ГОРОД: ИЛИ УДОБНЫЙ?

ИЕ! СПЕЦИАЛЬНЫЙ ЖУРНАЛ!

ть руководителю, ответственному за безопасность организации, или начальнику технического отдела!

BEWARD SV5020RBZ

4K ВИДЕО РЕАЛЬНОГО ВРЕМЕНИ

IP-камера SV5020RBZ формирует высококачественное видео с максимальным разрешением 3840 x 2160 пикселей и 30 кадр/с. Таким образом, при видеомониторинге больших пространств обеспечивается высочайшая детализация изображения. Разрешение 8 Мп реального времени и аппаратный 2xWDR (до 120 дБ) позволяют круглосуточно фиксировать в мельчайших подробностях все события в зоне наблюдения.

DOUBLE SCAN

AUTO FOCUS

Встроенная монтажная коробка

IP-камера SV5020RBZ оснащена монтажной коробкой, встроенной в кронштейн. Нет необходимости в приобретении и установке дополнительной монтажной коробки рядом с камерой, что делает её монтаж значительно проще и быстрее.

ОСОБЕННОСТИ КАМЕРЫ:

- Разрешение 8 Мп (4К) 3840 x 2160 @ 30 кадр/с
- Высокочувствительный сенсор SONY Starvis
- Double Scan – аппаратный 2xWDR, до 120 дБ
- Мощная ИК-подсветка, до 60 м
- Моторизованный объектив, 3–11 мм, F1.4
- Цифровая стабилизация изображения
- Встроенная видеоаналитика: 8 режимов
- Рабочий диапазон температур от -40 до +60 °C
- Поддержка SIP-протокола

www.beward.ru

Издатель – компания Groteck с 1993 года

СИСТЕМЫ БЕЗОПАСНОСТИ

Журнал для руководителей и специалистов в области безопасности

S&S

февраль – март 2020 № 1 (151)

Лучшие продукты. Новинки 2020

Эпоха эмоционального AI

Рейтинг видеокамер

Эволюция менеджера

"Утечка мозгов" в камеру

GDPR-террористы

Спасет ли страховка от пожара?

★ ЖУРНАЛ СИСТЕМЫ БЕЗОПАСНОСТИ ★ ЖУРНАЛ СИСТЕМЫ БЕЗОПАСНОСТИ

25 ЛЕТ

УМНЫЙ ГОРОД: УСТОЙЧИВЫЙ ИЛИ УДОБНЫЙ?

www.secuteck.ru

ВНИМАНИЕ! СПЕЦИАЛЬНЫЙ ЖУРНАЛ!

Передать руководителю, ответственному за безопасность вашей организации, или начальнику технического отдела!

Международный

ТБ ФОРУМ®

Технологии Безопасности

БИЗНЕС В ТРЕНДЕ: ТЕНДЕНЦИИ. ИНВЕСТИЦИИ РЕШЕНИЯ. ЛИЧНОСТИ

ОТРАСЛЕВЫЕ РЕШЕНИЯ • КЕЙСЫ ПО ВЕРТИКАЛЬНЫМ РЫНКАМ • БЕЗОПАСНЫЙ УМНЫЙ ГОРОД • СОВЕЩАНИЕ СИТИ-МЕНЕДЖЕРОВ • ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ • ТРЕКИНГ И МОНИТОРИНГ • ТРАНСПОРТИРОВКА ВАЖНЫХ ГРУЗОВ • КИБЕРУГРОЗЫ СИСТЕМАМ БЕЗОПАСНОСТИ • КОНВЕРГЕНЦИЯ ИТ И СБ • БИЗНЕС-АНАЛИТИКА • УПРАВЛЕНИЕ РИСКАМИ • ПРЕДОТВРАЩЕНИЕ ПОТЕРЬ • МОДЕЛЬ УГРОЗ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ • РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ • ИНЖЕНЕРИЯ БЕЗОПАСНОСТИ • АРХИТЕКТУРА И ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ • НОВЫЕ ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ И ОЦЕНКА ПРОЕКТОВ • БЕЗОПАСНОСТЬ НАЦИОНАЛЬНЫХ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ • КРИТИЧЕСКИЕ И ОСОБО ВАЖНЫЕ ОБЪЕКТЫ • ЗАЩИТА ПЕРИМЕТРА • АНТИТЕРРОР • ИМПОРТОЗАМЕЩЕНИЕ • ЛОКАЛИЗАЦИЯ ПРОИЗВОДСТВА • СТАРТАПЫ В БЕЗОПАСНОСТИ • ПИЛОТНЫЕ ПРОЕКТЫ

9–11 февраля 2021

КРОКУС ЭКСПО

КОВОРКИНГ ДЛЯ ПРОФЕССИОНАЛОВ

- Конечных заказчиков
- Промышленных предприятий
- Городских администраций
- Проектных организаций
- Монтажных организаций
- Инсталляторов
- Интеграторов
- Служб безопасности
- Специальных служб
- Министерств и ведомств

Регистрация по ссылке GO.TBFORUM.RU

Groteck Business Media

www.tbforum.ru

Умные города – драйвер глобальной цифровизации

Андрей Мирошкин,
генеральный директор
компании “Гротек”

Наталья Матлахова,
руководитель проекта
“Системы безопасности”
компании “Гротек”

Марина Бойко,
главный редактор проекта
“Системы безопасности”
компании “Гротек”

Эксперты оценивают идеологическую готовность мира стать тотально цифровым в 80%. Бурный рост IP-технологий, развитие инструментов видеоаналитики и влияние искусственного интеллекта на все процессы развития общества, несомненно, затрагивают и сферу безопасности, которая в наши дни обеспечивает не только качество жизни и устойчивое развитие, но и национальный и технологический суверенитет государства.

Следуя за тенденциями развития отрасли, наше издание тоже меняется. Небольшая рубрика “Цифровая трансформация: AI, умный город, IoT” становится полноценным разделом, “Видеонаблюдение” расширяется до “Видеонаблюдения и видеоаналитики”, все чаще публикуются материалы о беспилотных авиационных системах, интегрированных комплексных решениях, новых видах угроз и противодействиях им.

В этом номере мы акцентируем внимание на умном городе и цифровом ЖКХ – его составной части. По оценкам ООН, мировая урбанизация уже составляет более 50% и достигнет 70% к 2050 г. Крупнейшие мегаполисы генерируют 57% мирового ВВП, а корпорации все чаще делают выбор не между странами, а между городами.

Именно города сталкиваются с большим числом проблем, вызовов и угроз – транспортных, экологических, миграционных... Поэтому неизбежна трансформация управления развитием городов, которое все больше опирается на передовые и инновационные технологии, большие данные и цифровизацию.

Именно умные города выступают главным драйвером развития видеоаналитики, мировой рынок которой, по оценкам аналитического агентства MarketsandMarkets, прирастает на 21,5% ежегодно: распознавание автомобильных номеров, лиц и эмоций, детекция оставленных предметов, анализ потоков людей и транспорта... Поэтому мы посчитали уместным в данном номере спецпроект “Камеры с видеоаналитикой” и привлекли к обсуждению этой темы широкий круг экспертов.

Еще один акцент делаем на IP-домофонию, которая при грамотном построении может стать важнейшей частью унифицированной городской среды: обеспечить контроль доступа и видеоконтроль прилегающей домовой территории, связь с экстренными службами, оповещение населения в случае чрезвычайных ситуаций.

И наконец, к новому деловому и строительному сезону в специальном разделе мы представляем “Лучшие продукты 2019. Новинки 2020”.

Мы привлекли к работе над номером более пятидесяти экспертов и собрали под этой обложкой много интересного, познавательного и полемичного.

Читайте наши издания.
Регистрируйтесь на наши мероприятия.
Следите за новостями на сайтах.
Оформляйте подписку на www.secuteck.ru/subscription

Электронная версия журнала www.secuteck.ru/imag

СИСТЕМЫ БЕЗОПАСНОСТИ

www.secuteck.ru

SECURITY AND SAFETY

Журнал для руководителей и специалистов в области безопасности

№ 1 (151) февраль – март 2020

В НОМЕРЕ

Генеральный директор ООО "Гротек": Андрей Мирошкин

Издатель: Владимир Вараксин

Руководитель проекта: Наталья Матлахова

Консультант проекта: Марина Садекова

Главный редактор: Марина Бойко

Редакторы: Анастасия Разбойникова, Анна Миронова

PR-менеджер: Екатерина Кузьмина

Менеджеры: Наталья Зинина, Ольга Терехова, Татьяна Чаусова

Департамент распространения: (495) 647-0442

Юрисконсульт: Кирилл Сухов

Производственный менеджмент: Татьяна Мягкова

Дизайн, верстка: Ольга Пирадова

Дизайн первой обложки: Ольга Пирадова

Корректор: Галина Воронина

Учредитель и издатель ООО "Гротек"

Журнал "Системы безопасности" № 1 за 2020 г.

Издание зарегистрировано в Комитете РФ по печати Свидетельство ПИ № 77-16428 от 22.09.03 г.

Для почты: 123007 Москва, а/я 82

www.secuteck.ru,

тел.: (495) 647-0442

Отпечатано: в ЗАО "Lietuvos rytas", Вильнюс, Литва, тираж 25 000 экз.

Цена свободная

СИСТЕМЫ БЕЗОПАСНОСТИ
www.secuteck.ru
№ 1 (151) февраль – март 2020
S&S
SECURITY AND SAFETY
Журнал для руководителей и специалистов в области безопасности

В НОМЕРЕ

СИСТЕМЫ БЕЗОПАСНОСТИ
www.secuteck.ru
№ 1 (151) февраль – март 2020
SECURITY AND SAFETY
Журнал для руководителей и специалистов в области безопасности

В НОМЕРЕ

СИСТЕМЫ БЕЗОПАСНОСТИ
www.groteck.com
int@groteck.ru
№ 1 (151) February – March 2020
SECURITY AND SAFETY
Industry Magazine for Security Professionals
FEATURES

XXV юбилейный Форум "Технологии безопасности": эффективная площадка для коммуникаций

Международный форум "Технологии безопасности", который прошел с 11 по 13 февраля в Крокус Экспо, отметил в этом году свое 25-летие. Это мероприятие – отраслевая платформа для диалога, взаимодействия и сотрудничества в сфере национальной безопасности, крупнейший съезд руководителей по безопасности. Форум был и остается самым влиятельным событием в России для руководителей и специалистов, принимающих решения в области обеспечения безопасности, защиты информации и цифровизации предприятий

Безопасность в наши дни обеспечивает не только качество жизни и устойчивое развитие страны. Это вопрос национального и технологического суверенитета. Форум "Технологии безопасности" под руководством активно действующего оргкомитета в максимальной степени учитывает национальную повестку дня, это инвестиции в безопасность, подготовка кадров, развитие инфраструктуры, разработка новых продуктов и систем.

За 25 лет развития Форум "Технологии безопасности" прошел путь от выставки к платформе непрерывного диалога и взаимодействия: рабочие мероприятия Форума происходят ежемесячно в течение года, а февральское событие является крупнейшим на пространстве России и СНГ местом выработки решений и обмена опытом, местом встречи руководителей и специалистов из всех отраслей российской экономики.

Формы и методы работы Форума построены таким образом, чтобы эффективно налаживать сотрудничество всех заинтересованных сторон: органов власти и самоуправления, потребителей и производителей, общественных объединений и центров компетенции.

Главные принципы построения программы мероприятий и экспозиции ТБ Форума – опора на активных и профессиональных людей, создающих архитектуру и технологии обеспечения безопасности, создание условий для эффективного взаимодействия, снижение барьеров и обеспечение прозрачности сотрудничества.

Прошедшие три дня органично объединили **годовую программу консультативных встреч по каждому направлению безопасности**

Владимир Шелепов, ГКС (АО "Группа Систематика")

Мы оцениваем наше участие в юбилейном XXV Форуме "Технологии безопасности" как плодотворное и успешное. Благодарим организаторов за кропотливую работу по подготовке и проведению мероприятия, особо хотим отметить количественное и качественное увеличение аудитории Форума. Наши эксперты приняли активное участие в целом ряде конференций и консультационных встреч с заказчиками. Мы очень рады, что представленные ГКС собственные разработки, продукты и системы привлекли внимание большого количества посетителей Форума. Нам удалось успешно продемонстрировать решения, которые могут быть с пользой применены для обеспечения комплексной безопасности отдельных предприятий, объектов, городов и даже стран.

Окончательные итоги работы нам еще предстоит подвести, и, конечно же, основная работа еще впереди, но уже сейчас можно уверенно сказать, что мы очень довольны участием в Форуме. Мы также планируем принять деятельное участие в других мероприятиях, которые уже традиционно проводятся компанией "Гротек" в промежутке между ежегодными форумами.

Желаем организаторам не снижать планку и в будущем году сделать Форум еще более насыщенным и продуктивным!

Алексей Данилевский, Райффайзенбанк

Как и всегда, Форум был организован на высочайшем профессиональном уровне. Я думаю, без преувеличения можно сказать, что Форум задал планку качества, на которую следует ориентироваться другим организаторам подобных мероприятий. Экспозиция произвела самые положительные впечатления. Подбор тем конференций и круглых столов, состав их участников позволяли провести время с пользой любому посетителю. При этом как выступающий и модератор могу сказать, что аудитория была очень активная, думающая, вникающая в суть обсуждаемых вопросов. Слушатели показали высокий уровень профессионализма, с ними доклад превратился в настоящую интерактивную дискуссию. Мне кажется, основная польза от таких мероприятий – личное общение близких по духу и профессиональным компетенциям людей. И в этом отношении ТБ Форум показал себя с наилучшей стороны – новые знакомства, обсуждение острых вопросов со старыми знакомыми, с которыми из-за большой загруженности как раз и удается встретиться только в рамках Форума. Лично для меня мероприятие было очень полезным в профессиональном плане.

Александр Колычев, Правительство Вологодской области

Форум "Технологии безопасности" 2020 позволил ознакомиться с передовыми разработками в области обеспечения безопасности. Программа конференций и круглых столов охватывает множество различных тем, относящихся к безопасности, как на государственном уровне, так и в различных отраслях. В рамках Форума можно познакомиться с новейшими разработками в области обеспечения безопасности. В рамках конференции "Цифровая трансформация: от безопасного города к безопасному региону" был представлен опыт Москвы и Подмосковья по развитию систем видеонаблюдения, опыт Вологодской области и Калуги в реализации сегментов безопасного города, а также представлены технические новинки в данной сфере. Вместе с тем интересно было бы послушать про опыт других регионов по развитию систем безопасного города. Хочется поблагодарить организаторов за приглашение принять участие в работе Форума. Живое общение и обмен мнениями позволяют находить новые пути в развитии систем обеспечения безопасности.

Алексей Савельев, ООО "Аблой"
Аудитория Форума прекрасная, мы на этом рынке уже давно, так что были и наши старые знакомые, но, что очень важно, было много новых конечных потребителей из области энергетики, транспорта, промышленности. Мы эту категорию клиентов относим к PEU (Professional End Users), и для того, чтобы найти этих новых потенциальных клиентов, мы и участвовали в мероприятии.
Встречи с представителями аэропортов, ж/д транспорта, ТЭК, Газпром нефти и метрополитенов были интересными и конструктивными, хотя эффективность таких встреч можно оценить не сразу, а через несколько месяцев.
Заказчики были разные, из разных вертикалей, как раз те, кого мы и ожидали увидеть. Думаю, что мы были в нужном месте, в нужное время и с нужными решениями! Спасибо профессиональной команде "Гротек" за прекрасный Форум и до встречи в следующем году!

Андрей Скворцов, ПСЦ "Электроника"
Наша компания принимала участие одновременно в экспозиции, конференциях и круглых столах Форума "Технологии безопасности" 2020. Такой формат участия – самый продуктивный. На конференции присутствовали ведущие эксперты отрасли и ключевые заказчики. Полученная на наш доклад обратная связь оказалась ценной. После выступления специалисты приходили на стенд компании и более подробно знакомились с нашими продуктами, а поскольку стенд был удачно расположен в центре экспозиции, посетители уделяли нам большое внимание. Мы много лет участвуем в ТБ Форуме и можем отметить увеличение количества представителей крупных заказчиков в этом году. Все это благодаря активной работе организаторов и проведению серии предварительных встреч с заказчиками в течение года.

Александр Кочегаров, Дирекция по закупкам и капитальному строительству ПАО "Газпром нефть"
Участие в Форуме "Технологии безопасности" 2020 считаю высокорезультативным, учитывая количество установленных новых контактов и возможность дальнейшего взаимодействия по вопросам повышения эффективности процессов капитального строительства с применением современных технологий и решений.
Активные обсуждения проблематики применения БВС в капитальном строительстве, поиск новых технологий и решений, повышающих эффективность деятельности, лишний раз доказывают высокую заинтересованность аудитории в решении данных вопросов.
Формат проведения закрытых встреч с представителями компаний – участниками экспозиции был полезным и продуктивным. По результатам проведенных переговоров готовим предложения о возможности организации дальнейшего взаимодействия.

и крупнейший съезд руководителей и специалистов. В течение всего 2019 г. обсуждались требования и задачи, специфика объектов, предлагались решения по внедрению или модернизации систем безопасности. В рабочих группах по подготовке события приняли участие 380 экспертов, был проведен подробный разбор актуальных проблем и возможностей, подготовлены инициативы и предложения.

Национальная повестка Форума задавалась в программе совещаний, встреч и в экспозиции, созданной участниками организационного комитета и рабочих групп, объединяющих представителей органов власти, регуляторов, крупнейших российских государственных предприятий и корпораций.

Для специалистов каждого направления и сектора была сформирована отдельная программа: в рамках ТБ Форума 2020 прошли **14 VIP-мероприятий** по вопросам национальной безопасности, встречи высокого уровня, визиты региональных и международных делегаций, обсуждения норм и требований, всероссийский смотр решений и технологий, программа закрытых встреч с заказчиками.

Главное отличие деловой программы 2020 – **практическая направленность и поддержка** проектов, которые российские потребители реализуют на своих объектах, формирование эффективной среды для укрепления межведомственного сотрудничества и совместного создания решений, ценных для российских и иностранных заказчиков.

Всероссийский смотр новейших технологий и решений обеспечения безопасности и защищенности объектов и инфраструктуры состоялся в экспозиции ТБ Форума.

Что порадовало участников на Форуме "Технологии безопасности" 2020?

Качественная аудитория

Ядро аудитории (60%) – 4 498 крупных конечных потребителей из всех регионов России, государственные организации и крупнейшие корпорации. Именно они составляют 80% объема всех бюджетов на оборудование и услуги безопасности в России.

7 497 руководителей и специалистов, за три дня работы посетивших выставки и конгресс. Каждый день – новый сегмент аудитории:

- представители государственных ведомств и министерств;
- руководители объектов транспорта и транспортной инфраструктуры;
- городские, муниципальные и региональные администрации;
- владельцы спортивных объектов и организаторы спортивных и массовых мероприятий;
- ответственные за пожарную безопасность мест массового пребывания людей;
- руководители по информационной и комплексной безопасности объектов промышленности, нефтегазового сектора и электроэнергетики;
- руководители служб безопасности, экономической безопасности, противодействия хищениям ритейлеров и торговых центров;
- проектировщики и ответственные за безопасность при строительстве объектов;
- директора по безопасности, руководители информационно-аналитических отделов, отделов ИБ, физической защиты, собственной безопасности банков и финансовых организаций.

14 VIP-мероприятий деловой программы

4 277 (на 20% больше, чем в 2019 г.) делегатов приняли участие в 12 конференциях и двух круглых столах. Значительно вырос должностной уровень докладчиков и слушателей.

В этом году отмечена высокая активность представителей промышленности, ТЭК и нефтегазовой отрасли. В центре внимания профильной конференции – критически важные объекты и информационные инфраструктуры, промышленная безопасность и цифровые технологии.

Защита верхней полусферы и использование БПЛА в безопасности обсуждались на нескольких мероприятий, включая профильный круглый стол.

Изменения, ожидаемые в системе противопожарной защиты, затрагивают работу тысяч предприятий. МЧС России, Союз страховщиков России и руководители торговых центров, банков и гостиниц поделились своими планами и обсудили нововведения.

Руководители мест массового пребывания **вынуждены решать задачу обеспечения безопасности посетителей, а объекты культуры – еще и обеспечивать защиту от преступных посягательств на предметы культурного наследия**. Эти и другие вопросы активно обсуждались на соответствующей конференции.

Цифровизация во всех сферах изменяет управление территориями, экономику регионов, взаимодействие с гражданами, среду ведения бизнеса. Самым важным в развитии региональных программ безопасности, умных городов и даже районов поделились городские администрации и сити-менеджеры.

Информационные системы и инфраструктуры, безопасная разработка – все самое главное по защите информации узнали руководители департаментов ИБ на единственной в году конференции ФСТЭК России, посвященной новым требованиям и лучшим практикам.

Новый этап развития начинается в сфере транспортной безопасности. Именно в транспортной безопасности первыми внедряются передовые модели управления, такие как управление инцидентами и геоинформационные системы. Конференция 2020 г. отметила новую высоту достижений мирового уровня и собрала для обмена опытом ключевых специалистов со всей страны.

Трансформация бизнес-модели банковского сектора, реализуемая крупнейшими финансовыми организациями страны, невозможна без устойчивости к внешним и внутренним воздействиям и угрозам. Конференция SecuFinance вызвала высокий интерес как со стороны банкиров, так и со стороны их коллег в других секторах. Традиционный подход и искусственный

Евгения Колесняк, ООО "АСС"
Площадка ТБ Форума очень важна, так как здесь собираются и производители, и конечные потребители. Чтобы обеспечить прямой диалог между ними, нужно такое мероприятие. Мне нравится на этом мероприятии открытость общения, можно спокойно говорить о том, что беспокоит тебя как специалиста, и рассказывать про комплексные решения, которые помогут решить проблемы пришедших сюда экспертов.

Олег Калугин, ФКУ Упрдор Москва – Волгоград
С каждым годом обсуждение острых проблем для сферы транспортной безопасности в рамках конференции "Терроризм и безопасность на транспорте" на ТБ Форуме становится все более активным. Я приехал сюда именно с целью обсудить практические вопросы, связанные с транспортной отраслью как представитель субъекта транспортной инфраструктуры. Таких мощных площадок для обсуждения насущных вопросов очень мало.

Григорий Сизов, Департамент здравоохранения г. Москвы
Формат ТБ Форума, безусловно, был успешным и интересным. Очень важным было объединение в рамках конференции по тематике ситуационно-аналитических центров коллег из разных сфер, но работающих в едином направлении. Мы увидели, что формат работы схож и вне зависимости от вида деятельности – функциональность во многом совпадает, и успешные практики могут быть транслированы в смежные сферы.

интеллект в задачах безопасности, единая биометрическая система, предикативная аналитика и контроль за персоналом – вот неполный список этого насыщенного мероприятия.

Розничные сети в России расширяются и укрупняются, сталкиваясь с новыми вызовами эффективности и безопасности. Развитие дистанционной торговли порождает новые задачи в управлении логистикой, снижение затрат на персонал требует надежного машинного зрения и интеллекта, а инцидент-менеджмент обслуживает потребности бизнеса. Участники конференции SecuRetail оценили интересное и практичное содержание этой ежегодной встречи.

На конференции по тематике ситуационно-аналитических центров участники обменялись практическим опытом создания кейсов эксплуатации ситуационных и диспетчерских центров в различных отраслях и убедились, что успешные практики могут быть транслированы в смежные сферы.

Основным вектором развития современного общества является курс на цифровую экономику. Реализация данного направления невозможна без обеспечения гарантий безопасности и доверия в рамках критической информационной инфраструктуры. **Впервые прошла конференция, посвященная обсуждению совершенствования российской нормативной базы, разработке российских технологических решений,** которые позволят реализовать современные цифровые сервисы при наличии гарантий доверия и безопасности.

Обсуждения в рамках Форума и его рабочих групп направлены на выявление практически ценных идей с учетом цифровизации в строительстве и диалог ключевых участников. **Конференция для проектировщиков дала старт практическим обсуждениям в рабочих группах в течение года.**

Системы видеоаналитики являются мейнстримом всей концепции видеонаблюдения, так как позволяют превратить пассивное видеонаблюдение в активный процесс контроля и повышают ценность подобных систем для бизнеса в несколько раз. Последние достижения в области искусственного интеллекта и самообучающихся нейросетей обсудили на межотраслевом круглом столе.

На форуме выступило 258 докладчиков – регуляторы, крупнейшие заказчики, разработчики и признанные эксперты.

Смотр решений и технологий

В экспозиции смотра технологий свои решения продемонстрировали 44 новых участника, среди которых 3С ГРУПП ЛТД, Bosch Системы Безопасности, IBS Platformix, InfoWatch и др.

Серия встреч регуляторов, заказчиков и поставщиков

Впервые была реализована полноценная программа встреч с заказчиками в VIP-Lounge: в 17 встречах приняли участие 78 представителей заказчиков и 181 представитель компаний участников и партнеров Форума. Среди участников: ГКУ "Московская безопасность", АО "Сити-XXI век", ГК ПИК, аэропорт Домодедово, ПАО "НК "Роснефть", Газпром нефть, Норникель, Росатом, ФГБУ "Администрация морских портов Черного моря", ПАО "ДВМП", АО "Судоходная компания "Волжское пароходство", АО "НИПИГАЗ", Администрация Губернатора Новосибирской области, ГАУК г. Москвы ПКиО "Красная Пресня", ФГБУ "Российская государственная библиотека", Международный аэропорт Сабетта, АВИАКОМПАНИЯ ЭЙР-БРИДЖКАРГО, Мособлгеотрест, СПб ГУП "Пассажиравтотранс", ГБУ "Мостранспроект", Московский метрополитен, ТС "Монетка", Макси, Касторама Рус, X5 Retail Group, АО "ФПК", Дирекция железнодорожных вокзалов, ФГУП "ГлавНИВЦ", РТРС, Теле 2, Севералмаз, ЕвроХим, Райффайзенбанк, Альфа-Банк и др.

Отраслевая ТБ-премия 2020

Продукты и решения партнеров Форума, рекомендованные для тестирования и внедрения:

- Biosmart Quasar – сочетание современных технических параметров с привлекательным дизайном и высокой степенью надежности;
- интеграционная платформа "Интегра 4D-Планета Земля" – единое информационное пространство, которое объединяет все доступные источники информации на территории объекта и города;
- M2Медиа.Видео – интеллектуальная система видеонаблюдения и аналитики на транспорте;
- профессиональная радиосвязь МАКВИЛ – единственная всероссийская сеть для критических коммуникаций;
- vGate R2 – сертифицированное средство защиты платформ виртуализации, изолирующее приложения друг от друга;
- RuSIEM: всё под контролем – радикальное сокращение количества различных инцидентов, увеличение экономической эффективности работы организации и уменьшение финансовых потерь;
- центр мониторинга ИБ "Сокол" – мониторинг информационных систем с любой отраслевой спецификой заказчика;
- нейросеть от Спецлаб GOALcity – исключает помехи и отслеживает реальное поведение людей и автомобилей.

Что нас ждет на 26-м Форуме "Технологии безопасности" в 2021 г.

XXVI Международный форум "Технологии безопасности" – это непрерывная программа коммуникаций заказчиков, регуляторов и поставщиков в течение года: еженедельные встречи разработчиков с крупными заказчиками, круглые столы и заседания экспертных групп, а в феврале 2021 г. – всероссийский смотр решений и технологий и 15 отраслевых конференций. ■

www.tbforum.ru

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Шлагбаум PERCo GS04

- Управление от СКУД, пульта ДУ, радио-брелоков
- Управление по звонку, с помощью приложения (III кв. 2020)
- Комплектация стрелой прямоугольного или круглого сечения
- Установка справа или слева от зоны проезда
- Сигнальная индикация, фотоэлемент защиты, буферная накладка
- Защита механизма шлагбаума при наезде автомобиля
- Встроенная система обогрева механизма управления
- Двигатель с планетарным редуктором
- Гарантийный срок – 5 лет

perco.ru 8-800-333-52-53

PERCo

SICUREZZA и SMART BUILDING EXPO:

два мероприятия, одна прекрасная возможность

В Италии, в Милане, с 13 по 15 ноября 2019 г. прошла выставка SICUREZZA, тематика которой – безопасность и противопожарная защита. Она проводится раз в два года и по праву считается главным европейским событием в этой сфере (организатор – компания Fiera Milano International S.p.A)

Директор выставки Паоло Пицокаро

SICUREZZA 2019 приняла 28 629 профессиональных посетителей из 88 стран. Свою продукцию представляли 619 экспонентов (их число увеличилось на 33% по сравнению с прошлой выставкой), 30% общего числа участников составили зарубежные компании из 37 стран, в том числе и российские.

Параллельно с SICUREZZA в Милане второй раз прошла выставка Smart Building Expo, посвященная автоматизации и умным технологиям для зданий.

Посетители этих выставок ознакомились с самыми передовыми технологиями, решениями и оборудованием в профильных сферах, разработанными в соответствии с актуальными трендами отрасли – интеграцией, цифровой трансформацией, искусственным интеллектом, оценили новые продукты. Сегодня обеспечение безопасности – это не просто установка определенного оборудования, это комплексное решение, которое разрабатывается на основе изучения контекста, начиная с тщательной оценки различного рода рисков. Главные тенденции рынка безопасности – быстрая реакция на актуальные запросы и одновременно учет наиболее вероятных будущих вызовов и потенциальных векторов развития как соответствующих сфер рынка, так и общества в целом.

Организаторы подготовили очень насыщенный календарь конференций, семинаров и других мероприятий, всего более 100 в течение трех дней! Большое внимание было уделено различного рода обучению, по темам от городской безопасности до кибербезопасности, с учетом последних стандартов и правил, которым должны следовать проектировщики и монтажники.

В рамках выставки Smart Building Expo прошла конференция Milano Smart City Conference, где состоялась дискуссия на тему "Умный город" и обсуждалось влияние новых технологий на развитие городов. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

И снова лучшие:
ААМ Системз, партнер HID Global № 1

В 2019 г. компания "ААМ Системз" снова, второй год подряд, стала лучшим партнером HID Global в России и Восточной Европе по направлению "Физический доступ"

Компания HID Global (США) – лидирующий в мире производитель решений для идентификации в системах физического доступа. Миллионы людей более чем в 100 странах мира используют продукты и услуги HID Global для безопасного доступа в здания и помещения.

Сотрудничество, проверенное временем

Компания "ААМ Системз" не случайно лидирует в списке партнеров HID Global. За 18 лет сотрудничества наши специалисты в совершенстве освоили продукты бренда, наработали серьезный опыт и получили высочайшую квалификацию.

Мы предлагаем своим партнерам продукцию на выгодных условиях и защищаем проекты, разработанные на базе оборудования HID Global и наших программно-аппаратных комплексов.

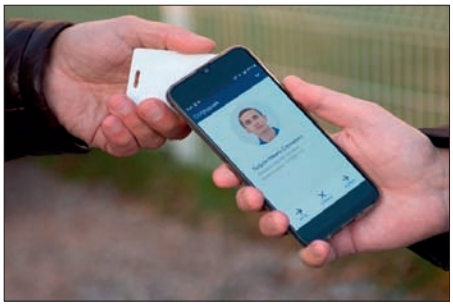
Благодарим партнеров за признание и надеемся на успешное продолжение и развитие сотрудничества! ■

Система контроля доступа PERCo-Web: новые возможности

Новые подходы к построению системы, мобильная регистрация, отправка отчетов и уведомлений о событиях

Система контроля доступа без выделенного сервера

Система контроля доступа PERCo-WEB может работать без выделенного сервера – в качестве сервера используются контроллеры PERCo нового поколения. Такое решение станет оптимальным для небольших объектов, где организован контроль доступа на входе и в несколько внутренних помещений.



Система без выделенного сервера может обработать данные 500 сотрудников и 500 посетителей и иметь в составе до 10 контроллеров. Такая архитектура упрощает внедрение системы и снижает ее стоимость.

Мобильный терминал регистрации для удаленных объектов

Смартфон с NFC-модулем может использоваться в системе PERCo-WEB в качестве регистрирующего устройства. Мобильный терминал предназначен для работы на объектах, где невозможно установить стационарный терминал регистрации, но необходим контроль доступа и учет сотрудников, например, в шахтах, на строительных площадках, нефтяных вышках.

Основные функции мобильного терминала – регистрация проходов сотрудников и посетителей и учет рабочего времени. При чрезвычайной ситуации мобильный терминал позволяет сформировать эвакуационный отчет, содержащий информацию об уже эвакуированных и еще остающихся на объекте сотрудниках.

Реакции на события в системе

В ПО PERCo-WEB добавлена возможность задавать реакции на события в системе – алгоритм действий, необходимых для контроля и управления. Возможна настройка отправки уведомлений посредством Viber, e-mail, СМС, а также всплывающих окон на ПК операторов системы, отправки отчетов по e-mail, настройка последовательности команд управления устройствами, выполняемых сервером системы.

Сотрудники службы безопасности могут оперативно получать информацию о событиях системы, руководители – отчеты о дисциплине за определенный период. ■

Казино: видеонаблюдение и безопасность на первом месте

Мировой рынок систем управления казино достигнет 15 млрд долларов к 2027 г., сообщает исследовательское агентство Grand View Research, ежегодный прирост при этом составит около 15%

Операции в казино связаны с денежными транзакциями, что приводит к частому мошенничеству и спуфингу. Чтобы обезопасить себя от подобных преступлений, владельцы и управляющие активно инвестируют в техническое оснащение заведений системами безопасности, и в частности видеонаблюдением.

Системы безопасности – это значительная часть сегмента управления казино, в 2019 г. их доля предположительно составила 1,2 млрд долларов. Автоматизация процессов приведет к дальнейшему увеличению этой доли сегмента. Видеоаналитика, распознавание автомобильных номеров, распознавание лиц и автоматизированные системы видеонаблюдения все шире применяются в игровых клубах.

Среди набора инструментов для управления казино на первое место выходит аналитика, и казино превращаются в центры обработки данных. Владельцев казино интересует поведение клиентов, игровые предпочтения, шаблоны ставок и вероятности исходов игр. Аналитические инструменты позволяют операторам игорного клуба предоставлять клиентам персонализированные игровые возможности, повышая уровень их удержания и оптимизируя игровые операции.

В управлении казино аналитика выделяется как самое активное направление, ежегодно прирастая на 16%.

Картину могут "подпортить" игровые онлайн-платформы, которые получают все более широкое распространение. ■

По материалам
www.securityworldmarket.com

Взрывной рост рынка систем видеонаблюдения: 15% в год еще не предел

Исследовательское агентство Memoori прогнозирует рост индустрии систем безопасности с 19,15 до 35,82 млрд долларов к 2024 г. Это самый высокий показатель прогнозируемого роста за все время существования агентства, причем основанный на реальном положении дел и подкрепленный различными факторами. Один из основных – выход программного обеспечения со встроенной ИИ-аналитикой на массовый потребительский рынок. Аналитики предсказывают средний ежегодный рост этого сегмента в 15%, хотя потенциал Интернета вещей (IoT) еще даже не полностью раскрыт

В Memoori предполагают, что ИИ станет основным драйвером на рынке систем безопасности в ближайшие 10 лет, при этом доля ведущего игрока – Китая в сегменте программного обеспечения с использованием искусственного интеллекта составит более 50% уже к 2024 г. Единственным ограничителем роста может стать активная защита приватности, столь популярная на Западе.

Облачные сервисы завоевывают доверие

Согласно отчету, результаты 2019 г. наглядно показывают, что облачные сервисы (в частности, VSaaS) смогли доказать свою эффективность и вырываются из нишевого сегмента в массовый. Спрос на облачное видеонаблюдение значительно вырос в 2019 г., прогнозируется дальнейший рост не менее чем 12% ежегодно в течение пяти лет.

В самые ближайшие годы умные здания станут реальностью, а IP-камеры – непосредственной частью всей системы, что в совокупности даст конечному потребителю море возможностей для решения вопросов, не связанных напрямую с безопасностью.

IP-видеокамеры становятся одним из самых мощных и функциональных устройств, используемых в обеспечении безопасности зданий

Интеграция с системой физической охраны сегодня является стандартным требованием, а объединение с ИТ-системами уже данность на корпоративном рынке. В случае со зданиями и системами Building IoT все сервисы внутри строений объединяются в один, экономя ресурсы, железо и стоимость ПО, а IP-камеры играют ведущую роль в такой системе.

География роста

Последние восемь лет география рынка систем видеонаблюдения значительно менялась, Азиатский регион демонстрировал наибольшие показатели роста, ежегодно увеличивая свою долю, и он имеет еще огромные возможности. Китай – основной потребитель и главный фактор роста в этом регионе. Сегодня его доля пока меньше половины рынка видеонаблюдения Северной Америки, в то время как потенциальный объем рынка Китая аналитики оценивают как вдвое больший. ■

По материалам www.securityworldmarket.com

ИК-детекция укрепляет позиции

Согласно последним исследованиям, в сегменте инфракрасной детекции прогнозируется мировой рост объема рынка с 498 млн долларов в 2020 г. до 683 млн долларов в 2025 г. с ежегодным повышением на 6,5%

Основным драйвером роста выступает высокий спрос на инфракрасные датчики со стороны решений для детекции движения, людей, измерения температур и охранных целей. Проникновение инфракрасных технологий в газовый анализ и активный интерес к неохлаждаемым инфракрасным детекторам также значительно стимулируют рост.

Пироэлектрики

Сегмент пироэлектрических инфракрасных детекторов займет лидирующую долю на рынке инфракрасной детекции к концу 2020 г. Такие датчики используются для самых разных повседневных задач – детекции и подсчета людей, бесконтактного измерения температуры и, конечно же, охранных функций (обнаружение проникновений).

NIR и SWIR

Доля технологий и устройств, использующих NIR (Near Infra-Red, ближняя область ИК-спектра) и SWIR (Short Wave Infra-Red, коротковолновый ИК-диапазон) к 2025 г. значительно вырастет в основном благодаря широкому применению SWIR-детекторов в видеонаблюдении, гигрометрах, спектроскопии, термографии, а также различных научных исследованиях, в том числе объектов искусства.

На данный момент стоимость коротковолновых детекторов выше, чем средне- (MWIR) или длинноволновых (LWIR), что ограничивало их применение. Однако технологические усовершенствования помогают постепенно снижать цену на эти устройства, что, безусловно, положительно повлияет на распространение SWIR-детекции.

Основные потребители

Северная Америка, предположительно, сохранит крупнейшую долю рынка в 2020 г. США и Канада остаются наиболее крупными потребителями инфракрасных датчиков и детекторов. Европейский рынок занимает второе место, а Великобритания и Германия – лидирующие позиции на нем. ■

По материалам www.securityworldmarket.com

6 трендов безопасности в 2020 году от лидеров рынка

Лидеры мирового рынка систем физической безопасности поделились своими ожиданиями относительно 2020 г. и спрогнозировали основные рыночные тренды

1. ИИ: отделяем правду от вымысла

Несмотря на то что искусственный интеллект все больше становится привычным понятием, его реальное значение пока еще переоценено. В 2020 г. активное развитие получат ИИ-системы и машинное обучение в сфере безопасности и в умных городах для более эффективного использования физических ресурсов. Распознавание автомобильных номеров благодаря ИИ будет выведено на новый уровень, с чтением более сложных знаков, распознаванием регионов и повышенной точностью.

2. Распознавание лиц и приватность

В 2020 г. разработчикам систем распознавания лиц необходимо действовать совместно с регуляторами и постоянно принимать во внимание вопросы приватности. Наравне с развитием самого качества распознавания мы увидим системы, более тщательно проработанные с точки зрения взаимодействия с персональными данными, встроенную защиту от утечек и в целом более высокий уровень безопасности пользования для сохранения приватности.

3. Физическая идентификация

Развитие облачных сервисов систем контроля доступа приведет к повышенному спросу со стороны среднего и малого бизнеса. Основным фактором будет стоимость решений, так как не каждая компания может себе позволить приобрести полноценную систему СКУД для своих задач. Функционал облачных сервисов все более приближается к десктопным версиям, и это тоже значительно влияет на спрос.

4. Защита данных блокчейном

Блокчейн в основном ассоциируется с криптовалютами, но эта технология уже начала распространятся на другие сегменты. По сути, блокчейн – гарантированный, неуничтожаемый журнал отслеживания изменений. Использование блокчейна в безопасности позволит избежать махинаций с видео, данными контроля доступа и идентификацией задним числом. Любые изменения, совершаемые в такой системе, могут быть отслежены, а журналирование событий, основа всего блокчейна, не может быть уничтожено, так как хранится распределенно. Уже сегодня крупный бизнес начинает использовать блокчейн-технологии для защиты своих данных, и в ближайшее время ожидается ее широкое распространение в сфере безопасности.

5. Фокус на кибербезопасности

Чем больше накопленных данных, тем большей защиты они требуют. В 2020 г. продолжится активное объединение технической экспертизы по всему миру с целью выработки наиболее эффективных решений по защите данных от взломов и утечек. Производители также будут вынуждены подключиться к этой работе, чтобы обеспечить себе встраиваемые механизмы защиты данных, работающие по умолчанию. Идеальная картина, к которой все стремятся, – абсолютная безопасность пользователя при гарантированной приватности и сохранении прав и свобод.

6. Интеграция с IoT

Компании – производители систем безопасности, безусловно, будут пытаться скооперироваться с масштабно надвигающейся IoT-реальностью, чтобы предоставить своим пользователям больше возможностей мониторинга и управления системами. Способность компании "держаться на плаву" будет напрямую зависеть от гибкости в вопросах интеграции со сторонними устройствами и сервисами. ■

По материалам www.securityworldmarket.com, www.asmag.com

Первый IoT-датчик на растительном топливе

Первый в мире датчик с растительными элементами питания успешно передал данные в космос. Новая технология питания электрических устройств, базирующаяся на сборе электроэнергии с живых растений и бактерий, была применена в Нидерландах

В представленном прототипе устройства получаемого тока достаточно, чтобы питать ряд простейших датчиков и светодиодную индикацию. Прототип устройства передает данные по технологии LoRa и позволяет оценивать температуру, влажность почвы, напряжение и передавать данные на спутник.

Использование такого типа устройств имеет огромный потенциал: сбор данных с сельскохозяйственных угодий сегодня ограничен именно необходимостью применения элементов питания, которые требуют постоянного обслуживания и в целом являются токсичными для сельского хозяйства.

Предложенная технология позволяет сделать экологичное и при этом полностью самодостаточное устройство, не зависящее от солнечного света и времени суток. Основная идея принадлежит голландскому стартапу Palant-e, а пилотный проект активно поддерживается Европейским космическим агенством, что дает надежду на быстрое развитие технологии и ее массовое внедрение. ■

По материалам www.securityworldmarket.com

Рынок видеонаблюдения: 2020 год – 20 млрд долларов

Аналитическое агентство IHS Market представило прогноз, по которому объем мировых продаж видеокамер, регистраторов, ПО и аксессуаров для видеонаблюдения достигнет 20 млрд долларов в 2020 г.

Основными игроками на рынке остаются США и Китай, при этом Китай занимает первое место с долей в 45%. Прогнозируется 10% общего годового роста, по сравнению с 2019 г. В регионах наиболее активное развитие покажут Индия и Юго-Восточная Азия.

IHS отмечает, что основными факторами роста выступят видеоматериалы Deep Fake, развитие 5G-сетей и так называемый искусственный интеллект вещей (AIoT). В 2020 г. количество камер, установленных по всему миру, достигнет 1 млрд единиц. Это доказывает, что вопросы приватности и защиты частной жизни становятся все более актуальными. Количество материалов Deep Fake будет расти в прогрессии, и с этим необходимо бороться.

Готовность производителей к переходу на 5G также окажет существенное влияние на весь рынок видеонаблюдения, он может значительно измениться, начиная со сроков доставки видео до хранилищ и потребителя и заканчивая повышением качества изображения в целом. ■

По материалам www.securityworldmarket.com

Мировой стандарт умного дома на подходе

Open Connectivity Foundation (OCF), один из ведущих фондов, занимающихся стандартизацией в области IoT, в январе 2020 г. впервые продемонстрировал универсальный облачный интерфейс OCF Universal Cloud Interface (UCI). Это первое решение для унификации IoT-экосистемы по схеме "облако – облако" с использованием открытых стандартов. В демонстрации участвовали мировые вендоры устройств Smart Home, такие как BSC Computer GmbH, Commax, Haier, LG Electronics, Resideo, Samsung Electronics и Sure Universal

OCF UCI – это программный интерфейс, который позволяет упростить и стандартизировать интеграцию облачных платформ между собой, а также между устройствами и облаком. Фактически было представлено конкретное API для использования во всей IoT-индустрии, и его повсеместное внедрение может привести к стремительному развитию рынка, снимая вопросы о совместимости и поддержке проприетарных протоколов.

Идеальная совместимость

Некоторые компании из числа участников OCF планируют запустить устройства с поддержкой UCI уже в 2020 г. Повышение гибкости и вариативности умного дома сыграет ключевую роль в развитии всей индустрии, которой уже сейчас прогнозируют не менее чем 13% ежегодного роста. С развитием программы спецификаций OCF производители смогут создавать продукты, которые способны без дополнительных усилий работать с другими OCF-устройствами и платформами, вне зависимости от сферы применения.

Стандарты, предлагаемые OCF, включают в себя интеграционные возможности для различных популярных протоколов, таких как Bluetooth, Enocean, Zigbee и Z-wave. Использование единого стандарта предоставит пользователю более широкий выбор технологий и продуктов.

Для всех и везде

Рынок положительно реагирует на предлагаемые изменения, ведь развитие и поддержка проприетарных API требует постоянных затрат и ресурсов. Принимая во внимание, что количество различных типов IoT-устройств для обеспечения комфорта, безопасности и мониторинга в умном доме вскоре превысит 200, деятельность по развитию проприетарных протоколов выглядит устаревшей и экономически невыгодной.

OCF UCI является открытым стандартом, базируется на OCF Framework и работает на базе локальных сетей, что делает его доступным для повсеместного применения. ■

По материалам www.securityworldmarket.com

Умный транспорт: расстановка сил на рынке

Рынок умного транспорта ежегодно растет на 6,8% в Европе и на 7,3% в Северной Америке, что позволит этим регионам к 2023 г. достичь объемов этого продукта 2,16 млрд долларов и 1,07 млрд долларов соответственно

В области развития Intelligent Transport Systems сохраняются положительные тенденции, основанные на:

- постоянно растущем интересе к умному транспорту;
- обеспокоенности общества по поводу безопасности передвижения;
- прямой заинтересованности городов в сокращении издержек и повышении эффективности управления.

За последние два года на рынке появились первые компании-лидеры: в Европе основными провайдерами ITS являются Trapeze Group (Канада) и INIT (Германия). В Северной Америке лидирующие позиции занимают компании Clever Devices и Condeunt. Число организаций, предлагающих свои услуги в этой области, ежегодно увеличивается.

Количество автомобилей со встроенными компьютерами и GPS уже достигло достаточно высокого уровня в Западной Европе и Северной Америке, в то время как Восточная Европа и средиземноморские страны отстают.

На развитых рынках набирает силу тренд ITxPT – открытая ИТ-инфраструктура для общественного транспорта, что означает более гибкую интеграцию систем управления трафиком со сторонними ИТ-системами с открытой платформой. Передовые позиции здесь занимают страны Северной Европы, где ИТ-инфраструктура городов находится на высоком уровне. ■

По материалам www.securityworldmarket.com

Каждый миллиметр под контролем

Многозонный металлодетектор МД "Паутина-2М"

ЧТО УНИКАЛЬНОГО

1 Выбор контрольной зоны
Возможность выбрать ширину контрольной зоны от 700 до 1500 мм при помощи одного прибора.

2 Универсальный подход
Изменяемая контрольная зона позволяет использовать один МД в разных местах, исключает ошибки при выборе МД на стадии проектирования.

3 Надежная работа
Обеспечение высокой чувствительности в МД с расширенным проходом до 1,5 м.

ЗАЧЕМ ПОКУПАТЬ

4 Для любых объектов
Предназначен для любых предприятий и учреждений, в которых есть необходимость организации контроля доступа.

5 Длительная гарантия
Бесплатное послегарантийное обслуживание в течение 5 лет после окончания гарантии.

6 Варианты исполнения
Доступен индивидуальный дизайн либо стандартное внешнее исполнение.

ПОЧЕМУ ОЦЕНЯТ

7 Полный охват
Расширенная до 1,5 м зона контроля многозонного металлодетектора.

8 Соответствие требованиям
Высокая чувствительность при отсутствии ложных срабатываний. Соблюдение пожарных норм при выборе расширенного прохода.

Производитель: "Локаторная техника"
Розничная цена: 250 000 руб.
см. стр. 128 "Ньюсмейкеры"

Точный бесконтактный досмотр без вреда для окружающих

Проходная радиолокационная система досмотра РСД-01

ЧТО УНИКАЛЬНОГО

1 Принцип All-in-One
В одном устройстве объединены стационарный и ручной металлодетекторы, досмотровый сканер, интроскоп, детектор взрывчатых и наркотических веществ.

2 Детальное распознавание
Система в автоматическом режиме способна распознать геометрическую форму предмета, его расположение в пространстве и материал, из которого он изготовлен.

3 Без пауз и ограничений
Контрольная зона от 0,5 до 3 м. Бесконтактный досмотр осуществляется непрерывно и без ограничения по количеству одновременно проходящих людей.

ЗАЧЕМ ПОКУПАТЬ

4 Экономия на количестве оборудования
Сокращение расходов на оборудование зоны досмотра за счет использования одного устройства вместо нескольких.

5 Безошибочный контроль
Помогает избежать длительного досмотра с использованием разных устройств по отдельности. Исключается человеческий фактор и связанные с ним ошибки.

6 Для любых объектов
Любые предприятия и учреждения, где есть необходимость организации контроля доступа.

ПОЧЕМУ ОЦЕНЯТ

7 Без вреда для людей
В устройстве используется радиолокационный способ обнаружения. Система не представляет вреда для окружающих.

8 Точно, быстро, удобно
Дистанционное обнаружение любых предметов и веществ. Отсутствие каких-либо помех для работы данной системы и отсутствие ограничений по месту установки.

Производитель: "Локаторная техника"
Розничная цена: 600 000 руб. (минимальная комплектация), 1 500 000 руб. (максимальная комплектация)
см. стр. 128 "Ньюсмейкеры"

Самая яркая звезда в галактике лицевых терминалов

Терминал Biosmart Quasar

BIOSMART

ЧТО УНИКАЛЬНОГО

1 Гибкое решение
Интеграция с платежными системами, вендинговыми автоматами.
Индивидуальные решения под заказчика.

2 Высокая скорость
Время идентификации менее 1 с.

ЗАЧЕМ ПОКУПАТЬ

3 Экономия ресурсов
Сокращение затрат с помощью УРВ, экономия времени за счет быстрой идентификации.

4 Повышение безопасности
Решает проблемы, связанные с вопросами безопасности, – защита от несанкционированного прохода благодаря уникальному алгоритму предотвращения фальсификации данных.

5 3 потребительских рынка
Ритейл, HoReCa, безопасность.

ПОЧЕМУ ОЦЕНЯТ

6 Инновационная разработка
1. Алгоритм компании Biosmart.
2. Сочетание технических возможностей и дизайна.
3. Индивидуальные сценарии и решения под каждого заказчика.

7 Широкая интегрируемость
Возможность подключения к системам других производителей.

Производитель: ООО "Прософт-Биометрикс"
www.bio-smart.ru
Ценовой сегмент: средний
см. стр. 128 "Ньюсмейкеры"

Персональная облачная СКУД в каждой компании

Локальное облачное программное обеспечение для СКУД Guard Plus

Guard Plus

ЧТО УНИКАЛЬНОГО

1 Концепция локального облака
Guard Plus на локальном сервере организует частную облачную СКУД, которая полностью принадлежит клиенту, что позволяет ему самостоятельно обеспечивать желаемый уровень безопасности данных. Работа со СКУД происходит через любой браузер.

ЗАЧЕМ ПОКУПАТЬ

2 Выгодно всем
Проектно-монтажные организации оценят упрощенную установку на локальный сервер и понятный алгоритм настройки работы ПО с оборудованием. Конечные пользователи обратят внимание на современный дружелюбный интерфейс, возможность настраивать СКУД и просматривать отчеты из любой точки мира, где есть Интернет.

3 Удобный и надежный доступ
Организация единой СКУД на разнесенных друг от друга объектах. Доступ к информации по трудовой дисциплине и настройке системы из любой точки мира. Многопользовательский режим с разграниченными уровнями доступа.

4 Для бизнеса
ПО предназначено для малого, среднего и крупного бизнеса с развитой собственной локальной сетью.

ПОЧЕМУ ОЦЕНЯТ

5 Понятное и гибкое решение
Простота установки и эксплуатации, экономичность, кросс-платформенность, масштабируемость.

6 Веб-приложение
Обработка информации распределена между браузером и сервером.

Производитель: Iron Logic
Розничная цена: от бесплатно до 28 000 руб.
см. стр. 128 "Ньюсмейкеры"

Видеонаблюдение премиум-класса по доступной цене

IP-камеры серии AXIS M11

ЧТО УНИКАЛЬНОГО

1 Инновационный чип
Новое поколение недорогих камер AXIS M11 создано на базе инновационного чипа собственной разработки ARTPEC-7. Камеры имеют HD-разрешение 720p, 2 Мпкс или 5 Мпкс, частоту 30 кадр/с.

2 Четкая картинка в любых условиях
Технология Axis Lightfinder позволяет получать реалистичные цвета при слабом освещении, а Axis Forensic WDR обеспечивает четкое изображение, даже когда в кадре присутствуют одновременно темные и светлые области.

3 Поддержка H.264/H.265
Технология Axis Zipstream с поддержкой кодирования H.264/H.265.

ЗАЧЕМ ПОКУПАТЬ

4 Экономичный и быстрый монтаж
Серия AXIS M11 поддерживает технологию PoE и резервное питание постоянного тока, что обеспечивает гибкие возможности монтажа, позволяет не прокладывать дополнительные кабели и сохранить данные при отключении электричества. Камеры оснащены креплением CS, поэтому пользователи могут быстро заменить объектив в соответствии с определенными условиями и целями съемки.

5 Для административных и общественных зданий
Экономичные сетевые камеры AXIS M11 поддерживают все стандартные функции Axis и предназначены для охраны магазинов и складских помещений, школ, банков, офисных зданий, гостиниц и т.д.

ПОЧЕМУ ОЦЕНЯТ

6 Запись звука
Камеры AXIS M1134, AXIS M1135 и AXIS M1137 предназначены для установки в помещениях, оснащены встроенным микрофоном с возможностью записи звука, что позволяет прослушивать и записывать звук в заданной зоне.

7 Защита от воды, коррозии, пыли и ударов
Кожухи уличных камер AXIS M1135-E и AXIS M1137-E имеют степени защиты IP66, IK10 и NEMA 4X.

Производитель: Axis Communications см. стр. 128 "Ньюсмейкеры"

Видеокодеры с чипом нового поколения и поддержкой HD-аналога

AXIS M7104 и AXIS P7304

ЧТО УНИКАЛЬНОГО

1 Чип ARTPEC-7
Новые 4-канальные видеокодеры AXIS серий M71 и P73 оснащены чипом последнего поколения ARTPEC-7, который существенно улучшает функции кибербезопасности.

2 Технология ZipStream
AXIS M7104 и AXIS P7304 оснащены технологией Zipstream с поддержкой форматов сжатия видео H.264/H.265, что значительно снижает объем передаваемого трафика и затраты на хранение файлов, обеспечивая при этом высокое качество изображения.

3 Видеоаналитика
Устройства поддерживают функции интеллектуального анализа изображения, такие как детектор движения и оповещения при несанкционированном проникновении.

ЗАЧЕМ ПОКУПАТЬ

4 Функционал под задачу
AXIS M7104 представляет собой экономичный вариант видеокодера. Модель серии P73 дополнительно оснащена входами для внешних аналоговых или цифровых микрофонов, а также линейными выходами. Это устройство поддерживает двустороннюю передачу аудио и имеет функции обнаружения.

ПОЧЕМУ ОЦЕНЯТ

5 Управление PTZ
Порты RS-485/422 позволяют управлять аналоговыми PTZ-камерами с функциями панорамирования, наклона и зума.

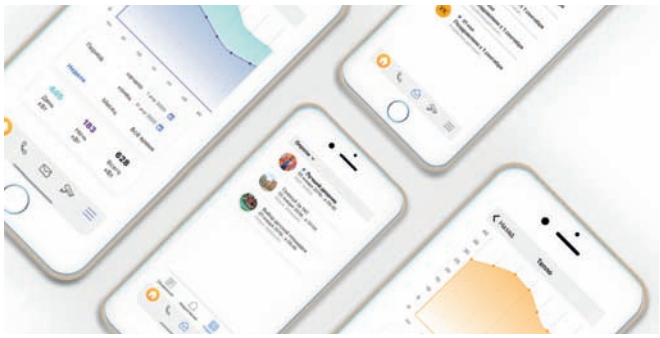
6 Открытая платформа
Как и другие продукты компании, AXIS M7104 и AXIS P7304 можно использовать в сочетании с оборудованием и ПО других поставщиков.

7 Варианты хранения данных
Видеокодеры предоставляют возможность сохранять данные на сервере, локальном диске или в облаке, а благодаря технологии PoE для прямого подключения к IP-сети и подачи питания требуется всего один сетевой кабель.

Производитель: Axis Communications см. стр. 128 "Ньюсмейкеры"

Облачно-цифровая платформа с элементами искусственного интеллекта

Система The Butler



ЧТО УНИКАЛЬНОГО

1 Интеграционные и функциональные возможности:

- контроль и управление доступом;
- просмотр камер видеонаблюдения;
- проверка показаний электроприборов и приборов учета воды/тепла;
- взаимодействие управляющей компании с собственниками через сообщения, заявки на сервис, голосование и опросы;
- интеграция со сторонними системами.

ЗАЧЕМ ПОКУПАТЬ

2 Диджитализация сервисов

Платформа позволяет, с одной стороны, свести в единую точку многие сервисы, которые предоставляются пользователям в разрозненном виде через различные системы, а с другой – автоматизировать процессы, выполняемые вручную на бумаге.

3 Платформа предназначена для:

1) компаний, строящих многоквартирные дома;
2) управляющих компаний многоквартирных ЖК, отелей, апартаментов и др.;
3) собственников загородных домов и таунхаусов.

Решения The Butler установлены и успешно функционируют в смарт-комплексах одного из ведущих застройщиков Санкт-Петербурга.

ПОЧЕМУ ОЦЕНЯТ

4 Высокотехнологичная начинка

В решении использованы SIP, FFMPEG, REST API, WEB, MongoDB, нейронные сети и другие технологии, работающие на платформах Linux, Android и iOS.

5 Адаптация под заказчика

Полная кастомизация дизайн-интерфейса и максимальная гибкость под нужды заказчика.

Производитель: ООО "АйТиФрог"
Ценовой сегмент: средний

см. стр. 127 "Ньюсмейкеры"

Интеллект. Качество. Прогресс

Тепловизор GIT M-серии

ЧТО УНИКАЛЬНОГО

1 Обнаружение и сопровождение 24/7

Интеллектуальный поворотный тепловизор круглосуточного обнаружения и сопровождения объектов с детектором людей и автотрекингом.

2 Виртуальный купол

Тепловизор создает виртуальный купол над защищаемым объектом, может автоматически сопровождать воздушные, наземные и надводные цели.

3 Мощные технические параметры

Модель обладает самой высокочувствительной в индустрии матрицей 35 мК с разрешением 640x512 пкс (VGA) и светосильным объективом с автофокусом.

ЗАЧЕМ ПОКУПАТЬ

4 Эффективность и гибкость

Тепловизор обладает оптимальным соотношением "цена/качество/эффективность". Создан в виде конфигуратора, адаптируемого под конкретную задачу.

5 Охрана особо важных, энергетических и транспортных объектов

Комплексное наблюдение за охраняемой территорией и воздушным пространством, обнаружение и сопровождение дронов, работа в паре с радиолокационной станцией. Снижение нагрузки на оператора.

ПОЧЕМУ ОЦЕНЯТ

6 Аналитика и интеграция

Полностью цифровой прибор со всеми современными аналитическими функциями и интеграцией по отраслевым стандартам ONVIF, H.265, H.265.

7 Высокая адаптивность

Ключевая особенность, заложенная в прибор, – адаптивность параметров тепловизора GIT M-серии под конкретную задачу и объект.

Производитель: ООО "ГИТ СИСТЕМС"
Розничная цена: зависит от конфигурации

см. стр. 128 "Ньюсмейкеры"

Безопасность реальна!

Новый полноростовой роторный турникет "ПР1/3М2"

ЧТО УНИКАЛЬНОГО

1 Модульный подход
Перевод СБ на модульную базу с целью унификации, взаимозаменяемости и создания предпосылок для дальнейшей стандартизации.

2 Бесшумная работа
Запатентованная производителем система доводки и фиксации делает работу механизма турникета плавной, бесшумной, долговечной. Имеется функция AntiPassBack.

3 Внедрение на 30% проще
Модульная система конструкции упрощает и облегчает сборку и последующую установку турникета на 30%. Наличие крепежных элементов, установленных в корпусе, обеспечивает стыковку турникета с полноростовым ограждением.

ЗАЧЕМ ПОКУПАТЬ

4 Лучшее соотношение "цена/качество"
Новый элегантный дизайн, компактные размеры и высокие эксплуатационные возможности по доступной цене.

5 Универсальное решение для проходных
Турникет подойдет для офисных и административных зданий, банков, учебных заведений, заводов и других объектов.

ПОЧЕМУ ОЦЕНЯТ

6 Три в одном
1. Новый элегантный дизайн.
2. Модульная система конструкции турникета.
3. Универсальность.

7 Удобный монтаж
Гибкая модульная конструкция упрощает и облегчает сборку и последующую установку турникета. Возможность стыковки с полноростовым ограждением.

Производитель: ООО ПК "РОСТЕВРОСТРОЙ"
Розничная цена: 287 740 руб. (бюджетный вариант)
см. стр. 128 "Ньюсмейкеры"

Самый умный из всех

Домофон R29C

ЧТО УНИКАЛЬНОГО

1 Надежный биометрический доступ
3D-распознавание лиц с функцией определения живого объекта, две камеры для обнаружения объема + ИК-датчик.

2 Локальное хранение
База хранится в зашифрованном виде, может использоваться в сетях, где нет доступа в Интернет.

3 Преимущества
- 10 уровней настройки строгости распознавания лиц.
- 4 способа идентификации пользователей (камера, ПИН, карта, BLE).
- ОС Android для легкой кастомизации.

ЗАЧЕМ ПОКУПАТЬ

4 Работа со сторонними решениями
Высокий уровень надежности и легкость интеграции с уже существующими системами, кастомизация начального экрана.

5 Объекты применения
- Жилые комплексы бизнес-класса и выше.
- Офисные центры класса B+ и выше.
- Удаленные объекты высокой важности с затрудненным доступом и регулярной сменой персонала (например, объекты с вахтовым методом работы).

ПОЧЕМУ ОЦЕНЯТ

6 Инновационность
- Собственный алгоритм распознавания лиц.
- Трехмерное распознавание с помощью двух камер.
- Считыватель BLE.
- 7" сенсорный экран.
- Поддержка Akuvox Cloud.

7 Локальное распознавание лиц
Биометрический доступ по лицу без использования внешних серверов распознавания (например, на буровых комплексах, где нет доступа в Интернет).

Производитель: Akuvox
Представляет InPrice Distribution
Розничная цена: 88 400 руб.
Ценовой сегмент: высокий
см. стр. 128 "Ньюсмейкеры"

Больше объектов меньшими силами

Беспроводная система охранно-пожарной сигнализации, оповещения и локализации "СТРЕЛЕЦ-ПРО"

ЧТО УНИКАЛЬНОГО

1 Больше возможностей
"СТРЕЛЕЦ-ПРО" обеспечивает пожарную безопасность объектов любой сложности, он оповещает о пожаре, управляет эвакуацией и определяет местоположение людей по персональным браслетам снаружи и внутри здания.

2 Глобальный роуминг
Благодаря технологии глобального роуминга (автовыбор машрута связи устройств) повышается живучесть системы и упрощаются процессы проектирования и пусконаладки.

3 Уникальность
10 лет работы батарей, время запуска оповещения – 3 с, 2000 устройств в системе, дальность связи – 1200 м.

ЗАЧЕМ ПОКУПАТЬ

4 Динамическое управление эвакуацией
В состав "СТРЕЛЬЦА-ПРО" входит беспроводная система динамического управления эвакуацией "Нить Ариадны", которая не только обнаруживает дым, но и оповещает о пожаре, указывает направление к безопасному выходу с помощью светозвуковой дорожки.

5 Типы объектов
- Жилые дома
- Торговые центры
- Промышленные предприятия и др.

ПОЧЕМУ ОЦЕНЯТ

6 Беспроводное решение
В данной разработке использованы последние достижения в области беспроводных технологий:
- глобальный роуминг и динамическая маршрутизация передачи сигналов;
- двухсторонний протокол обмена данными между устройствами;
- алгоритмы борьбы с помехами и замираниями.

Производитель: ООО "АРГУС-СПЕКТР"
Ценовой сегмент: средний
см. стр. 127 "Ньюсмейкеры"

Новое качество обслуживания систем охранной сигнализации

Вибрационный адресный охранный извещатель "С2000-В"

I место в номинации "Охранная сигнализация" в конкурсе "Лучший инновационный продукт" в рамках самой крупной в РФ международной выставки Securika Moscow 2019

ЧТО УНИКАЛЬНОГО

1 Автоопределение работоспособности
На плате извещателя установлен эталонный источник вибрации (вибромоторчик), который периодически формирует тестовые воздействия, позволяющие автоматически определять работоспособность чувствительного элемента и силу прижатия извещателя к защищаемой поверхности.

2 Передовой метод эксплуатации
Впервые обслуживание охранной сигнализации приближается по своей методике и обслуживанию к адресно-аналоговой пожарной сигнализации.

ЗАЧЕМ ПОКУПАТЬ

3 Оптимизация затрат
Использование меньшего количества извещателей для защиты особо важных помещений. Простота и снижение затрат на техническое обслуживание охранной сигнализации.

4 Экономия сил и времени
Отпадает необходимость в ежемесячной рутинной и крайне трудоемкой проверке проверке работоспособности извещателя.

5 Сохранность всех видов имущества
"С2000-В" предназначен для использования в банках, музейных фондах и помещениях хранения оружия.

ПОЧЕМУ ОЦЕНЯТ

6 Минимум ложных срабатываний
Чувствительный элемент – цифровой акселерометр. Современный процессор поддерживает мощный математический аппарат и благодаря этому позволяет защититься от ложных срабатываний. Активная акустическая самодиагностика.

7 Охраняемая площадь больше
Защищаемая площадь сплошной бетонной, железобетонной или кирпичной конструкции – до 30 кв. м, что в 3 раза превосходит соответствующий показатель обычных извещателей.

Производитель: ЗАО НВП "Болид"
Розничная цена: 1105 руб.
Ценовой сегмент: средний
см. стр. 127 "Ньюсмейкеры"

ЧТО УНИКАЛЬНОГО

1 16 000+ камер в одной системе
Решение QVR Pro с модулем QVR Center позволяет организовать распределенную систему видеонаблюдения, включающую в себя до 128 устройств и объединяющую свыше 16 000 камер.

2 Масштабируемость
Широкий потенциал масштабирования системы, собственный набор программных модулей расширения функционала. Взаимодействие с любыми сторонними решениями.

3 Наследование
Возможности интеграции с существующими решениями для видеонаблюдения от QNAP.

ЗАЧЕМ ПОКУПАТЬ

4 Защита людей и имущества
Платформа подойдет для любых отраслей, где нужна защита от внешних факторов и угроз, обеспечение безопасности людей (работающих, учащихся или отдыхающих), материальных ресурсов или ценностей.

5 Емкость системы
Зачастую требования вынуждают заказчика хранить видеоархив от 6 до 12 месяцев. Благодаря аппаратной платформе сетевого накопителя с возможностью подключения SAS-модулей расширения платформа QVR Pro может предложить систему с глубиной архива свыше 2200 Тбайт.

ПОЧЕМУ ОЦЕНЯТ

6 Легко настроить, удобно работать
Пользователи оценят удобство, информативность и простоту взаимодействия с платформой QVR Pro как на этапе установки, так и в процессе работы и дальнейшего масштабирования системы. После установки QVR Pro из центра приложений сетевого накопителя пользователю сразу доступно 8 базовых каналов для подключения IP-камер и запуска системы видеонаблюдения. Благодаря выверенному дизайну и набору инструментов платформа упрощает жизнь операторам и администраторам.

7 Возможности и производительность
Платформа поддерживает все необходимые протоколы для взаимодействия с камерами и обработки входящих и исходящих событий, включая интеграцию с IoT-ресурсами и распознавание лиц. Она предоставляет ряд программных интерфейсов для интеграции с существующими решениями клиентов.

Производитель: QNAP
qnap.ru
Розничная цена: зависит от конфигурации

см. стр. 128 "Ньюсмейкеры"

Комфортный проход для сотрудников и посетителей

Сенсорный барьер Argus 40/60/80

ЧТО УНИКАЛЬНОГО

1 Изящное решение
Современные сенсорные барьеры становятся частью дизайна интерьера офисов, сохраняя при этом весь свой функционал.

2 Особенности
1. Уникальный дизайн XEA.
2. Новые материалы (алюминий вместо нержавеющей стали).
3. Большой выбор цветов отделок, бесшумная работа.

3 Совершенство внутри и снаружи
Барьеры Argus имеют эргономичный дизайн, аккуратные стыки материалов, световые направляющие линии и подсветку прохода Ambilight. Модульность и наличие большого количества датчиков и настроек повышают их функциональность до уровня премиального продукта.

ЗАЧЕМ ПОКУПАТЬ

4 Все в одном устройстве
Эстетичный дизайн, широкая цветовая гамма, модульность, высокий уровень безопасности.

5 Высота створок на выбор
Барьеры могут быть выполнены как со стандартными створками высотой 900 мм, так и с высокими створками высотой 1200, 1400, 1600 или 1800 мм на выбор.

ПОЧЕМУ ОЦЕНЯТ

6 Высококлассное производство
Переход от тяжелой нержавеющей стали к легкому алюминию. Сенсорные барьеры (включая всю электронику) производятся на собственном заводе dormakaba в Германии.

7 Цветовая гамма
Доступны цвета Digital Silver, Corporate Satin, True White, Deep Black, Vector Edge, Core Steel, Organic Sand.

Производитель: dormakaba Deutschland GmbH
Розничная цена: 12 606,3 евро (с НДС)
Ценовой сегмент: средний
см. стр. 128 "Ньюсмейкеры"

Доступ по смартфону для всех

Программное обеспечение для мобильного доступа через дверь evolo smart

ЧТО УНИКАЛЬНОГО

1 Ничего лишнего
Решение для удобного администрирования и использования СКУД без карт и стационарного ПО.

2 Все, что нужно, – BLE
Доступ к двери по имеющему функционал BLE смартфону с любой ОС.

ЗАЧЕМ ПОКУПАТЬ

3 Без абонентской платы
Управление через бесплатное ПО, устанавливаемое на смартфон. Нет дополнительных затрат, кроме единоразовой покупки виртуального ключа – 379 руб. за постоянный ключ.

4 Для малых предприятий и жилого фонда
Готовое защищенное решение для малых объектов и жилого фонда.

ПОЧЕМУ ОЦЕНЯТ

5 Гибкое решение
Используется технология BLE (Bluetooth Low Energy) с настраиваемой дистанцией чтения ключа.

6 Понятное ПО
Простой процесс покупки и управления ключами пользователей.

Производитель: dormakaba GmbH (Германия)
Розничная цена: 378 руб. за постоянный ключ
см. стр. 128 "Ньюсмейкеры"

Мое лицо – мой пропуск

Биометрический терминал FaceStation 2 для СКУД и УРВ

ЧТО УНИКАЛЬНОГО

1 Биометрия + классика СКУД
Сочетание в одном устройстве современных биометрических и классических технологий идентификации.

2 4 неоспоримых преимущества
1. Качество.
2. Скорость.
3. Надежность.
4. Универсальность.

ЗАЧЕМ ПОКУПАТЬ

3 Бесконтактная биометрическая технология
Удобная и простая биометрическая идентификация на основе сканирования лица.

4 Удобно, безопасно, гигиенично
Замена идентификации сотрудника или посетителя по картам на идентификации по лицу. Лицо, в отличие от карты, нельзя забыть, потерять, передать другому, украсть.

5 До 30 000 пользователей
Терминал предназначен для объектов и компаний, где требуется СКУД на основе биометрии, – банки и офисы, промышленные предприятия, объекты транспорта и энергетики.

ПОЧЕМУ ОЦЕНЯТ

6 Заменяет несколько устройств
Может одновременно использоваться в качестве считывателя (карт, смартфонов, ПИН-кода), IP-видеодомофона, контроллера СКУД и терминала УРВ.

Производитель: Suprema
Ценовой сегмент: средний и высокий
Розничная цена: 84 000 руб.
Представляет "ААМ Системз"
см. стр. 127 "Ньюсмейкеры"

Шлагбаум PERCo GS04

Контроль въезда на территорию

ЧТО УНИКАЛЬНОГО

1 Широкий диапазон рабочих температур
Встроенная система обогрева механизма управления обеспечивает работу шлагбаума при температуре -40…+55 °С.

2 Гарантийный срок – 5 лет
Увеличить срок эксплуатации позволяют защита механизма управления при наезде автомобиля и двигатель с планетарным редуктором.

ЗАЧЕМ ПОКУПАТЬ

3 Удобство управления
Шлагбаум может управляться с помощью пульта ДУ, радиобрелоков или от СКУД. Функция управления по звонку и через мобильное приложение будет реализована в III квартале 2020 г.

4 Быстро и надежно
- Скорость открытия – 3–6 с.
- Пропускная способность – 3000 автотранспортных средств в сутки.

5 Универсальность применения
Шлагбаум устанавливается при въезде на территорию промышленных предприятий, торговых и бизнес-центров, коттеджных поселков, жилых комплексов, автостоянок. Модульность конструкции позволяет подобрать шлагбаум к различной ширине проезда.

ПОЧЕМУ ОЦЕНЯТ

6 Удобство настройки
Плата управления находится в верхней части тумбы под съемной крышкой, что удобно при конфигурации шлагбаума.

7 Защита автомобиля
Наличие сигнальной индикации, буферной накладки стрелы и предустановленного фотоэлемента.
Изменение направления движения стрелы при обнаружении препятствия.

Производитель: PERCo
Ценовой сегмент: средний
см. стр. 128 "Ньюсмейкеры"

Николай Махутов
Руководитель комиссии РАН по техногенной безопасности, член-корр. РАН, д.т.н., проф.

Таисия Шепитько
Директор Института пути, строительства и сооружений МИИТ, почетный транспортный строитель РФ, д.т.н., проф.

Владимир Балановский
Член комиссии РАН по техногенной безопасности, действ. член АПК и ВАНКБ, проф. Академии военных наук

Алексей Авдонов
Генеральный директор ООО "Интерправо Инвест"

Игорь Грунин
Руководитель Экспертно-аналитического центра инженерно-технического аудита ООО "Технологический институт "ВЕМО"

Нина Николаева
Помощник члена Совета Федерации

Владимир Подъяконов
Член комиссии РАН по техногенной безопасности, член Экспертного совета Комитета ГД по региональной политике и проблемам Севера и Дальнего Востока, к.и.н.

Противодействие вызовам гибридной войны

Анализ практики обеспечения безопасности на транспортно-пересадочных узлах

Комиссия РАН по техногенной безопасности совместно с Академией военных наук провела анализ воздействия природных, техногенных факторов и актов незаконного вмешательства на транспортно-пересадочные узлы, в ходе которого выявлены новые виды угроз, реализуемые в ходе гибридных войн, и определены пути повышения эффективности обеспечения безопасности транспортно-пересадочных узлов

В современных условиях повышается значимость обеспечения безопасности на объектах транспортной инфраструктуры

Основными чертами XXI века является нарастание и распространение новых форм противоборства между Россией и США. Гибридная война против России и ее союзников в настоящее время приняла ожесточенную форму. В результате изменения баланса военных и невоенных видов борьбы на современном этапе гибридная война фактически становится новой формой межгосударственного противоборства.

Расстановка приоритетов

Появление новых изощренных форм агрессии обусловливает необходимость заблаговременного создания механизмов нейтрализации негативного влияния внешних вмешательств и внутренних экстремистских действий. Вопросы противодействия гибридной войне как новой форме межгосударственного противостояния должны быть выделены в качестве одного из приоритетных направлений научно-технических исследований.

Проблемы развития транспортной системы России с позиции обеспечения национальной безопасности целесообразно оценивать через призму соблюдения стратегических национальных приоритетов, которые обозначены в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации № 683 от 31.12.2015 г.

В условиях резко меняющейся внешней и внутренней политической, национальной и общественной обстановки, повышения вероятности природных и техногенных деструктивных воздействий, АНВ, в том числе терактов, на объектах транспортной инфраструктуры (ОТИ) РФ повышается значимость обеспечения безопасности и их мобилизационной готовности.

Транспортный комплекс РФ вынужден решать сложнейшую проблему, связанную с массовым созданием транспортно-пересадочных узлов (ТПУ) – комплексов, осуществляющих перераспределение пассажиропотоков между различными видами транспорта и попутное обслуживание объектами социальной инфраструктуры

Тотальная разобщенность

Транспортный комплекс РФ вынужден решать сложнейшую проблему, связанную с массовым созданием транспортно-пересадочных узлов (ТПУ) – комплексов, осуществляющих перераспределение пассажиропотоков между различными видами транспорта и попутное обслуживание объектами социальной инфраструктуры. На сегодняшний день хаотично сложилась и действует обширная сеть ТПУ различных видов.

Они включают в себя элементы с совершенно различными целями – ОТИ, торгово-развлекательные комплексы (ТРК), объекты городской инфраструктуры. Их строительство – очень сложная и дорогостоящая задача, особенно на существующих ОТИ, где плотная застройка и действуют градостроительные ограничения.

Когда ТПУ строится частным инвестором, ему для компенсации затрат выделяются коммерческие площади – ТРК или подобные объекты, которые сдаются в аренду множеству организаций разных форм собственности. При этом нарушаются основные принципы формирования безопасности на территории ТПУ:

- отсутствует единая законодательная и нормативно-техническая база;

Проблемы развития транспортной системы России с позиции обеспечения национальной безопасности целесообразно оценивать через призму соблюдения стратегических национальных приоритетов, которые обозначены в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации № 683 от 31.12.2015 г.

- соблюдаются только финансовые интересы инвесторов;
- отсутствует ответственность владельцев ТРК перед владельцами других элементов ТПУ и государством;
- на площадке несколько хозяев, действующих разобщенно, внутри ТРК могут быть сотни арендаторов;
- неэффективное взаимодействие, приводящее к полному отсутствию ответственности за безопасность эксплуатации отдельных частей ТПУ.

Существенные осложнения в оптимизации построения ТПУ вызываются наличием диаметрально противоположных требований к функционированию его отдельных частей

ТПУ "Саларьево" с торгово-развлекательный комплексом

Существенные осложнения в оптимизации построения ТПУ вызываются наличием диаметрально противоположных требований к функционированию его отдельных частей.

Транспортная часть ТПУ должна создаваться с учетом минимизации времени пребывания людей (пассажиров) на территории ОТИ, в то время как основная цель ТРК – обеспечить максимальное время пребывания посетителей (потенциальных покупателей) на его территории. Соответственно, разнятся угрозы, цели и задачи нарушителей – реализаторов АНВ. На территории ТПУ постоянно находится большое количество людей, что требует эффективного комплексного подхода к обеспечению их безопасности. АНВ в деятельность ТПУ остаются уязвимой областью транспорта и мобилизационной готовности РФ. Положение особенно обостряется в условиях гибридной войны.

Реализация проектов крупномасштабных ТПУ, включающих в себя объекты городской и транспортной инфраструктуры нескольких видов транспорта, диктует принципиально новые постановки проблемы обеспечения надежности и комплексной безопасности проектируемых и эксплуатируемых объектов с учетом потенциальной опасности и возможных крупномасштабных ущербов от природных и техногенных аварий, актов незаконного вмешательства, в том числе терактов.

Безопасность архитектурно- и объемно-планировочных решений

В процессе анализа уже спроектированных ТПУ становится ясно, что появился новый вид безопасности – безопасность архитектурно-планировочных и объемно-планировочных решений объекта. Задача осложняется тем, что законодательные акты и нормативно-техническая документация в части обеспечения безопасности ТПУ отсутствуют. Архитекторы разрабатывают архитектурно-планировочные и объемно-планировочные решения без учета специфических требований к ТПУ как комплексу, включающему в себя ОТИ. Это приводит к дублированию и параллельному формированию отдельных, не связанных между собой, систем безопасности объектов различных инфраструктур (городского и междугородного транспорта, городских объектов, ТЭК, ТРК) и не позволяет сформировать единый для всех объектов системный подход к противодействию АНВ и антитеррористической защите. На территории ТПУ расположены объекты транспортной и городской инфраструктуры различного функционального назначения, для которых необходимо определить требования по обеспечению безопасности, структурированные применительно к территориальной и функциональной структуре ТПУ. Безопасность этих объектов прямо сказывается на общественно-политической жизни страны, ее социально-экономическом развитии и обеспечении национальной безопасности. Концентрация промышленных предприятий вокруг ТПУ обостряет проблему обеспечения их безопасности, а недостатки систем могут использоваться террористическими и криминальными элементами для деструктивного воздействия на системы жизнеобеспечения и их критически важные элементы.

Отсутствие комплексного подхода

Перед транспортным комплексом стоят разноплановые задачи, поэтому он нуждается в комплексном использовании лучших практик по различным направлениям. При таком подходе оптимальное комплексирование методов технологии безопасности с целью консолидации ресурсов, создание схем эффективного совместного использования различных методов, их сочетание с ресурсосберегающими технологиями позволяет повысить надежность принимаемых проектных решений при фиксированных затратах, положительно решить ключевую проблему безопасности – планово-убыточности (сделать безопасность как минимум самоокупаемой).

В настоящее время отсутствуют единые комплексные подходы по согласованному решению вопросов обеспечения безопасности подобных объектов. Различные аспекты общей системы безопасности находятся в ведении различных ведомственных структур, не обеспечивая необходимую координацию решения вопросов на разных уровнях и в разных зонах ответственности, что провоцирует появление "слабых звеньев" в системе защищенности, нерациональность и дисбаланс затрат при построении отдельных сегментов системы безопасности. Отсутствует возможность отбора рациональных решений из имеющегося множества приемлемых вариантов в каждом конкретном случае с получением синергетических эффектов.

Когда ТПУ строится частным инвестором, ему для компенсации затрат выделяются коммерческие площади – ТРК или подобные объекты, которые сдаются в аренду множеству организаций разных форм собственности. При этом нарушаются основные принципы формирования безопасности на территории ТПУ

Анализ обеспечения безопасности транспортной системы России, с учетом ее интеграции в ТПУ в условиях деструктивного воздействия на них природных и техногенных факторов, АНВ, в том числе терактов, показывает, что при решении проблемы общественной безопасности на транспорте необходимо провести изучение и согласование различных регламентирующих эти вопросы законодательных актов с учетом ФЗ №184 от 27.12.2002 г. "О техническом регулировании", определяющего виды безопасности, содержание и применение технических регламентов. На уровне законодательных и нормативно-правовых актов должно быть проведено разграничение зон ответственности между задачами физической и антитеррористической защиты, при этом система физической защиты должна быть ориентирована на противодействие именно проектной угрозе объектам транспортной инфраструктуры.

Неотложные вопросы нормативно-правового регулирования

Нормативная и регулирующая деятельность защиты от АНВ в мировой практике имеет преобладающий реагирующий характер. События АНВ являются редкими, с вероятностью около $P = 10^{-8}$, примерно на два порядка более редкими, чем общая статистика транспортных происшествий. Задача принципиально усложняется, поскольку нарушитель находится в потоке пассажиров с вероятностью около 10^{-7}. Он может отсутствовать среди пассажиров транспорта, если было намерение заложить взрывное устройство и не ехать. Нарушителем может быть пассажир или работник транспорта. Описание формализованных условий блокирования угроз, контура защиты и исключение события АНВ нужно для обеспечения безопасности ТПУ. Необходимо установление единообразного порядка нормативно-правового регулирования в области обеспечения безопасности на территории ТПУ с учетом специфики формирования архитектурной среды – безопасности архитектурно-планировочных и объемно-планировочных решений объекта. Таким образом, становится очевидно, что архитектор должен быть одним из главных творцов не только совершенного с эстетической стороны, но и безопасного ТПУ как объекта городской архитектуры.

Настало время совершенствовать архитектурные объемно-планировочные решения и инженерные системы ТПУ, делая их более защищенными от проявления АНВ. ТПУ характеризуется большим количеством распределенных объектов сложной функциональности и интеграции со смежными системами (различными инженерно-техническими подсистемами, каналами связи), требующих комплексного подхода при разработке систем безопасности. Характерным является положение, связанное с тем, что в настоящее время существуют законодательные требования к антитеррористической защищенности объектов транспортной инфраструктуры (ОТИ) в целом, но нет сводов правил обеспечения антитеррористической защищенности зданий и сооружений ОТИ, а также нормативно-технических требований к разработке мероприятий по противодействию террористическим актам на территории зданий и сооружений ОТИ, что особенно важно применительно к их инженерным системам. Важным является установление единообразного порядка нормативно-правового регулирования в области обеспечения безопасности на территории ОТИ с учетом специфики формирования архитектурной среды – безопасности архитектурно-планировочных и объемно-планировочных решений объекта. Необходимо управление качеством систем комплексной безопасности ТПУ как многофункциональных комплексов, с учетом безопасности их объемно-пространственных решений.

Значимость отделочных материалов

Безопасность пребывания людей в зданиях ТПУ обеспечивается, среди прочего, выбором применяемых конструктивных и отделочных материалов. Ввиду того, что ТПУ относится к объектам, разрушение которых может привести к большим социальным, экологическим и экономическим потерям, при проектировании должно быть предусмотрено недопущение прогрессирующего обрушения.

Важен выбор применяемых отделочных материалов, которые представляют собой дополнительную опасность в случае проведения актов незаконного вмешательства (АНВ) с использованием взрывчатых веществ. Объемно-компоновочные решения, зонирование отдельных элементов ТПУ также должны отвечать требованиям безопасности.

Основные этапы создания ТПУ с учетом требований управления качеством

Управление качеством систем комплексной безопасности транспортно-пересадочных узлов с учетом безопасности объемно-пространственных решений
Разработка методологии определения производственно-экономического уровня систем комплексной безопасности с учетом специфики безопасности архитектурно-планировочных и объемно-планировочных решений по показателям стоимости и технологичности их создания, надежности, электромагнитной совместимости и др. Позволяет прогнозировать динамику развития вариантов систем комплексной безопасности ТПУ и сформировать перспективные требования к ним при создании новых поколений систем
Разработка методологии оптимизации структуры и параметров систем комплексной безопасности ТПУ с учетом специфики формирования безопасности архитектурно-планировочных и объемно-планировочных решений. Позволяет вырабатывать компромиссные архитектурно-конструктивно-технологические решения в интересах всего процесса создания многоуровневых и многофункциональных систем комплексной безопасности за счет системного согласования экономического критерия оптимальности и технических показателей качества, учитывающих условия разработки, производства и эксплуатации ТПУ
Разработка методологии структурного и параметрического синтеза, обеспечивающей оптимизацию различных вариантов межблочного комплексирования систем безопасности ТПУ, создающей возможность минимизации технологических затрат на их производство, обеспечивающей возможность формирования высокоэффективных многоуровневых систем комплексной безопасности ТПУ
Разработка комплекса экономико-математических и физико-математических моделей и методик для расчета, анализа и оптимизации стоимостных и конструктивных параметров и показателей качества перспективных вариантов систем комплексной безопасности ТПУ. Позволяет формировать эффективные алгоритмы автоматизированного решения задач синтеза, отличающихся высокой размерностью и недостаточностью информации со стороны архитектурной части проекта, для совершенствования принимаемых решений и генерирования вариативных предложений по оптимизации структуры проекта ТПУ на всех уровнях детализации
Разработка общесистемных и частных алгоритмов синтеза вариантов систем комплексной безопасности ТПУ, основанных на применении метода дискретного программирования, ранжирования определяющих фиксируемых и управляемых параметров, эвристических приемов направленного перебора возможных вариантов и интерактивного режима обработки информации, обеспечивающих решение задач структурной и параметрической оптимизации систем комплексной безопасности ТПУ за минимальное время
Разработка принципов построения специального программного обеспечения для синтеза вариантов систем комплексной безопасности ТПУ с учетом специфики безопасности объемно-пространственных решений и организации функционального взаимодействия программных компонентов моделирования электромагнитных, теплофизических, механико-прочностных процессов для реализации системного подхода к оптимизации структуры и параметров систем комплексной безопасности ТПУ и повышения экономической эффективности, технического уровня, качества разработки и производства перспективных систем комплексной безопасности

Архитекторы разрабатывают архитектурно-планировочные и объемно-планировочные решения без учета специфических требований к ТПУ, включающим ОТИ, что приводит к дублированию и параллельному формированию отдельных, не связанных между собой, систем безопасности объектов различных инфраструктур: различных видов транспорта, городских объектов, ТЭК и т.д. Это не позволяет сформировать единый для всех объектов многофункциональных комплексов системный подход к противодействию АНВ и к антитеррористической защите

Требуемая система государственных мер

Защита жизни и здоровья людей на территории ТПУ от АНВ, в том числе терактов, а также от чрезвычайных ситуаций природного и техногенного характера возможна только с помощью реализации определяемой государством системы правовых, экономических, организационных и иных мер, соответствующих угрозам. Эта система мер предусматривает:

- проведение оценки уязвимости объектов;
- их категорирование;
- разработку планов обеспечения безопасности;

- реализацию организационных и технических мероприятий в соответствии с утвержденными планами обеспечения безопасности на территории ОТИ (организацию досмотра пассажиров, транспортных средств, груза, багажа, ручной клади и личных вещей).

Применительно к ТРК необходимо разработать соответствующие аналогичные подходы к реализации мер безопасности. Уже на стадии проектирования этих разноплановых объектов все меры должны реализовываться по единой методике и вне зависимости от характера объекта предусматривать общие подходы к зонированию и выявлению критических элементов объектов. Это позволит избежать положения, когда часть готового ТПУ не имеет хозяина и лица, ответственного за реализацию мер по противодействию АНВ. Существует множество неучтенных обстоятельств, которые необходимо рассматривать как условия для формирования угроз АНВ. Например, стоянки личного транспорта не рассматриваются с точки зрения угрозы проведения АНВ на территории объектов ТПУ.

Безопасность ТПУ обеспечивается, среди прочего, выбором конструктивных и отделочных материалов

Оптимизация и согласование всех систем и процессов

Уже существует и в перспективе предполагается сохранение разделения синтеза систем комплексной безопасности на внутриблочный, межблочный и внешний. Для повышения эффективности систем комплексной безопасности особое внимание необходимо уделять межблочному синтезу, который занимает наиболее значительный объем конструкций систем комплексной безопасности и имеет высокую трудоемкость (стоимость) производства. Объемно-компоновочные решения, зонирование отдельных элементов ТПУ также должны отвечать требованиям безопасности. При этом необходимо учитывать роль систем комплексной безопасности, которые не существуют сами по себе, а создаются для защиты объекта, облик которого формируется архитектором еще на стадии концептуальной проработки проекта, на основе технического задания и задания на проектирование.

Таким образом, появляется возможность оптимизации и согласования всех систем на самых ранних стадиях, с учетом предъявляемых к ТПУ, порой взаимоисключающих, требований. Системы комплексной безопасности должны являться развитием, органичным дополнением, быть интегрированы в архитектурный облик ТПУ. Они представляют собой элементы городской инфраструктуры, обеспечивающие ее мобилизационную готовность, что вызывает усиление тенденции к расширению сети систем комплексной безопасности, обладающих различными вариантами конфигурации. Основные этапы этой работы определяются исходя из управления качеством систем комплексной безопасности ТПУ с учетом безопасности их объемно-пространственных решений.

Анализ позволяет наметить комплексы работ, результаты которых являются основой для формирования архитектурной среды ТПУ с учетом требований безопасности архитектурно-планировочных и объемно-планировочных решений. Такой подход, когда оптимизируется деятельность абсолютно всех участников процесса разработки систем комплексной безопасности ТПУ и впервые используется опыт архитекторов по формированию безопасных объектов городской архитектуры, позволяет получить синергический эффект и улучшить производственно-экономические показатели. С другой стороны, это дает возможность надежно парировать деструктивные воздействия на ТПУ факторов различной природы, значительно повысить способность локализовать последствия чрезвычайных ситуаций и ликвидировать их.

3 направления действий

Можно наметить основные пути исправления имеющихся в настоящем недостатков:

1. Формирование вокруг ОТИ ТПУ, их моделирование, создание для них единых систем безопасности и ситуационных центров, входящих в распределенную сеть.
2. Стратегическое планирование и прогнозирование, проактивный, предупредительный подход к разработке способов обеспечения безопасности. Применение методов управления изменениями и проектами, мониторинг, анализ, прогнозирование и управление рисками и стойкостью ТПУ. Использование "террористического форсайта" для формирования угроз, технологий, оборудования и сценариев, которые могут быть использованы при АНВ.
3. Управление персоналом на основе методов управления качеством для минимизации уязвимостей ТПУ, связанных с некомпетентностью и/или нелояльностью сотрудников. Повышение результативности действий персонала путем эффективной организации и обеспечения процессов его отбора, оценки, разработки практико-ориентированного повышения квалификации и подготовки персонала сил обеспечения безопасности и всего персонала ТПУ. Повсеместное обучение по программам "Культура безопасности".

Необходимо организационное объединение, технологическая интеграция, системное комплексирование аппаратно-программных комплексов, обеспечивающих деятельность в рамках этих направлений, в единую систему управления изменениями качества безопасности. Реализация взаимосвязанного и согласованного комплекса мероприятий на ТПУ на новом научно-технологическом уровне должна привести к максимально высоким результатам в обеспечении безопасности.

Список литературы

1. Градостроительный кодекс Российской Федерации от 29.12.2004 г. № 190-ФЗ (ред. от 31.12.2014 г., с изм. и доп., вступ. в силу с 01.04.2015 г.). http://www.minstroyrf.ru/upload/iblock/263/Градостроительный кодекс.pdf.
2. Балановский В.Л., Любимов К.М., Мануилов Н.Н., Власов Д.Н., Бахирев И.А., Попова Е.В. Управление качеством систем комплексной безопасности транспортно-пересадочных узлов с учетом безопасности объемно-пространственных решений // Качество и жизнь. 2016. № 3.
3. Бартош А. Гибридная война – новый вызов национальной безопасности России // Национальная оборона. 2019. № 9. С. 82–86.
4. Бойцов Б.В., Балановский В.Л., Шепитько Т.В., Денисов В.В., Лысов Д.А. Инструменты внедрения инноваций в сфере безопасности транспортных комплексов // Качество и жизнь. 2018. № 4 (20).
5. Бойцов Б.В., Балановский В.Л., Шепитько Т.В., Денисов В.В., Щербина В.И. Обеспечение безопасности городских объектов транспортной инфраструктуры // Качество и жизнь. 2018. № 4 (20).
6. Власов Д.Н. Транспортно-пересадочные узлы крупнейших городов (на примере Москвы): моногр. / Д.Н. Власов. – М.: АСВ, 2009.
7. Власов Д.Н. Структура и состав нормативных требований к городским транспортно-пересадочным узлам // Градостроительство. 2015. № 3 (37).
8. Данилина Н., Власов Д. Система транспортно-пересадочных узлов и "перехватывающие" стоянки: моногр. / Н. Данилина, Д. Власов. – Германия, LAP LAMBERT Academic Publishing, 2013. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Умный город: "цифра" или система взаимоотношений?

Концепция умного города (Smart City) зародилась в мировой урбанистике в конце 1990-х гг., прежде всего как внедрение информационных технологий в городскую инфраструктуру, и претерпела существенное развитие до современной модели, предусматривающей не только различные способы применения умных технологических решений, но и активное вовлечение жителей и бизнеса в их развитие. Сегодня умный город – это цифровизация и модернизация городской инфраструктуры и услуг в целях улучшения социальных, экономических и экологических условий жизни людей и повышения привлекательности и конкурентоспособности городов

Ирина Генцлер
Директор направления
"Городское хозяйство"
Фонда "Институт экономики города", к.т.н.

Татьяна Лыкова
Главный специалист направления
"Городское хозяйство"
Фонда "Институт экономики города"

На практике сосуществуют два подхода к оценке уровня интеллектуальности города и рейтингованию умных городов:

- первый учитывает степень развитости и применения информационных и коммуникационных технологий (ИТ), наличие электронных сетей, вовлеченность Интернета в городскую среду и т.д.;
- второй рассматривает результат воздействия ИТ на город в формате комплексных показателей уровня развития и интеграции сфер городского хозяйства, пригодности городской среды для жизни, а также степени доступности услуг для населения, наличия обратной связи с горожанами и уровней их участия, осведомленности и т.д.

Подходы разные – цель одна

В рамки первого подхода укладываются "родственные" понятию умного города более узкие концепции, такие как цифровой город (Digital City), интеллектуальный город (Intelligent City) и информационный город (Information City), которые выделяют цифровизацию как главную отличительную черту умного города. Подходы к разработке и реализации ведомственного проекта Минстроя России "Умный город" в рамках национальной программы "Цифровая экономика" показывают, что в России концепция умного города также понимается как цифровизация, развитие определенных умных технологий и их внедрение в городскую инфраструктуру.

Другой подход трактует умный город ближе к понятию устойчивого города (Sustainable City), стремящегося к балансу между развитием городских пространств, защитой природной среды и достижением справедливого распределения доходов, занятости, а также качества муниципальных, коммунальных и транспортных услуг.

На наш взгляд, многочисленные концепции умного города – это концентрация на отдельных элементах единой системы, в которую включены не только объекты цифровизации (город в целом, отдельные виды городской инфраструктуры или городских сервисов, конкретные городские здания или сооружения и т.д.), но и ее субъекты (органы городского управления, городское сообщество, организации/бизнесы, жители), связанные определенными взаимоотношениями. При таком подходе умный город – это умные инфраструктура, пространства, здания и умные люди.

Иерархия и функции объектов и субъектов

Умный город как система объектов и субъектов, взаимосвязей и взаимоотношений между ними показан на схеме. Она представляет иерархию объектов воздействия со стороны информационных технологий от умной квартиры до умной системы городского управления и субъектов от одного человека до городского сообщества и муниципалитета.

Каждый субъект умного города имеет и проявляет определенную заинтересованность в развитии и повышении комфортности пользования объектами разного уровня и, соответственно, может хотеть, чтобы эти объекты стали умными. Кроме того, есть еще деятельность самих субъектов, которая может стать умной и более эффективной, в том числе может позволять своевременно принимать правильные решения. Таким образом, для формирования умного города требуются техника и технологии для использования не только на материальных объектах (зданиях, элементах инфраструктуры и др.), но и в деятельности человека и общества.

Каждый субъект в системе может выполнять разные функции. Максимальное число таких функций выполняет город в лице органов местного самоуправления и городских организаций. Они одновременно могут быть заказчиком или покупателем ИТ, использовать ИТ для управления своей деятельностью и оказания муниципальных услуг бенефициарам – гражданам, сообществу. Отдельный человек в этой системе может быть покупателем ИТ, пользователем, бенефициаром, а также быть интегрированным участником, наполняя систему данными.

Опережающее развитие информационных технологий

Следует отметить, что сегодня формирование умного города в меньшей степени зависит от муниципалитета, городского сообщества или его отдельных представителей, чем от ИТ-компаний, поскольку именно они генерируют идеи и технологии. Информационные технологии развиваются стремительными темпами, ежедневно на рынок поступает множество предложений как по самим технологиям, так и по техническому оснащению для их использования. Создается впечатление, что на любой запрос со стороны потребителей уже существует или очень быстро может быть разработан ответ в виде специального гаджета или приложения к уже существующему универсальному гаджету. При этом разработчики в силу своей профессиональной подготовки, знаний и пользовательской продвинутости по сравнению с обычными людьми ориентируются не только и даже не столько на текущие запросы, транслируемые существующими потребителями, сколько на свои представления о запросах со стороны гипотетического потребителя – интегрированного, осведомленного, восприимчивого и "жадного" до обновлений. Технологии опережают запросы и уровень подготовленности остального сообщества. Например, сегодня обычные граждане – владельцы смартфона используют далеко не все его функции, встроенные по умолчанию, и пользуются весьма ограниченным набором скачиваемых приложений. Для многих смартфон – это просто замена городского телефона. В то же время смартфон может стать частью систем умного города, будучи оснащен рядом датчиков и сенсоров, с ведома или без ведома пользователя встроенных в широкую интернет-инфраструктуру для сбора и обобщения данных, например о городской миграции, работе транспорта, здравоохранения, социальных офисов и разной другой информации.

Сдерживающие факторы и ограничения

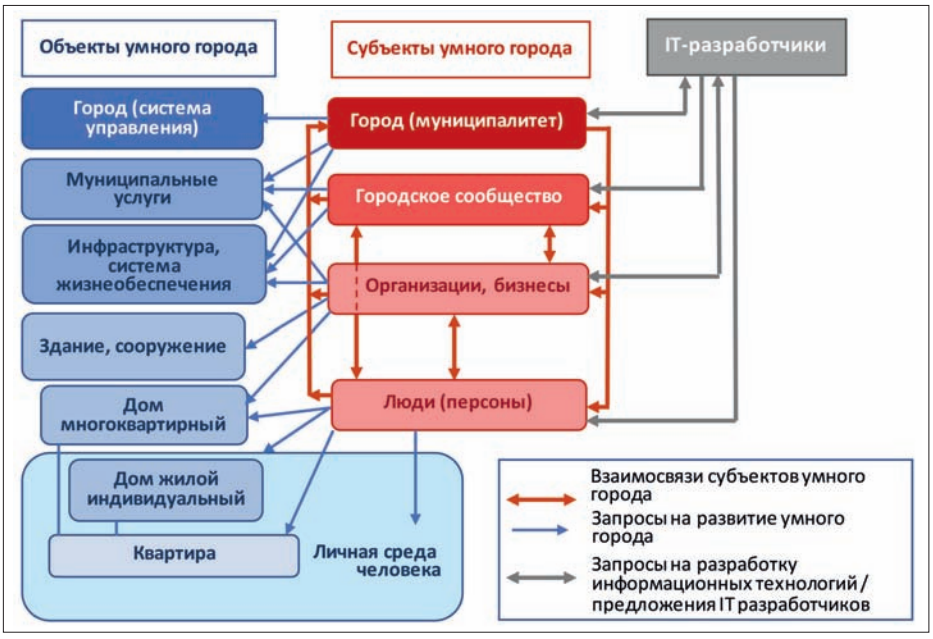
На развитие умного города влияют не только технологические, но и экономические, социальные, организационные, а иной раз и правовые

факторы: доступна ли умная технология приобретателям финансово, осознают ли они ее полезность и необходимость, готовы ли они интеллектуально и эмоционально изменить сложившиеся привычки и практики и перейти на новые технологии, кто принимает решение о внедрении новой технологии – одно лицо или множество лиц, нет ли правовых барьеров для создания той или иной умной системы, и т.д.

Практически все участники приведенной выше системы взаимоотношений имеют определенные ограничения, прежде всего финансовые, для того чтобы приобретать и пользоваться умными технологиями. В отношении людей это возможность или невозможность иметь компьютер или смартфон с выходом в Интернет. В отношении большинства городов – невозможность в короткий период времени сделать все городские системы умными из-за бюджетных ограничений.

Примером правовых ограничений можно считать нормы жилищного законодательства, которые сегодня препятствуют развитию умного ЖКХ, которое воспринимается многими прежде всего как умные городские системы ресурсоснабжения и повсеместная установка интеллектуальных систем управления и учета потребления коммунальных ресурсов. Барьер связан с тем, что законодатель определил общедомовой прибор учета как общее имущество собственников помещений в многоквартирном доме. Согласно закону, система приборного учета потребления ресурсов в многоквартирном доме принадлежит собственникам помещений и может быть установлена только по их решению. Кроме того, собственники должны утвердить расходы не только на установку системы, но и на ее последующее обслуживание и замену. Для создания умной общедомовой системы нужно не только общее решение всех собственников, но и готовность каждого собственника впустить установщиков в свою квартиру для установки индивидуальных приборов как конечного элемента системы. Несогласие даже одного человека делает бессмысленной общедомовую систему в целом. Таким образом, коммунальное предприятие, создавая умную инфраструктуру, не может замкнуть всю технологическую цепочку поставки коммунального ресурса, поскольку на границе раздела отсутствует учет потребления, принадлежащий предприятию.

Помимо системы учета потребления ресурсов любое решение о внедрении тех или иных умных решений в многоквартирном доме также должно приниматься собственниками на общем собрании, вплоть до решения о проведении тех самых общих собраний с использованием информационных технологий. Поэтому сегодня в российских городах сделать умным индивидуальный дом или квартиру проще, чем многоквартирный дом.



Умный город как система объектов и субъектов, взаимосвязей и взаимоотношений между ними

Необходим комплексный подход

Умный город в идеале – это единая умная система, в которой все взаимосвязано и все умны. Сегодня же на практике опережающими темпами "умнеют" одни городские сферы, а другие отстают. Это подтверждается в том числе различными международными рейтингами умных городов, которые оценивают степень интеллектуальности города по совокупности отдельных умных городских отраслей. В России (возможно, потому, что наша страна позже других приступила к созданию умных городов) акцент делается на цифровизации, которую можно внедрить административными методами, а это чревато тем, что конечные цели не будут достигнуты. Из виду зачастую упускаются такие аспекты, как потенциальный охват городских жителей внедряемыми цифровыми технологиями, готовность людей воспринять и применять новое, а также экономическая доступность умных технологий для российских городов и жителей страны.

Необходим комплексный подход и разработка дорожной карты в качестве первого шага на пути создания умного города. При этом в условиях ограниченности ресурсов и необходимости поиска наиболее эффективных решений, влекущих устойчивые результаты, муниципалитеты все равно вынуждены будут расставлять приоритеты и принимать решения о том, какую городскую сферу сделать умной вперед других. При этом муниципалитет должен будет понимать, насколько востребовано выбранное решение и будет ли купленная технология применяться и в каком масштабе. Когда нет возможности приобрести сразу большой объем софта и крупномасштабную информационную инфраструктуру и приходится выбирать какие-либо отдельные решения с возможностью их развития, модификации и дополнения в дальнейшем, у руководителя города есть варианты: принять решение на основании собственного представления о том, что нужно населению, или вовлечь городское сообщество в обсуждение потребностей и приоритетов.

10 вопросов перед цифровизацией

Выбор направления движения к технологии умного города – это не просто отношения типа "заказ – поставка" между администрацией города и ИТ-разработчиками, а диалог между администрацией города и городским сообществом. А значит, умные цифровые технологии нуждаются в умных социальных технологиях – партисипаторном бюджетировании, соучаствующем проектировании, социальном партнерстве.

Важно ответить на следующие вопросы:

1. Кто заказчик, а кто пользователь?
2. Есть ли сформулированный спрос на данную технологию от данной категории пользователей?
3. Насколько пользователь сам является умным, то есть осведомленным и интеллектуально подготовленным для того, чтобы применять умную технику и технологию?
4. В какой степени пользователь готов стать частью систем умного города? Есть ли у него необходимая степень доверия к тем, кто внедряет умную технологию, чтобы позволить считывать свою информацию без персонального участия, или необходимая степень заинтересованности, чтобы лично принимать участие в сборе и трансляции информации?
5. Достаточно ли пользователь технически оснащен (имеет ли необходимую технику), чтобы стать вовлеченным в системы умного города?
6. Есть ли необходимость во внедрении информационной технологии сегодня?
7. Какая часть городского населения сможет пользоваться данной технологией сегодня? А завтра?
8. Какую пользу получит город, городское сообщество, городское хозяйство и отдельные жители?
9. Сопоставима ли потенциальная польза с понесенными затратами?
10. Какую часть выделенных ресурсов при необходимости придется потратить на подготовку, обучение и вовлечение пользователей? Кто будет это делать?

Таким образом, решение о цифровизации российских городов, принятое централизованно, может воплощаться в жизнь непосредственно в городах только при нахождении в каждом таком городе ответов, которые удовлетворят все стороны процесса – и заказчиков, и благоприобретателей, и разработчиков. Чтобы города "поумнели", умными должны быть не только ИТ-разработчики, но и муниципалитеты, и население. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Внимательнее на дорогах!

Автоматическая фиксация нарушений ПДД в Вологодской области

Вологодская область – это регион с развитой системой дорожной сети. Если по площади она занимает 26-е место в России, то по общей протяженности автомобильных дорог (более 28 тыс. км.) – 17-е место в стране и 1-е место в Северо-Западном федеральном округе. С целью повышения безопасности на дорогах в Вологодской области с 2014 г. активно развивается система автоматической фиксации нарушений правил дорожного движения

Александр Колычев
Председатель Комитета гражданской защиты и социальной безопасности Вологодской области

Для обеспечения эксплуатации системы автоматической фиксации нарушений ПДД на территории области с 1 января 2014 г. в казенном учреждении Вологодской области "Центр обеспечения региональной безопасности" создано специализированное подразделение. В период с 2014 по 2015 г. в рамках федеральной целевой программы "Повышение безопасности дорожного движения на 2013–2020 гг." Вологодская область получила 22 передвижных комплекса, еще порядка 25 комплексов было получено от УМВД России по Вологодской области, которое эксплуатировало их ранее. К началу 2016 г. система насчитывала 75 комплексов.

Список нарушений расширяется

В 2016 г. в рамках контракта на создание аппаратно-программного комплекса "Безопасный город" на территории пилотных муниципальных образований Вологодской области было дополнительно приобретено 75 комплексов автоматической фиксации нарушений правил дорожного движения, – таким образом, значительно увеличилось их количество. Был расширен перечень фиксируемых в автоматическом режиме нарушений, к привычному превышению скорости добавились такие нарушения, как:

- проезд перекрестка на запрещающий сигнал светофора;
- выезд за стоп-линию;
- выезд на полосу встречного движения;
- движение по полосе для маршрутных транспортных средств;
- нарушения правил остановки и стоянки транспортных средств;
- непредоставление преимущества пешеходу на пешеходном переходе.

Вандалозащитный бокс для размещения передвижного комплекса

Система автоматической фиксации нарушений ПДД на территории Вологодской области насчитывает 170 комплексов, из которых:
- **стационарных – 60;**
- **передвижных – 106;**
- **мобильных – 4.**

Мобильные комплексы используются для фиксации нарушений правил остановки и стоянки транспортных средств

Динамичный контроль

В связи с отсутствием достаточного количества инфраструктуры на дорогах области, а также с целью оперативного влияния на аварийность большой упор был сделан на организацию работы с помощью передвижных комплексов.

Правительством области совместно с Госавтоинспекцией проводится постоянный анализ мест совершения дорожно-транспортных происшествий. Для оперативного влияния на обстановку с аварийностью Правительством Вологодской области совместно с Управлением ГИБДД УМВД России по Вологодской области принято решение о еженедельном изменении адресного плана работы передвижных комплексов, который разрабатывается совместно представителями КУ ВО "Центр обеспечения региональной безопасности" и Госавтоинспекции области.

Для обеспечения безопасности и возможности приблизить места работы комплексов к местам совершения дорожно-транспортных происшествий принято решение при размещении на дорогах использовать комплексы в вандалозащитных боксах. Они не требуют постоянного близкого присутствия оператора с автомобилем, соответственно такие комплексы можно разместить в любом месте на обочине дороги. Чтобы исключить наезды автомобилей, комплексы, как правило, устанавливаются за барьерное ограждение.

Единая система сбора данных

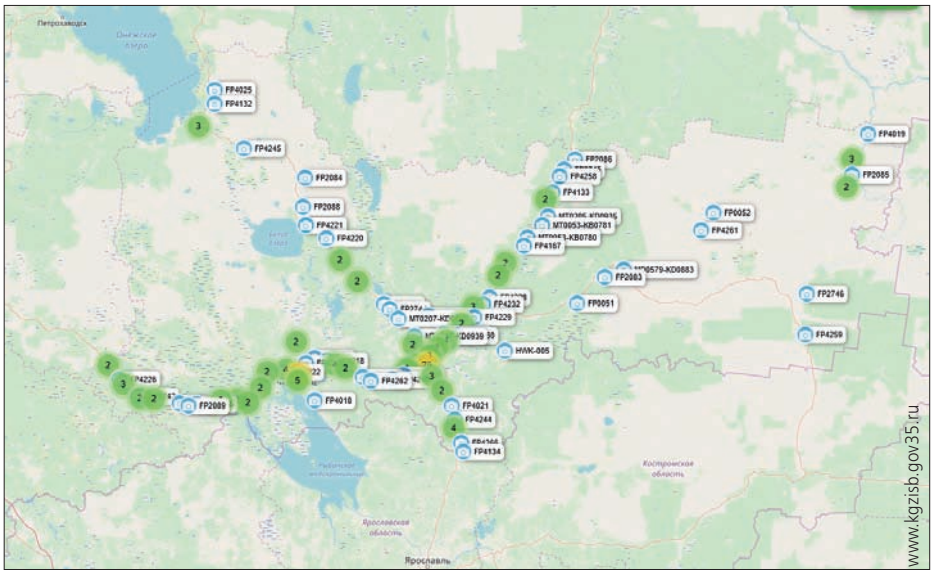
Казенное учреждение Вологодской области "Центр обеспечения региональной безопасности" в повседневной деятельности в режиме реального времени контролирует работу оборудования: ведется учет времени работы комплексов, правильность их настройки, соответствие введенных ограничений действующим схемам организации дорожного движения. Все работающие комплексы отображаются на карте, через которую доступен просмотр всех настроек.

В Вологодской области в 2016 г. была создана система сбора, обработки и хранения информации о зафиксированных нарушениях правил дорожного движения. К ней подключены все эксплуатируемые на территории области комплексы. Загрузка материалов в систему настроена таким образом, что как только комплекс (в том числе и передвижной) фиксирует нарушение, оно сразу же попадает в систему, то есть исключена возможность человеческого вмешательства в процесс загрузки материалов. Сама система также исключает возможность полного удаления данных. Доступ к системе имеют сотрудники КУ ВО "Центр обеспечения региональной безопасности" и ЦАФАП Управления ГИБДД УМВД России по Вологодской области.

За время эксплуатации системы автоматической фиксации нарушений правил дорожного движения (с 2013 по 2019 г.) на автомобильных дорогах, где массово используются комплексы (основные транспортные магистрали Вологодской области), наблюдается снижение всех основных показателей аварийности:
- **количества ДТП – на 30,3%;**
- **количества погибших – на 35,8%;**
- **количества раненых – на 30,1%**

Мониторинг транспорта в реальном времени

Большинство комплексов автоматической фиксации нарушений ПДД, эксплуатируемых на территории Вологодской области, фиксируют не только нарушения, но и весь поток транспортных средств.



Карта установки комплексов фиксации проходящих транспортных средств

В Вологодской области создана система мониторинга передвижения транспортных средств, которая предназначена для фиксации всего проходящего транспорта комплексами, расположенными на дорогах и улицах городов. Эта система формирует единую базу зафиксированных транспортных средств. Доступ к работе с системой в режиме реального времени обеспечен представителям правоохранительных органов. Ежедневно в нее попадает информация о фиксации свыше 800 тыс. транспортных средств.

Серверная группировка системы позволяет хранить данные в системе мониторинга передвижения транспортных средств как минимум один год для работы в оперативном режиме с отображением фотографий транспортных средств, и еще дополнительно два года для работы в ограниченном режиме без фотографий с отображением списков номерных знаков зафиксированных автомобилей, времени и адреса.

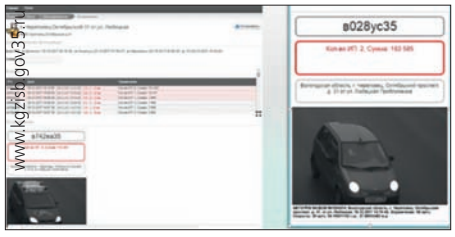
Оператору предоставлена широкая вариативность запросов: можно задавать фильтры по местам фиксации, направлениям движения, временным отрезкам, полностью или частично вводить символы государственных регистрационных знаков и т.д.

Комплексами, фиксирующими номерные знаки транспортных средств, перекрыты основные улицы городов Вологды и Череповца, а также основные трассы, проходящие по Вологодской области. Информация из данной системы активно используется правоохранительными органами для оперативного отслеживания передвижения транспортных средств, выявления находящихся в розыске автомобилей и раскрытия преступлений и правонарушений, совершенных с их применением.

Проверочные рейды на дорогах

Ввиду того что в систему мониторинга попадает информация о передвижении транспортных средств и с передвижных комплексов автоматической фиксации нарушений ПДД, в ней доступны данные о передвижении автомобилей по всем основным транспортным артериям Вологодской области.

Эта система широко используется при проведении совместных рейдов для выявления должников по налогам и штрафам, в которых участвуют сотрудники КУ ВО "Центр обеспечения региональной безопасности", ГИБДД и УФССП. Благодаря загрузке в систему мониторинга базы судебных приставов, содержащей информацию об автомобильных номерах и сумме долга у собственника транспортного средства, сотрудники ГИБДД и УФССП, работая на мероприятии (проводится вблизи установленного стационарного комплекса), оперативно узнают, что в отношении собственника конкретного транспортного средства, которое проезжает через участок, где проводится мероприятие, возбуждено одно или несколько исполнительных производств. Это транспортное средство останавливается, и далее производится проверка его водителя и собственника, сначала по линии Госавтоинспекции, а затем по линии судебных приставов.



Интерфейс работы системы выявления должников в потоке транспортных средств

При таких мероприятиях также используются различные базы Госавтоинспекции:

- транспортные средства, собственники которых не оплатили штрафы за нарушение правил дорожного движения;
- транспортные средства, собственники которых задерживались в состоянии опьянения или лишены прав;
- машины, находящиеся в розыске, и т.д.

Нарушители обнаружены

Данная работа организована с января 2017 г. Всего за период с 2017 по 2019 г. проведено более 200 таких рейдов, в результате которых:

- остановлено 12 230 транспортных средств должников;
- наложено почти 2 тыс. арестов на имущество должников, из которых 1,8 тыс. – на транспортные средства;
- 266 транспортных средств были эвакуированы и помещены на специализированные стоянки.

Сумма арестованного имущества составила почти 500 млн рублей. В местах проведения рейдов должниками погашена задолженность на сумму свыше 16 млн рублей. (наличными и безналичными денежными средствами).

По линии ГИБДД было выявлено более 4 тыс. нарушений правил дорожного движения. Самые распространенные нарушения – неуплата штрафа в установленный законом срок, а также наличие тонировки. Кроме того, во время почти каждого рейда выявляются водители, управляющие транспортным средством будучи лишенными такого права, а также лица, находящиеся за рулем в состоянии опьянения.

Мобильный комплекс фиксации государственных регистрационных знаков транспортных средств

Курс на мобильность

Ввиду того что при проведении рейдов необходимо получать информацию со стационарного комплекса, фиксирующего номерные знаки автомобилей, с целью расширения географии проведения таких мероприятий в 2019 г. был закуплен мобильный комплекс на базе транспортного средства. Он позволяет организовать работу практически в любой точке области. В 2020 г. планируется активизировать данное направление, также в последующие годы запланировано расширение сети комплексов автоматической фиксации нарушений правил дорожного движения по всей Вологодской области. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Иван Тушко
Специалист-эксперт в области обеспечения транспортной безопасности, магистр юриспруденции

Городской наземный электрический транспорт: как обеспечить безопасность

Транспортная безопасность занимает важное место в системе устойчивого функционирования умного города. Она приобретает особую значимость при возникновении потенциальных внутренних и внешних угроз незаконного вмешательства и террористических актов, в частности во время и после их совершения. Данная статья посвящена текущему состоянию обеспечения безопасности и антитеррористической защищенности городского наземного электрического транспорта, выявлению практических проблем в реализации действующего законодательства и анализу достаточности системы принимаемых мер со стороны государства и субъектов транспортной инфраструктуры

Троллейбус типа ЯТБ-1

Наземный электрический транспорт, основными средствами передвижения которого являются трамваи и троллейбусы, – один из главных перевозчиков пассажиров внутри городов. К его основным преимуществам перед транспортом с двигателями внутреннего и внешнего сгорания относятся высокая производительность и экологичность.

Электротранспорт существует уже более века и хорошо зарекомендовал себя благодаря надежности. При этом приоритетом для общества и властей всегда было устойчивое функционирование транспортного комплекса в целях перевозки пассажиров, а вопросы обеспечения безопасности стали приобретать принципиальное и стратегическое значение лишь в последние годы.

Терроризм – угроза № 1

Основную угрозу для транспортной безопасности России представляют террористические акты. Их совершение на общественном транспорте приводит к значительным жертвам среди населения и дестабилизации общественной жизни, а также способствует развитию чувства неуверенности граждан в собственной безопасности, что в конечном счете и является основной целью террористов[1].

Последним и самым ярким примером терроризма в сфере наземного электротранспорта остается теракт, совершенный утром 30 декабря 2013 г. в Волгограде. Целью террористической атаки стал троллейбус № 1233. В момент движения по маршруту № 15А в салоне произошел взрыв мощностью около 4 кг в тротиловом эквиваленте. По данным следствия, взрывное устройство привел в действие террорист-смертник, в результате чего транспортное средство было полностью разрушено.

Последствия теракта 30 декабря 2013 г. в Волгограде

По официальной информации, на месте происшествия погибли 11 человек, при транспортировке в больницы умерли еще 3 человека. 27 пострадавших были госпитализированы, в том числе грудной ребенок. В последующие дни в больнице скончались два человека.

Это в очередной раз доказало, что создание реально действенной системы безопасности на объектах транспорта является приоритетным направлением для всех органов исполнительной власти федерального уровня и административных подразделений на уровне местного самоуправления, а также для самих организаций сферы транспортного обслуживания, независимо от форм организационно-правовой направленности[2].

Произошедшее событие и текущее состояние обеспечения транспортной безопасности на городском наземном электрическом транспорте заставляет обратить внимание на наиболее существенные проблемы, требующие решения со стороны государства и транспортного сообщества.

Отсутствие системности принимаемых мер

Террористические акты, происходящие на транспорте, в значительной степени повышают внимание к отрасли: ускоряется совершенствование нормативной правовой базы, объекты транспорта и транспортных средств оснащаются более современными эффективными инженерно-техническими средствами, разрабатываются новые методы и системы безопасности.

Так, после печальных событий в Волгограде приказом Минтранса России № 7 от 15 января 2014 г. были утверждены правила обеспечения безопасности перевозок пассажиров и грузов автомобильным транспортом и городским наземным электрическим транспортом и перечень мероприятий по соответствующей подготовке работников юридических лиц и индиви-

[1] Шомахов М.К. К вопросу обеспечения безопасности городского общественного транспорта от террористических угроз // Труды Академии управления МВД России. 2014, № 4 (32). С. 125–128.
[2] Амельчаков И.Ф., Тычинин С.В., Карагодин А.В., Москаленко С.А. Актуальные проблемы антитеррористической защищенности объектов транспортной инфраструктуры // Проблемы правоохранительной деятельности. 2017, № 1 (17). С. 6–10.

Троллейбусы Ярославля

дуальных предпринимателей, осуществляющих перевозки.

Кроме того, для обеспечения транспортной безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств городского наземного электрического транспорта раньше применялись требования приказа Минтранса России № 209 от 05 августа 2011 г. Впоследствии они были заменены обновленным обязательным комплексом принимаемых мер, установленных постановлением Правительства РФ № 924 от 14 сентября 2016 г., который состоит из четырех основных этапов:

1. Присвоение категории по транспортной безопасности Федеральным дорожным агентством (Росавтодор).
2. Проведение оценки уязвимости с последующим утверждением в Росавтодоре.
3. Разработка плана обеспечения транспортной безопасности (ПОТБ) с последующим утверждением в Росавтодоре.
4. Реализация ПОТБ, включая оснащение инженерно-техническими средствами.

Вопрос эффективности и целесообразности второго и третьего этапов отдельно рассмотрим ниже. Что же касается системности принимаемых мер, то важно отметить изменения в законодательной сфере, которые привели к бесполезности проведенных мероприятий и потраченных финансовых средств, а также снижению уровня антитеррористической защищенности электротранспорта.

Дело в том, что ранее многими транспортными предприятиями страны были организованы мероприятия по оценке уязвимости, которую проводят специализированные коммерческие организации, и разработке ПОТБ. Такие меры потребовали финансовых затрат, что, в свою очередь, смогло обеспечить для каждого объекта электротранспорта и транспортного средства наличие важных организационных документов, определяющих критические элементы, которые требуют защиты, а также порядки обеспечения данной защиты.

Однако постановлением Правительства РФ № 1697 от 29 декабря 2017 г. троллейбусные и трамвайные парки исключены из перечня объектов транспортной инфраструктуры, на которые распространяются требования законодательства в области обеспечения транспортной безопасности.

Более того, Федеральным законом № 270-ФЗ от 2 августа 2019 г. были внесены изменения в законодательство, в связи с чем оценка уязвимости и разработка ПОТБ для транспортных средств больше не требуется.

Вместе с тем финансовые средства, потраченные субъектами транспортной инфраструктуры (СТИ) за последние годы на исполнение обязательных требований, действие которых было отменено, возврату не подлежат, а наличие системного и комплексного подхода к обеспечению транспортной безопасности электротранспорта вызывает сомнение.

Низкая эффективность оценки уязвимости и разработки ПОТБ

Как сказано выше, оценка уязвимости и разработка ПОТБ – два важнейших этапа системы мер по транспортной безопасности, определенных государством.

Согласно национальному стандарту ГОСТ Р 57119–2016, оценка уязвимости состоит из четырех этапов.

Для чего необходим такой документ СТИ, который занимается перевозками? Прежде всего для того, чтобы обученные и аттестованные специалисты сторонней организации смогли объективно провести анализ обеспечения безопасности и выявить участки, требующие принятия соответствующих мер. Далее на основании результатов оценки уязвимости должен быть разработан следующий, пожалуй, самый фундаментальный документ – план обеспечения транспортной безопасности (ПОТБ), где будут содержаться порядки, инструкции и прочие документы, на основании которых предприятие станет осуществлять защиту[3].

Однако на практике большинство мер, рекомендованных специализированными организациями при проведении оценки уязвимости, не реализуются, так как не имеют правовой обязательной основы их выполнения.

Разрабатываемые же в настоящее время ПОТБ, по сути, являются для СТИ не руководством к проведению комплекса обоснованных мероприятий по транспортной безопасности на долгосрочный период, а отчетом перед компетентным органом о выполнении конкретной нормы законодательства.

При этом, аналогично ГОСТ Р 57119–2016, для ПОТБ отсутствует подобная научно-практическая методика, которая определяла бы цели, задачи и этапы проведения разработки данного документа.

Таким образом, вопрос об эффективности проведения оценки уязвимости и разработки ПОТБ является крайне актуальным.

В силу фактического износа многих транспортных средств для продления полезного срока использования трамвая или троллейбуса они нередко подвергаются ремонту, в результате чего изменяются технические и технологические свойства, что впоследствии не фиксируется в технических паспортах. Например, в транспортном средстве может

Этапы проведения оценки уязвимости

[3] *Тушко И.С. Оценка уязвимости транспорта. Эффективность и методы улучшения // Безопасность и охрана труда на железнодорожном транспорте. 2019, № 6. С. 62–67.*

Совмещенный трамвайно-троллейбусный парк в Санкт-Петербурге

изменяться количество сидячих мест, однако соответствующая информация заводу-изготовителю не отправляется. Это порождает определенные коллизии и противоречия при подготовке организационных документов по транспортной безопасности, в том числе оценке уязвимости.

Установление границ зоны транспортной безопасности и КПП

В настоящее время границы и конфигурация зоны транспортной безопасности для объекта электротранспорта и транспортного средства определяются специализированными организациями в процессе оценки уязвимости и устанавливаются СТИ на основании этих рекомендаций. Однако на государственном уровне отсутствует научно-практическая программа или методика, в соответствии с которыми было бы возможно провести обоснование установления данных границ и мест размещения КПП.

При проведении оценки уязвимости объектов электротранспорта и транспортных средств Санкт-Петербурга и Самары автором статьи применялась "Методика расчета границ зоны транспортной безопасности и критических элементов с учетом ущерба возможных последствий от совершения АНВ", разработанная на основе обобщения многолетних работ по оценке уязвимости, а также исследований других ведущих научно-исследовательских учреждений.

Данная разработка позволила применить научно-практическое обоснование при определении границ зоны транспортной безопасности и расчете возможного ущерба от АНВ. Она показала высокую эффективность на практике и позволила исключить субъективность экспертного мнения.

Отсутствие защищенности трамвайных и троллейбусных парков и транспортных средств

Как уже отмечалось, ранее был проведен комплекс мероприятий в области обеспечения антитеррористической защищенности трамвайных и троллейбусных парков, который, несмотря на потраченное время и деньги, оказался невостребованным. Сегодня разработка и принятие мер по транспортной безопасности данных объектов лежат на плечах транспортных предприятий и отсутствуют в поле ведения контрольно-надзорной деятельности.

Многими работниками СТИ остро ощущается недостаточность научно-практических подходов, методик, моделей для анализа защищенности своего предприятия и применения научно обоснованных решений в осуществлении мер для обеспечения антитеррористической защищенности.

Правоприменители обращают внимание на тот факт, что в действующем законодательстве, регулирующем вопросы обеспечения транспортной безопасности, отсутствовала и до сих пор отсутствует дефиниция государственной политики транспортной безопасности, не конкретизированы цели и меры, направленные на ее обеспечение[4].

В результате отсутствие нормативно-правового регулирования и контрольно-надзорной деятельности в части обеспечения транспортной безопасности троллейбусных парков и трамвайных депо не позволяет СТИ обеспечить должный уровень их антитеррористической защищенности.

Невостребованной оказалась и реализованная система мер по обеспечению антитеррористической защищенности трамваев и троллейбусов в связи с изменениями законодательства (Федеральный закон № 270-ФЗ от 2 августа 2019 г.). Оценка уязвимости и разработка ПОТБ для транспортных средств ушли в прошлое, а новые меры по их защите будут содержаться в новом организационном документе – паспорте обеспечения транспортной безопасности транспортного средства.

Стоит отметить, что типовые формы указанных паспортов будут установлены Правительством Российской Федерации, но пока данного нормативного правового акта еще не существует. Иными словами, лишь после издания постановления Правительства РФ об утверждении типовых форм данных паспортов можно будет говорить о каких-либо новых мероприятиях по транспортной безопасности в отношении транспортных средств[5].

Трамваи Москвы

[4] Тимченко А.В. Институционализация государственной политики обеспечения транспортной безопасности как форма интеграции системы государственной политики // Политическая наука. 2017. Спецвыпуск. С. 124–136.

[5] Тушко И.С. Изменения законодательства по обеспечению транспортной безопасности // Безопасность и охрана труда на железнодорожном транспорте. 2019, № 5. С. 65–67.

Троллейбусы Хабаровска

Таким образом, в отношении как троллейбусных парков и трамвайных депо, так и самих транспортных средств отсутствует нормативно-правовое регулирование мер, которые позволили бы СТИ обеспечить их защиту в должной степени. Достаточность проводимых мероприятий будет самостоятельно определяться и оцениваться каждым СТИ и может быть выявлена лишь при попытках совершения или совершении АНВ, в том числе террористических актов.

Здесь же стоит упомянуть о недостаточном уровне законодательной базы в области определения совместного порядка действий работников СТИ и правоохранительных органов при возникновении и ликвидации чрезвычайных происшествий, включающих в себя совершенные преступления террористического характера.

Аттестация сил обеспечения транспортной безопасности

Вопросу профессиональной квалификации лиц, выполняющих работы по обеспечению транспортной безопасности, в последнее время уделяется все большее внимание. И это объяснимо в силу необходимости совершенствования или получения новой компетенции для профессиональной деятельности по исполнению требований законодательства в сфере транспортной безопасности, в том числе антитеррористической защищенности.

Но несмотря на то, что данная деятельность активно развивается по всем видам транспорта уже более трех лет (начиная с 2016 г.), в ее реализации достаточно много моментов, требующих внимания и доработки со стороны соответствующих органов.

Перечни вопросов, используемых органами аттестации и аттестующими организациями для проверки соответствия знаний, умений и навыков аттестуемых лиц, определяются компетентными органами применительно к объектам транспортной инфраструктуры и транспортным средствам по видам транспорта. При этом перечни вопросов разработаны без учета специфики и особенностей функционирования транспортного комплекса по видам транспорта. Лица, назначенные ответственными за обеспечение транспортной безопасности в транспортном средстве (водители), также обязаны пройти указанную подготовку (обучение) и аттестацию.

В настоящее время низкий уровень подготовки водителей, по мнению субъектов автомобильного и электротранспорта, связан с избыточными требованиями, предъявляемыми законодательством. Фактически аттестуемые по транспортной безопасности водители должны обладать знаниями и умениями не только в области обеспечения транспортной безопасности на транспортном средстве, но и в сфере антитеррористической защищенности объектов транспортной инфраструктуры всего автомобильного транспорта и дорожного хозяйства.

Требует отдельного внимания вопрос гармонизации законодательства в сфере аттестации сил обеспечения транспортной безопасности и трудового законодательства.

Исходя из анализа выявленных проблем и практики обеспечения антитеррористической защищенности городского наземного электрического транспорта, можно сделать вывод о том, что, несмотря на значительный объем проведенных мероприятий по транспортной безопасности, сформирована лишь частичная защита объектов и транспортных средств. Постоянное развитие технологий в области транспорта и информации приводит к необходимости уделять больше внимания существующим в данной отрасли проблемам.

На пути к решению проблем

События, произошедшие в Волгограде в 2013 г., наглядно показали, что потенциальные угрозы совершения актов незаконного вмешательства, в том числе террористических, в деятельность транспортного комплекса могут стать непосредственными и прямыми угрозами для жизни и здоровья пассажиров и нанесения материального ущерба транспортным организациям.

Основные усилия по обеспечению внутригородской транспортной безопасности должны быть нацелены на правовое воспитание населения, разрешение кризисных и конфликтных ситуаций политическими методами, без силового воздействия, на подрыв основ терроризма путем пресечения попыток создания экстремистских организаций радикального толка. Требуется и более детальная проработка в законе конкретных антитеррористических мероприятий, проводимых на городском общественном транспорте.

На основании анализа текущего состояния обеспечения транспортной безопасности и антитеррористической защищенности электротранспорта, а также проблемных аспектов, выявленных в данном исследовании, можно говорить о наличии острой потребности в поиске путей решения существующих проблем.

1. Крайне важно обратить внимание на отсутствие нормативно-правового регулирования в части обеспечения транспортной безопасности троллейбусных и трамвайных парков, транспортных средств электротранспорта. Необходима разработка новых правовых актов, регламентирующих систему мер по антитеррористической защищенности данных уязвимых мест транспортного комплекса.

2. Необходимо направить силы на решение вопроса недостаточности научно-практических подходов, моделей и стратегий для анализа защищенности транспортных предприятий. Требуется разработка методик подготовки плана обеспечения транспортной безопасности объекта транспортной инфраструктуры и паспорта обеспечения транспортной безопасности транспортного средства. Для определения границ и конфигураций зоны транспортной безопасности и критических элементов необходимо наличие утвержденной на государственном уровне соответствующей методики с учетом ущерба возможных последствий от совершения АНВ.

3. Требуется гармонизация законодательства в сфере аттестации сил обеспечения транспортной безопасности с трудовым законодательством. В свою очередь, в области обеспечения аттестации важен комплексный подход к изучению проблемных практических вопросов реализации с пересмотром состава действующих категорий и типовых дополнительных профессиональных программ обучения.

4. Стоит укрепить нормативную базу в области проведения совместных мероприятий СТИ и правоохранительных органов при профилактике правонарушений, возникновении и ликвидации чрезвычайных происшествий, в том числе преступлений террористического характера.

Городской наземный электрический транспорт занимает важное место в транспортной системе любого крупного города России. Именно поэтому необходимо признать значительную роль обеспечения антитеррористической защищенности в перевозке пассажиров, для которых важна не только надежность поездки, но и ее безопасность. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

ЦУР – единая платформа управления Подмосковьем в режиме 24/7

Московская область в числе первых взяла на вооружение самые современные разработки в сфере цифровых технологий и управленческого учета и в рамках реализации национального проекта "Цифровая экономика" создала платформу для управления регионом – Центр управления регионом (ЦУР). Этот инструмент позволяет оперативно реагировать на все проблемы, возникающие в области, получать и обрабатывать максимально подробную информацию от жителей региона. И все это в режиме 24/7

Александр Краснов
Заместитель директора
ГКУ МО "МОЦ ИКТ",
советник министра государственного управления, информационных технологий и связи Московской области

Московская область в числе первых взяла на вооружение самые современные разработки в сфере цифровых технологий и управленческого учета и в рамках реализации национального проекта "Цифровая экономика" создала платформу для управления регионом – Центр управления регионом (ЦУР)

Главные цели создания Центра управления регионом – отслеживание, контроль, анализ проблемных областей Московского региона. Сроки обработки обращений и сообщений сокращены, обеспечен контроль решений проблем, жители получают качественные и полноценные ответы на свои обращения, а для Правительства Московской области формируются сводные аналитические данные по проблемам и запросам населения Московской области.

Структура ЦУР

ЦУР представляет собой межведомственную рабочую группу, в которой работают действующие сотрудники из ведомств Правительства Московской области. На сегодняшний день это 122 сотрудника из 30 ведомств и 11 отраслевых боксов: медицина, образование, ЖКХ, социальная защита, транспорт, экология, строительство, госуслуги, СМИ, безопасность, национальные проекты.

Для каждого ведомства определен топ проблем, которые им предстоит решать. По сути, сотрудники ЦУР – это контролеры качества работы своих ведомств. Они подсказывают решения, которые позволяют не допускать появление новых проблем.

Функционально Единый центр управления регионом (ЦУР) состоит из следующих подсистем:

- классификации и маршрутизации входящих обращений и сообщений;
- подготовки ответов;
- обратной связи и контроля удовлетворенности;
- контроля исполнения задач;
- мониторинга и аналитики;
- формирования предложений для дополнительного финансирования, позволяющая на основе поступивших обращений и сообщений формировать перечни задач, требующих ремонта, строительства, благоустройства;
- деперсонализации (обезличивания) сообщений;
- интеллектуальной обработки и машинного обучения;
- интеграции;
- администрирования;
- хранения данных;
- мониторинга доступности ЦУР;
- информационной безопасности.

Приоритетные задачи

Достижение главной цели ЦУР происходит через решение следующих основных задач:

- обеспечение приема обращений и сообщений граждан, поступающих в центральные исполнительные органы государственной власти (ЦИОГВ), государственные органы и органы местного самоуправления (ОМСУ) по любым доступным каналам обращений, а также публикуемых в социальных сетях;
- автоматическая рубрикация обращений и сообщений граждан;
- предварительный анализ поступающих обращений и сообщений граждан, автоматическое формирование задач для ЦИОГВ, ГО, ОМСУ, подведомственных организаций, выявление аналогичных обращений и сообщений граждан и подбор на их основе типовых проектов ответов, используемых для решения аналогичных проблем;
- автоматизация процедуры подготовки ответов за счет использования типизированных шаблонов ответов;
- контроль сроков и качества обработки обращений и сообщений граждан, в том числе контроль соблюдения сроков первичного рассмотрения задач, отложенных сроков и сроков окончательного решения вопроса;
- обеспечение информирования граждан о ходе обработки их обращений и сообщений через систему приема сообщений, региональный портал государственных услуг посредством автоинформирования по электронной почте и по телефону, а также посредством отправки личного сообщения пользователю социальной сети в сроки, определяемые Регламентом информационного взаимодействия участников государственной информационной системы Московской области "Единый центр управления регионом" (далее – Регламент информационного взаимодействия участников ЦУР);
- сбор информации об удовлетворенности граждан по результатам обработки их обращений и сообщений;
- сводный анализ результатов обработки обращений и сообщений граждан;
- формирование комплексной картины всех проблем, волнующих граждан, выявление наиболее проблемных объектов, требующих ремонта, благоустройства, строительства;
- отправка ответов на сообщения граждан, выгрузка ответов на обращения граждан в межведомственную систему электронного оборота для дальнейшей отправки в соответствии с законодательством об обращениях граждан и в установленные сроки.

Концепция работы

ЦУР – это принципиально новый подход к управлению и выстраиванию контроля за процессами. Концепцию его работы можно выразить так: "Все знаем – быстро решаем – не допускаем".

Концепция ЦУР

Проблему бессмысленно гонять по всем бюрократическим инстанциям. Она должна сразу поступать к тому сотруднику, который может ее решить. Например, порядка 40% всех жалоб, которые были получены на портале "Добродел", относились к деятельности управляющих компаний. В итоге все УК были зарегистрированы в единой системе. Теперь все жалобы по этой тематике сразу направляются в УК, минуя бюрократические издержки, и через 24 часа можно смотреть на изменение ситуации, о которой рассказал заявитель. Раньше подобная жалоба могла несколько дней "гулять" по ведомствам

1. Принцип "Знаем" подразумевает сбор, обработку и анализ информации. Она отображается на "тепловой карте" региона, где соответствующий цвет характеризует статус той или иной проблемы в конкретном муниципальном образовании. Так выявляются точки напряжения в регионе для понимания, где необходимо применить оперативное вмешательство для решения проблемы. Аналитический центр позволяет отслеживать динамику показателей в разрезе территорий в режиме онлайн. Однако недостаточно видеть красные лампочки на карте, необходимо быстро решать проблемы.

2. Принцип "Быстро решаем" означает быструю доставку жалоб от жителей региона, контроль исполнения и определение реальных сроков решения проблем. Поэтапный механизм решения вопроса в виде блок-схемы позволил увидеть узкие места и оптимизировать сроки без дополнительных финансовых затрат. При обработке жалоб каждой категории проблем присваивается свой срок решения, а сотрудники центра осуществляют непрерывный контроль качества решения проблем.

3. Принцип "Не допускаем" подразумевает недопущение повторения проблемы, работу над устранением ее причин. Это самая интеллектуальная часть задачи. Благодаря анализу информации выявляются истинные причины проблем, что позволяет сократить срок их решения и искоренить причину для предотвращения их возникновения в будущем. Трансформация процессов обработки жалоб позволила исключить лишних участников и сократить срок доставки жалобы до исполнителя. В настоящее время многие вопросы решаются за два дня, а в некоторых случаях – до 24 часов.

Типы данных

В ЦУР включаются следующие сведения:

- классификаторы тематик обращений и сообщений граждан, общероссийский классификатор обращений граждан и организаций, утвержденный решением рабочей группы при Администрации Президента Российской Федерации по координации и оценке работы с обращениями граждан для поступающих в ЦУР обращений граждан;
- обращения и сообщения граждан;
- задачи для ЦИОГВ, ГО, ОМСУ, подведомственных организаций, созданные на основе обращений и сообщений граждан;
- сроки решения задач по обращениям и сообщениям граждан;
- варианты решений проблем, о которых сообщают граждане;
- шаблоны типовых проектов ответов на обращения и сообщения граждан;
- готовые ответы на обращения и сообщения граждан;
- запросы уточняющих сведений у авторов обращений и сообщений, ответы на них и комментарии;
- статусы решения задач по обращениям и сообщениям граждан.

Категории жалоб

С помощью уникальных информационных систем в круглосуточном режиме производятся сбор и анализ данных во всех сферах жизнедеятельности Подмосковья. За 2019 г. получено и обработано 1,5 млн заявок.

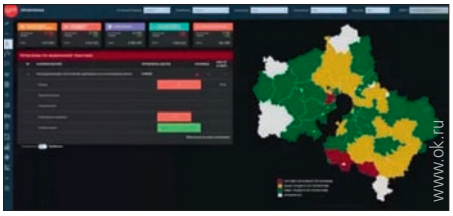
Анализ показывает, что:

- 70% заявок приходятся на операционные проблемы (то, что можно быстро решить и для этого не потребуется серьезных финансовых вложений – заделать, почистить, лампочку вкрутить);
- 30% – на ресурсоемкие жалобы (где нужны дополнительные ресурсы и финансы – что-то построить, модернизировать).

"Тепловая карта" проблем

Все проблемы, поступающие от жителей региона, автоматически собираются на "тепловой карте" без участия человеческого фактора. В ней указаны:

- направления, по которым поступили жалобы (по ним рейтинг формируется автоматически);
- тренды по новым, отложенным, просроченным и повторным жалобам (после запуска ЦУРа по ним наблюдается снижение);
- территории с наибольшим количеством проблем;
- блоки, в которых все муниципалитеты разделены по численности населения на три группы (крупные, средние и небольшие);
- зона ответственности исполнителей, у которых больше всего проблем (определяется системой).



"Тепловая карта" муниципальных центров

Объединение усилий

Когда были проанализированы 3,5 млн обращений граждан в 2018 г., стало понятно, что 70% проблем относится к полномочиям муниципальных образований.

Чтобы научить исполнителей на местах грамотной работе с сообщениями жителей, было принято решение о создании муниципальных ЦУРов. На данный момент открыты и активно работают 64 муниципальных филиала. Для выстраивания этой деятельности городским округам предоставляются методология, программные комплексы и другие инструменты работы с жалобами жителей.

Таким образом, ЦУР и муниципальные филиалы совместно в круглосуточном режиме выполняют функции стратегического, текущего и оперативного планирования, мониторинга и контроля исполнения управленческих решений, помогают значительно сократить время решения проблем граждан и отслеживают общую социально-экономическую ситуацию в Подмосковье. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Унификация IP-коммуникаций для города

В последние годы наблюдается тенденция унификации коммуникаций для города. Какие качественные изменения произошли в этом направлении и что нас ждет в будущем для обеспечения безопасности мегаполисов?

Ярослав Кузьмицкий
Директор по развитию бизнеса компании InPrice Distribution

Идеологическая готовность окружающего нас мира стать тотально цифровым оценивается в 80%. В Китае уже сегодня цифровые технологии позволяют жителям оплачивать покупки "лицом" и через мессенджеры, проходить в метро по биометрической верификации. Почему мы говорим о Китае? В первую очередь потому, что нигде в мире нет такого массового испытательного полигона, как в Китае. Поэтому если что-то работает там, то, вероятно, может быть применимо почти везде.

Биометрия, Интернет вещей, унифицированные коммуникации, мобильная парадигма и другие технологии в ближайшее время позволят реализовать аналогичные решения в нашей стране.

Точки роста и трансформации технологий

В последние 15–20 лет произошел бурный рост IP-технологий. Ярчайшим примером уже случившегося перерождения является видеонаблюдение, которое за это время из аналогового полностью трансформировалось в цифровое (включая чистое IP-видео и гибридные системы типа AHD с конечным хранением в цифре, с доступом к архиву по IP). Схожие процессы затронули телефонию, телевидение и радио. При этом телефония, телевидение и радио стали частью Интернета. Любопытным и знаковым фактом является открытие сервиса IP-телефонии (VoIP) Яндексом. Итак, Яндекс, который для многих в России тождественен понятию "Интернет", теперь и голосовой телеком-оператор. Он имеет номерные емкости, подключает офисы и частников и делает многое что еще, смыкая это со своими платежными и мобильными сервисами.

Значительные изменения технологического плана произошли и в области городского жилищно-коммунального хозяйства (ЖКХ). Множество приборов учета энергоресурсов стали умными и способными автоматически передавать показания. Переходит в область IP-вещания (и частично беспроводной передачи данных внутри сетей оповещения) и такой важный для города сегмент, как публичное оповещение о событиях гражданской обороны и пожарной безопасности. Становится частью городской среды IP-домофония, которая наконец перешла на протокол SIP, практически стала частью IP-телефонии и продолжает активно трансформироваться. Более того, при правильной административной постановке вопроса она окажется и легко интегрируемой, ввиду своей IP-/SIP-природы, в общегородскую IP-систему ГО и ЧС. В такой системе каждый IP-домофон может работать как точка публичного голосового оповещения.

Параллельно с технологическими процессами идет цифровизация банковских услуг и их трансформация в мобильный сервис. Все эти тренды можно назвать "лепестками одного цветка". Следующая очередь преобразования ждет оперативную групповую радиосвязь. Уже появились рации, работающие через LTE и Wi-Fi. Все это – составные части интегрированной унифицированной инфраструктуры IP-коммуникаций и идеологии цифрового города, приобретающего все большее значение в нашей жизни.

Биометрия, Интернет вещей, унифицированные коммуникации, мобильная парадигма – эти тренды объединяются друг с другом и на их основе появляются новые возможности и сервисы для преобразования окружающей нас действительности в полноценный цифровой мир. К ключевым уровням унификации можно отнести:

1. Инфраструктурный (транспортный) уровень – TCP-/IP-сети и Интернет (Ethernet, Wi-Fi, 5G/LTE/3G).
2. Протокольный уровень – SIP, HTTP (S), ONVIF/RTSP/RTMP и пр. Он используется для видеонаблюдения, домофонии, телефонии.

Для того чтобы полноценно заработал третий уровень – Интернет вещей, не хватает полной стандартизации конечных устройств, которые должны взаимодействовать между собой. Существующие стандарты (Bluetooth, LoRA, Z–Wave, ZigBee, RF433) пока ортогональны, но ожидается, что через некоторое время на этом уровне тоже будет четкая иерархия.

Распознавание по лицу – главный тренд

Распознавание по лицу – ключевая технология, которая будет в дальнейшем применяться на каждом шагу. Почему именно она?

Казалось бы, общеизвестное сканирование отпечатков пальцев дает достаточно точные результаты, однако на многих терминалах считывание происходит не моментально, а отказ в доступе может зависеть даже от аккуратности позиционирования пальца. К тому же руки могут быть грязными, слишком сухими или мокрыми, что препятствует однозначной дактилоскопической идентификации с первой попытки. Описанные факторы могут привести к формированию на проходных очередей. При этом дактилоскопическая идентификация имеет, безусловно, ценность для компании: она получает базу отпечатков сотрудников для разбора инцидентов. Лицо или радужку глаза злоумышленник или разгильдяй вряд ли оставит на месте происшествия, а вот отпечатки наверняка.

Сканирование радужки глаза – более дорогая, сложная и ресурсозатратная технология. Кто сталкивался с нею, отметит, что сканирование требует аккуратности и иногда процедуру приходится повторять. Точность идентификации очень высокая, но опять же нужно выдерживать дистанцию, точно смотреть в прибор. В общем, это решение отлично для высокоответственных учреждений, но явно НЕ массовое.

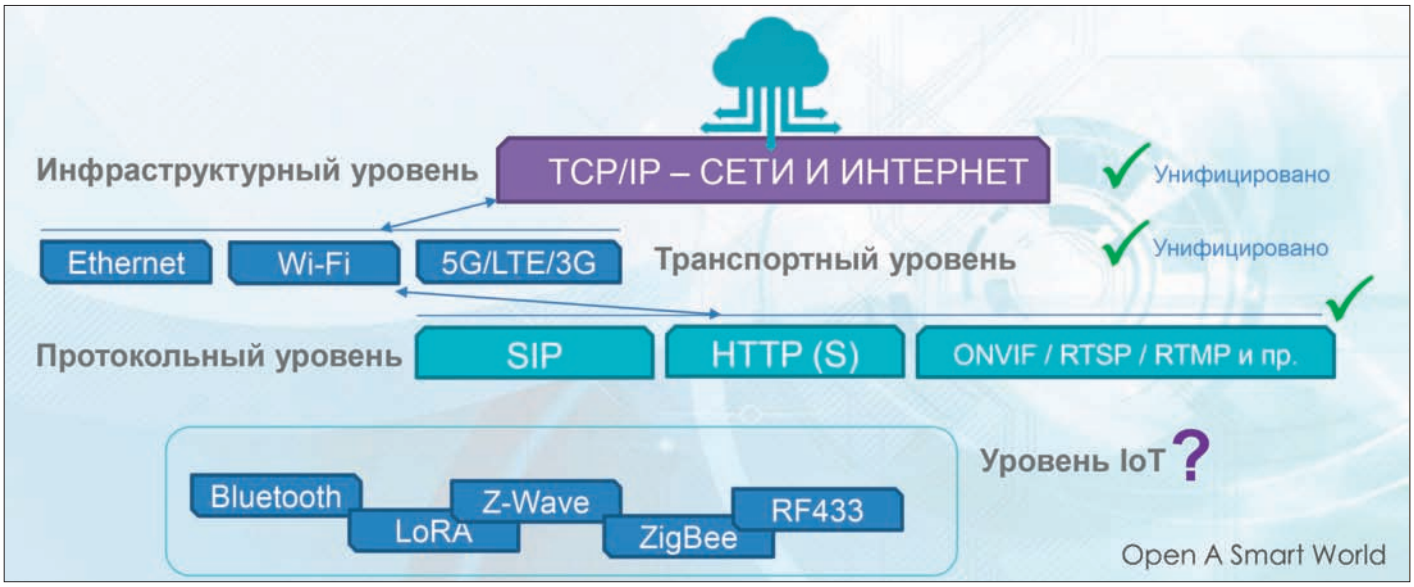
В то же время мы видим, что именно распознавание лиц уже начало применяться в Китае в массовом порядке при пропуске пассажиров в метро и поиске криминальных элементов. Аналогичный опыт есть и в Москве. Технология "дозрела" и стала доступнее. Конечно, коронавирус и маски сбили безапелляционный энтузиазм вокруг Face ID, но до этого распознание по лицу показало все свои преимущества, и это произошло именно благодаря применимости к массовым идентификациям. Верификация по лицу станет трендом, задающим для городского хозяйства важнейшую цифровую составляющую для осуществления платежей, для взаимодействия с государственными и частными сервисами. Даже производственные предприятия могут использовать эту технологию, например, для доступа работников к закрытым зонам.

Огромным, естественным и чуть ли не решающим плюсом лицевой биометрии является простота ее применения для потребителя. Лицо, в отличие от карты, нельзя "потерять", вам, собственно, ничего не нужно делать для прохода в дом и на работу, даже снимать перчатки. И потом, приятно, когда тебя узнают даже двери!

Интерком-системы – часть новой унифицированной цифровой среды города

Интеркомом на профессиональном языке называются специализированные переговорные устройства. Эти устройства при массовом применении в городском хозяйстве позволят осуществлять переговоры граждан с полицией, службами информации и эксплуатации объектов в режиме оперативной связи. Наиболее знакомыми нам интерком-системами, наверное, являются столбы SOS/INFO на станциях метро в Москве и Санкт-Петербурге, а также небольшие оранжевые киоски "гражданин – полиция". Если говорить о красно-синих стойках в метро, то это как раз пример реально работающей и эффективной IP-интерком-системы.

Как и все подобные устройства, стойки подключаются к сети через Ethernet и могут работать с городской системой оперативной связи и через облачные инфраструктуры федераль-



Платформы и ключевые уровни унификации

ных операторов типа "Ростелекома", и через локальные коммутационные узлы (IP-АТС) территориальных объектов, где они установлены. То есть они изначально предназначены быть частью унифицированных коммуникаций города.

Современная переговорная IP-система состоит из SIP-интеркома (по сути, IP-телефона в специальном антивандальном корпусе), IP-камеры, опционально элемента био-СКУД и обеспечивает:

- голосовые коммуникации – переговоры с собеседником, который может находиться на расстоянии тысяч километров;
- видеонаблюдение, так как каждое устройство IP-домофонии/интеркома оборудовано IP-камерой и является точкой видеофиксации;
- удаленное управление и реагирование на события;
- контроль доступа и оповещение населения.

Интерком и биометрия

Ранее мы говорили о биометрической идентификации по лицу и том, что она займет важную роль в нашей жизни. Но как это относится к так подробно описываемым интеркомам? Очень просто! С момента, когда гражданин получит цифровой профиль, включающий в себя голос, отпечатки и математическую модель лица, любое его обращение через городской интерком в службы оперативного реагирования или информирования будет автоматически идентифицироваться и журналироваться. При звонке по видеоинтеркому оператор службы информации или офицер полиции сразу обратится к вам по имени-отчеству и, естественно, будет заранее знать, где вы находитесь и куда присылать помощь.

Конечно, это только один пример из десятков возможных вариантов конвергенции лицевой биометрии и интерком-систем.

Смарт-интерком для жилых комплексов

Несмотря на очевидность необходимости перехода на полноценные IP-системы домофонии и смарт-интеркомов ввиду множества факторов-драйверов, таких как легкость массового удаленного обслуживания, высокое качество видео и аудио, возможность использования единой кабельной инфраструктуры для многих целей ЖК и др., даже новые ЖК зачастую запускаются на базе аналоговых систем по "программе-минимум". Положено запирающее устройство – получите. Нужно ли такое городу на перспективу? Скорее, нет. Хотят ли жильцы внедрить IP-домофонию? Скорее всего, тоже пока нет, так как опыта общения (особенно положительного) у них с ней не было. Кроме того, многие операторы делают очень неоднозначную и даже вредную вещь: они устанавливают IP-вызывную панель, раздают доступ к мобильным приложениям, ключ – и все. В квартире абонентского устройства нет, как его установить и какое именно – никто не знает, и в результате, забыв через полгода пароль/логин от приложения или сменив телефон, все ходят встречать гостей вниз. Прогресс?! Поэтому на ровном месте рождается отторжение этой "умной домофонии". "Раньше у бабушки хоть трубка была, – говорят люди, – а сейчас звонок должен приходить на приложение, а у нашей мамы кнопочный телефон и менять она его не хочет". Система приземления звонков на городской или мобильный номер (а это возможно) не продумана в ЖК и у оператора даже за дополнительную плату. В результате получается решенная наполовину ситуация. Домофон есть, он умный, а ввиду небрежного и некомплексного подхода установщиков пользуются его преимуществами только единицы.

Это комплексная проблема, и решать ее надо на уровне подхода. Бесполезно включать в проект реновации квартала только обновление вызывных панелей. Сразу возникнет и вопрос стационарных абонентских IP-устройств. По минимуму это должны быть переговорные устройства IP-аудио в каждой квартире, а оптимально – IP-мониторы. Иначе мы получим вышеописанную ситуацию.

Закладывать старые системы домофонии в новые ЖК – крайне вредная практика, которая будет напрямую тормозить общегородской переход к единому адресуемому пространству связи, контролируемому из ситуационных центров. При сегодняшних ценах на IP-домофоны и IP-мониторы в смете на постройку здания это малая капля, а вот отсутствие заложенной IP-инфраструктуры в дальнейшем все равно заставит эксплуатирующую организацию вернуться к решению этого вопроса. Только это будет сложнее и дороже, чем на момент формирования объекта.

IP-домофония может дать жителям ЖК реально новый уровень комфорта и сервиса, связать дом с городскими службами (вызов врача, такси, полиции и пожарных, получение/оплата счетов и пр.), однако инфраструктура должна тщательно продумываться и строиться с учетом долговременного запаса актуальности в процессе эксплуатации.

А что в старом фонде?

В современном ЖКХ на фоне повальной инсталляции координатно-матричных аналоговых устройств для домофонии существуют следующие проблемы и вызовы:

- неконтролируемый и нежурналируемый проход "непонятных" субъектов;
- "резиновые" квартиры и невозможность отслеживания жителей в них;
- использование подъездов для закладки наркотических веществ;
- насилие и криминал в подъездах;
- безнаказанный вандализм.

IP-домофон потенциально сможет помочь решить эти проблемы, а аналоговый – нет!

Понятно, что сам по себе IP-домофон этого сделать не сможет, но он может быть эффективным инструментом в руках компетентных органов и городских властей.

Есть ли перспективы у гибридных решений?

Попытки использовать старую, как правило существенно изношенную координатно-матричную инфраструктуру подъездов совместно с новыми IP-вызывными панелями (и наоборот) стратегически ни к чему хорошему не приведут. Технически это возможно. На рынке появилось некоторое количество образцов таких конвертеров, но надо понимать, что это малотиражные поделки и их стабильность неясна. Исключением являются некоторые вызывные панели со встроенными дублирующими выходами координатно-матрич-

ной домофонии. Однако в обоих случаях можно говорить только о неком временном "костыле", когда переход на полноценную IP-инфраструктуру экономически совершенно невозможен или стоит задача продекларировать факт установки IP-вызывных панелей в городе N. Задача вернется, и уже, скорее всего, с негативом хлебнувших "умной домофонии" потребителей.

Аналоговая домофония не отвечает задачам города XXI века. Ее недостаток – самозамкнутость и тупиковость:

- узкая специализация – это только переговорное устройство (домофон);
- сложность интеграции во внешнюю инфраструктуру;
- плохое качество связи даже внутри объектов;
- затруднения при адресации объекта извне (для ГО и ЧС);
- невозможность удаленной диагностики системы и сложность внедрения на ее основе новых сервисов.
- изношенность базовой кабельной инфраструктуры и потенциальная нестабильность.

IP-домофонизация, в свою очередь, имеет несомненные преимущества: она может стать частью городского видеонаблюдения и системы унифицированных коммуникаций.

На самом деле, любая вызывная IP-панель в подъезде является точкой переговоров как с жильцами, так и со службами оперативного реагирования, а также и частью системы оповещения. Большинство современных IP-вызывных панелей имеют ряд резервных кнопок прямо на клавиатуре, например "консьерж" или "оператор", и служебных, типа # и *, – эти кнопки могут программироваться на любой требуемый алгоритм вызова вплоть до передачи вызова по инстанции "вверх" в случае отсутствия ответа первого уровня и т.д. Кроме того, всегда возможно скоммутировать внешнюю кнопку паники, назначив ей нужный маршрут звонка. Таким образом, каждый подъезд мы можем превратить в точку оперативной связи с городскими службами экстренного реагирования. А встроенная IP-камера вызывной панели позволит принять вызов с видео и потом разобраться с обстоятельствами происходившего, изучив архив.

При выводе таких вызывных панелей на сервисы оператора можно достичь применения их в самых широких целях.

Есть еще одна неожиданная проблема в ЖКХ. Она связана с демонтированием радиоточек в квартирах в постсоветский период. С одной стороны, они, безусловно, себя изжили, но надо понимать, что их устранение разрушило систему оповещения населения.

К счастью, IP-домофония может выполнять функции оповещения при чрезвычайных ситуациях. В качестве точек оповещения могут выступать как вызывные подъездные или этажные панели, так и внутриквартирный монитор или переговорное устройство IP-аудио типа C312. Причем оповещение может быть как массовым синхронным, так и адресным – например, предписать эвакуацию только одного подъезда или этажа.

Варианты использования IP-коммуникаций

Возможности IP-интеркомов как части системы унифицированных коммуникаций города весьма широки. Рассмотрим несколько сценариев, в которых они уже успешно решают задачи по обеспечению безопасности граждан и информированию.

Для спасения на пляжах и в зонах отдыха

Проблема:

- при ЧС на пляжах и в парках у водоемов сообщения на пост спасения из-за паники поступают слишком поздно;
- раздетые и расслабленные люди судорожно ищут телефон, который оказывается разряжен или сеть перегружена.

Решение: использование SIP-интеркомов на пляжах и в городских парках с прямой коммутацией на службы спасения МЧС.

Полностью автономная точка с собственным питанием от солнечной батареи и каналом связи может выступать в роли публичной точки доступа Wi-Fi и точки круглосуточного видеоконтроля.

Для реализации программы "Умная и безопасная остановка"

Вызывная IP-панель обеспечит немедленную связь и реагирование в случае возникновения ЧС на остановочных комплексах, например, если у человека инсульт или сердечный приступ. Установка панели E21V решает задачи:

- мгновенной связи с экстренными службами нажатием одной кнопки;
- территориальной независимости ситуационного центра;
- возможности громкого встречного информирования о ГО и ЧС на местах;
- постоянного видеоконтроля и записи событий.

Для реализации программы "Умный и безопасный квартал + парк"

IP-SIP-вызывная панель, установленная в составе интегрированного решения "Умная опора освещения", обеспечит жителям квартала или посетителям парково-рекреационных зон немедленную связь с оператором службы информации или "Службы 112".

Умная опора – это:

- источник освещения и элемент декоративной точечной разноцветной подсветки;
- точка доступа в Wi-Fi-пространство города, метеостанция;
- точка видеоконтроля и панорамного доступа на 360 град.;
- элемент для трансляции музыки и информации по IP-сетям связи.

В случае возникновения экстренных ситуаций возможности смарт-опоры легко смещают свой акцент на оказание помощи и реагирование:

- кнопка паники и вызов полиции, скорой, а также других оперативных служб через встроенную интерком-панель E21A/V;
- выдача световой индикации о месте вызова и организация световой дорожки;
- осуществление громкого предупреждения о недопустимости правонарушений и сообщений уровня ГО ЧС.

Во многих случаях, когда счет идет на минуты и даже секунды, смарт-опоры освещения на базе системы унифицированных IP-коммуникаций позволят эффективно и быстро решать сложные ситуации, даже когда люди находятся в состоянии аффекта или травмированы, соответствующие службы будут точно знать, откуда пришел вызов и что происходит в непосредственной близости в этот момент.

Решение для железнодорожных составов и метро

В составе поезда необходима организация мгновенной и простой связи "пассажир – машинист" и голосовых анонсов "машинист – состав".

Проблемы:

- зашумленность, большие площади, загрязнения, вандалы;
- недоступность связи с участками из офиса или диспетчерской.

Решение:

- размещение SIP-интеркомов E21A/E21V во всех вагонах на постах связи "пассажир – машинист";
- использование выносных кнопок паники и экстренной сигнализации, активирующих возможный сценарий.

Каждая точка IP делает город умнее и безопаснее

Каждая точка IP представляет собой устройство, которое контролирует проход, обеспечивает видеоконтроль прилегающей территории и экстренную связь с полицией. IP-домофон позволяет осуществлять связь со всем экстренными службами и массово оповещать население в случае чрезвычайной ситуации. Можно будет выполнять оповещение и на уровне операторов, которые будут подключать IP-домофонию, и на уровне обслуживающих организаций. Задачи в этом случае могут быть разные: оповещение при пожаре, о взрывах на химических заводах, о загрязнениях.

Будущее IP-коммуникаций

Когда IP-коммуникации с помощью IP-домофонии прочно войдут в нашу жизнь, каждый получит свои выгоды.

Пользователь:

- биометрический проход домой;
- переадресовку звонков с домофона на мобильные и городские номера;
- новые сервисы;
- прогноз погоды, свежие новости;
- доступ к услугам типа mos.ru;
- возможность подать жалобу в управляющую компанию и в городскую администрацию;
- экстренную связь и др.

Управляющая компания:

- дополнительный заработок на сервисах и оборудовании;
- гарантию информирования жильцов о новостях и событиях в здании и во дворе;
- прием данных со счетчиков жильцов через мобильные приложения домофонии;
- простое удаленное управление системой;
- возможности рекламных услуг.

Город:

- видеофиксацию и выявление криминала;
- оперативное реагирование на вызовы;
- SOS, оповещение о ГО и ЧС;
- прямой интерфейс к жителю: опросы и пр.;
- учет количества проходов.

Удобно? Безусловно! Но чтобы это реализовать, нужно, чтобы IP-домофония стала массово использоваться. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Организация СКУД в многоквартирных домах комфорт-класса

Высокотехнологичный подход ГК "ПИК"

ГК "ПИК" – крупнейшая российская девелоперская компания, реализующая комплексные проекты в девяти регионах России и специализирующаяся на строительстве жилья комфорт-класса со всей необходимой инфраструктурой. Собственные производственные мощности позволяют компании ежегодно реализовывать свыше 1 млн кв. м недвижимости. Обслуживанием и эксплуатацией слаботочных систем в жилых комплексах занимается управляющая компания "ПИК-Комфорт", обеспечивая жильцам доступ к самым современным услугам и создавая комфортные условия для жизни. Андрей Овчаренко, инженер слаботочных систем ГК "ПИК", рассказал, какие технологии безопасности используются в новых ЖК, как организован контроль доступа на их территорию и за счет чего обеспечивается удобство и комфорт для жителей

Андрей Овчаренко
Старший инженер слаботочных систем ГК "ПИК"

– Какие основные задачи решаются с помощью СКУД в жилых комплексах?

– Современные системы контроля и управления доступом эффективно решают задачи обеспечения безопасности и предупреждают о проникновении посторонних лиц на подконтрольную территорию дома.

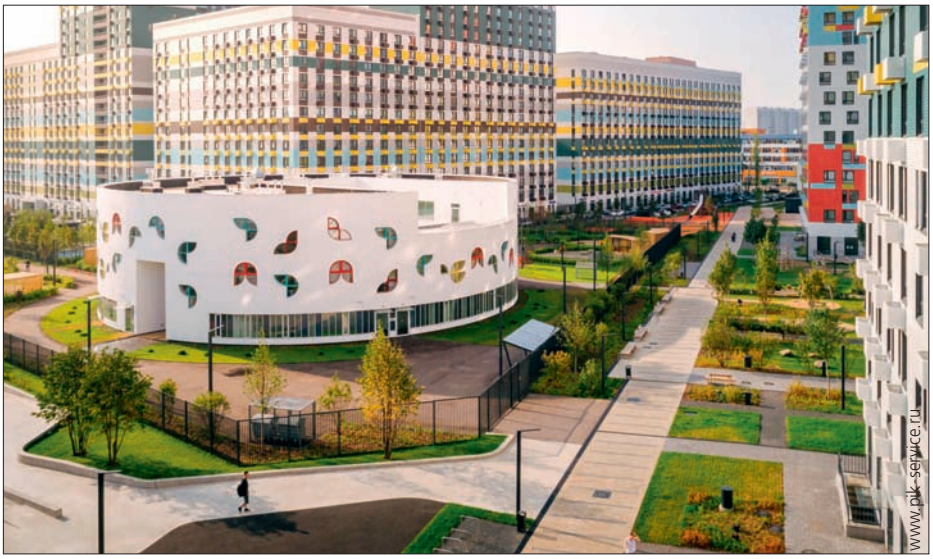
С помощью СКУД может осуществляться управление любыми дверьми, входящими в состав системы. Возможно слежение за дверьми по максимально дозволенной продолжительности ее нахождения в открытом состоянии. Для проведения всех необходимых проводов питания и подключения к локальной сети используется структурированная кабельная система.

В основе задач, решаемых системой контроля и управления доступом, лежит возможность разграничения полномочий персонала по времени и точкам доступа. Таким образом, типичными задачами, возлагаемыми на СКУД, являются:

- распределение прав доступа между собственниками и персоналом УК;
- протоколирование фактов прохода через контрольные точки;
- централизованное управление системой контроля доступа.

– При помощи каких инструментов контроля доступа обеспечивается безопасность, удобство и комфорт для жителей?

– Система СКУД, которая используется в многоквартирных домах так называемого нового фонда, обслуживаемых компанией "ПИК-Комфорт", является уникальным решением на рынке РФ и не имеет аналогов. Ее уникальность заключается в том, что это современное централизованное IP-решение. В основе системы СКУД лежат IP-домофоны, а также огромная кодовая база программного обеспечения, позволяющая централизованно ими управлять. В современных системах СКУД нет необходимости вешать ответную трубку в квартире и прокладывать к ней проводку: вызов с домофона приходит прямо на сотовый телефон собственника! В этом и заключается удобство и комфорт для жителей – возможность отвечать гостям, находясь в любой точке земного шара.



– Какую информацию и аналитику передает СКУД застройщикам, управляющим компаниям, жильцам?

– СКУД, как и полагается, собирает данные о времени прохода определенных ключей и хранит эти данные на протяжении длительного периода. Они могут быть раскрыты по официальному запросу правоохранительных органов и использованы по прямому назначению – для отслеживания и местонахождения злоумышленников.

– С какими другими системами интегрирована ваша СКУД?

– На сегодня система СКУД косвенно интегрирована с системой АСКУЭ и базируется на сетях ОСПД, которые являются основой слаботочных систем в МКД. Само собой, присутствует интеграция с охранно-пожарной сигнализацией для аварийного открытия замков в случае пожара.

На мой взгляд, будущее за интеграцией СКУД с системой лифтовой диспетчеризации. В ближайшие годы в домах комфорт-класса мы сможем увидеть подачу и вызов лифта брелоком от системы СКУД на нужный этаж, как сегодня это уже реализовано в элитных комплексах.

– Есть ли в планах внедрение программных подходов, аппаратной интеграции?

– В ближайших планах – интеграция видеоаналитики в систему охраны входов и разработка персональных предложений для пользователей интеллектуальных домофонов.

– Существуют ли в компании стандарты обслуживания жилых комплексов?

– Конечно, в компании существуют стандарты обслуживания ЖК, и в первую очередь они заключаются в скорости реагирования на заявки, поступающие от жильцов. Такой вопрос, как скорость и наличие ответа от УК на заявку собственника, регламентируется законодательно. УК "ПИК-Комфорт" успевает отрабатывать 99% заявок в минимальные сроки, которые значительно короче законодательно установленных.

– Как решается вопрос обработки и хранения персональных данных?

– Поскольку СКУД является централизованной и масштабной, можно предположить, что она собирает персональные данные жильцов, но это не так. Для доступа к системе жилец сам регистрируется с брелоками от домофона, которые получил в УК, и сам указывает свои

(или не свои) данные, которые будут использоваться как приветствие, но никак не контролируются со стороны УК.

– Без какого оборудования систем безопасности, по вашему мнению, нельзя обойтись при строительстве и эксплуатации современных ЖК?

– На мой взгляд, сегодня ни один современный МКД не строится без объединенной сети передачи данных, на которой базируются системы автоматической пожарной сигнализации (АПС), обнаружения вторжений (СОВ), охранного телевидения (СОТ), СКУД, автоматизированные системы коммерческого учета электроэнергии (АСКУЭ) и водоснабжения (АСКУВТ), системы лифтовой диспетчеризации.

– Какие новые современные технологии используются вашей компанией для охраны территорий, управления доступом, других задач при строительстве и управлении жилым фондом?

– ГК "ПИК" использует максимально возможное количество доступных современных технологий при строительстве дома и его слаботочных систем. Стоит отдельно отметить мониторинг всех ЖК в едином мониторинговом центре, который позволяет знать текущее состояние всех слаботочных систем дома в реальном времени и оперативно принимать действия по устранению аварий.

– На что, по вашему опыту, необходимо обращать внимание при выборе поставщиков оборудования?

– Выбор поставщиков – с этим сталкивался любой человек, начиная от выбора продавца стирального порошка и заканчивая выбором застройщика, в жилом комплексе которого он будет жить. Так и нам приходится выбирать поставщика оборудования, которое будет использоваться при строительстве. Для того чтобы принимать правильные решения, нужно владеть информацией о системах, которые представлены на рынке. В этой сфере конкуренция велика, каждый год появляются новые решения, потому приходится быть в тренде и понимать, какие есть альтернативы. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Безопасность и комфорт – базовые принципы создания умных городов

В современном мире города сталкиваются с большим числом проблем, вызовов и угроз: высокая плотность населения, растущая миграция, транспортные и экологические проблемы, изменение требований жителей и бизнеса к качеству городской среды и предоставляемых услуг. В этих условиях происходит постепенный пересмотр подходов к управлению развитием городов, которое все больше опирается на передовые информационные и коммуникационные технологии, цифровизацию и большие данные

Александр Бодров
Генеральный директор
АО "СФЕРА"

Даниил Бодров
Заместитель генерального директора
АО "СФЕРА"

Мировая урбанизация уже превысила 50% и достигнет 70% к 2050 г.

В идеале должен быть совершен переход к интегрированной цифровой городской экосистеме, которая отвечала бы на возникающие вызовы, способствовала бы удовлетворению потребностей всех ее участников (жителей, бизнеса, властей и т.д.), а также обеспечивала бы более эффективную интеграцию отдельных элементов городской инфраструктуры.

Города – это основа социально-экономического развития практически всех стран мира. По оценкам ООН, в 2015 г. мировая урбанизация превысила 50% и достигнет 70% к 2050 г. По мнению ряда исследователей, глобальная конкуренция постепенно переходит от стран к городам: 57% мирового ВВП генерируют 750 крупнейших мегаполисов, а корпорации все чаще делают выбор, например, не между Бразилией и Китаем, а между Сан-Паулу и Шанхаем.

Первые упоминания термина "умный город" (Smart City) появились в начале 2000-х гг. Развитие информационных технологий привело к тому, что восприятие концепции умного города значительно изменилось, но базовые принципы и подходы к использованию ИТ-инфраструктуры не потеряли своей актуальности.

Поколения умных городов

Исследование мировой практики позволяет определить три условных поколения умных городов. Первое поколение характеризуется переоснащением физической инфраструктуры и внедрением изолированных ИТ-решений, при этом основными заинтересованными лицами являются представители бизнеса – поставщики технологических решений и услуг.

Далее происходит формирование интеллектуальной цифровой инфраструктуры за счет внедрения широкополосного и мобильного доступа в Интернет, технологий IoT (Интернета вещей), основная роль отводится органам муниципальной власти.

Третье поколение характеризуется формированием полностью интегрированной интеллектуальной инфраструктуры, которая позволяет осуществлять сбор и аналитику данных в реальном времени, при этом цифровые сервисы дают возможность жителям города активно участвовать в процессе развития города и в принятии важных решений.

Сегодня принято говорить об умном устойчивом городе (Smart Sustainable City), в котором

технологические инструменты используются, с одной стороны, для повышения качества жизни, конкурентоспособности и эффективности функционирования, с другой – обеспечивают благоприятную безопасную социальную и экологическую среду.

В России проект "Умный город" реализуется в рамках национального проекта "Жилье и городская среда" и национальной программы "Цифровая экономика". Цели, обозначенные в этом проекте, соответствуют общемировым тенденциям: повышение конкурентоспособности российских городов, формирование эффективной системы управления городским хозяйством, создание безопасных и комфортных условий для жизни горожан.

В 2014 г. Правительством Российской Федерации принята концепция построения и развития аппаратно-программного комплекса "Безопасный город" с целью повышения общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач.

Органы власти субъектов Российской Федерации и муниципальные органы государственной власти обеспечивают комплексное решение вопросов по всем аспектам безопасности жизнедеятельности населения. Такие структуры, как центры управления в кризисных ситуациях (ЦУКС), дежурные диспетчерские службы, территориальные подразделения федеральных органов исполнительной власти, сконцентрированы на отдельных аспектах, например безопасности населения и муниципальной (коммунальной) инфраструктуры, включая общественную безопасность и защиту от чрезвычайных ситуаций, безопасности на транспорте и экологической безопасности.

Шанхай. Инвесторы все чаще делают выбор не между странами, а между городами

Первые упоминания термина "умный город" (Smart City) появились в начале 2000-х гг. Развитие информационных технологий привело к тому, что восприятие концепции умного города значительно изменилось, но базовые принципы и подходы к использованию ИТ-инфраструктуры не потеряли своей актуальности

Для эффективного и комплексного решения вопросов обеспечения общественной безопасности, безопасности среды обитания и рационального развития ландшафта автоматизации городских территорий необходимо создание единого информационного пространства, обеспечивающего координацию действий и эффективное взаимодействие всех участников процессов и уровней управления, а также высокое качество и быстрота принимаемых решений.

Выход есть

Для решения этих задач целесообразно создание технологической платформы, обеспечивающей комплексную автоматизацию процессов для следующих целей:

- сбор первичной информации о состоянии среды обитания, а также информации по инцидентам и чрезвычайным ситуациям;
- автоматизация процессов реагирования и координация действий;
- передача первичной, агрегированной и аналитической информации участникам процессов всех уровней;
- поддержка принятия решений.

Применение комплексного подхода гарантирует ряд существенных преимуществ, главные из которых:

- сокращение издержек по управлению процессами обеспечения безопасности населения и среды обитания;
- оперативное предоставление полной и достоверной информации по инцидентам, угрозам и рискам всем заинтересованным лицам и организациям, включая СМИ;
- повышение качества оценки рисков и прогнозирования наступления и развития кризисных ситуаций и происшествий;
- повышение оперативности и качества реагирования на основе автоматизированного многофакторного анализа информации.

В результате внедрения такой платформы снижается ущерб и минимизируются последствия чрезвычайных ситуаций. Дополнительным положительным эффектом является улучшение бизнес-климата и общей социально-экономической обстановки.

Разумеется, технологическая платформа, создаваемая для решения вышеперечисленных задач, должна соответствовать повышенным требованиям в области безопасности и доступности, быть независимой от проприетарных продуктов и технологий глобальных корпораций. Для этого целесообразно внедрять и использовать технологии с открытым исходным кодом, что также согласуется с приказами Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об импортозамещении в ИТ и директивой Правительства РФ "О преимущественном использовании отечественного программного обеспечения", согласно которой доля отечественного программного обеспечения в органах власти и местного самоуправления, а также в госкомпаниях должна превысить 50% к 2021 г.

Препятствия для развития

Одно из наиболее существенных препятствий для развития и внедрения технологий умного и безопасного города – отсутствие нормативной документации для применения ряда технологических решений (включая Интернет вещей, большие данные, умные города, умное производство и т.д.). Нужно также отметить ограниченность бюджетных средств, которая не позволяет муниципальным органам государственной власти применять передовые технические решения.

Правильный подход

Очень важно методически правильно подходить к цифровизации городов. Необходимо проводить концептуальное и техническое проектирование, так как вновь создаваемые компоненты цифрового ландшафта должны вписываться в единую концепцию развития.

Формулировки целей и задач "Безопасного города" и "Умного города", указанные в нормативных документах, а также сложившаяся мировая практика позволяют сделать вывод о том, что концептуально умный город включает элементы безопасного города в части обеспечения безопасности населения, а также совершенствования системы управления. А безопасность и комфорт, как неразрывные понятия, закономерно вошли в список базовых принципов создания и развития умных городов. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Умный город: стрим от камер видеонаблюдения по радиолинку

Еще совсем недавно профессионалы в области безопасности скептически относились к установке беспроводных систем даже в ситуациях, когда протянуть оптоволокно к месту монтажа оборудования было проблематично… Специалисты зачастую выражали сомнения, могут ли многие беспроводные системы умного города работать надежно в защищенном режиме. Время расставило все по своим местам

Максим Редин
Региональный представитель компании Siklu Communication Ltd.

Сегодня технологические преимущества беспроводных решений отмели все подобные сомнения, во многом благодаря появлению надежного, простого в монтаже и доступного по цене решения. Появилась беспроводная технология на миллиметровых радиоволнах – E-band (70/80 ГГц), возможно, на сегодняшний день это одно из лучших решений в сфере беспроводных систем, активное развитие которых началось несколько лет назад.

Как это связано с умным городом?

Непростые вызовы, стоящие перед современным обществом, – террористические угрозы, криминальная обстановка, техногенные и природные катастрофы – требуют достаточно плотного размещения видеокамер и прочих датчиков безопасного города и умного города. Важно понимать, что разворачивание данных устройств идет поверх существующей и сложившейся телекоминфраструктуры, а не строится с нуля. Поэтому как планировщикам видеонаблюдения, так и сетевым архитекторам умного города зачастую весьма непросто размещать камеры и подключать их к существующей сети заказчика.

Частот нет, но вы держитесь©

На протяжении многих лет у профессионалов в области безопасности было только две возможности для передачи видео: по кабелю (оптоволоконный, медный) или через радиомост. Несмотря на повсеместное строительство оптоволоконных сетей (далее ВОЛС – волокно-оптическая линия связи) в городах, у ВОЛС остаются серьезные недостатки, которые "уравновешивают" их важные преимущества. Надежность, защищенность и скорость передачи данных по оптоволоконному кабелю высоки, но, к сожалению, цена, затраты времени и трудности на этапе проектирования и монтажа – тоже. ВОЛС – это всегда долго и дорого, подчас не укладывается в требуемые рамки (сроки и бюджет) конкретных проектов.

Лучше развивать ВОЛС как значимую опорную сеть, чем осуществлять физически разводку и разварку к каждому фонарному столбу, чтобы подключать все камеры уличного видеонаблюдения

По своему большому опыту знаю, что в центре городов кабельные канализации, как правило, уже забиты старыми кабелями, поэтому прокладка новых в существующую кабельную канализацию (инфраструктуру) зачастую сильно затруднена или вообще невозможна. Поэтому даже сегодня, несмотря на глубокое проникновение телекоммуникаций, вариант беспроводного канала все еще остается актуальным и востребованным. Скажу больше, порой без радиорешений не построить требуемую сеть. В то же время применение традиционной массовой беспроводной технологии в диапазоне ниже 6 ГГц – те самые частоты 2,4 ГГц, 5 ГГц – для сетей систем безопасности не "вытягивают", они не смогли стать надежным и гибким техническим решением, даже с массой оговорок.

Радиочастотный ресурс – ограничен

Отдельное внимание следует уделить выбору беспроводных технологий, которые смогут отвечать задачам безопасности и видеонаблюдения, решаемым планировщиками сетей для умного города. Поэтому рекомендую взвешенный подход, позволяющий определиться с технологией передачи данных, радиочастотным спектром и т.д. И тут важнейшую роль играет используемый частотный радиодиапазон. Дело в том, что радиочастотный ресурс сам по себе ограничен и исчерпаем, и за годы использования он уже значительно заполнен радиоисточниками. Наиболее остро стоит вопрос в популярных диапазонах 2,4 ГГц и 5 ГГц, которые активно используются населением под Wi-Fi, а также небольшими местными операторами для работы радиомостов и т.д. Все перечисленные выше факторы привели к сильному зашумлению данного популярного диапазона. И это несмотря на то, что на частотах 2,4 ГГц действуют ограничения от регулятора (которые часто нарушаются пользователями частот), а на использование частоты в полосе 5 ГГц необходимо получать разрешения. Именно плотная работа операторов на радиомостах в упомянутых частотах (Wi-Fi) оказывает наибольшее негативное влияние на данный спектр частот. Дело в том, что многие используют радиомосты 5 ГГц, в режиме "точка-многоточка", именно такая деятельность позволяет базовой станции излучать во всем секторе углов, потенциально мешая другим приемникам. А теперь представьте, что все пытаются так работать, создавая интерференцию и мешая друг другу. Напомню, это негативное явление называется интерференция радиоволн. Вдобавок на практике случается, что частотную регуляцию нарушают, и это приводит к значительному ухудшению интерференционной обстановки. Все вышесказанное привело к тому, что этот радиодиапазон (2,4 ГГц, 5 ГГц) был просто "убит". То есть услуги, реализованные на таких радиомостах, в данных частотах будут негарантированными ("как получится"). Нельзя также сбрасывать со счетов вполне реальную уязвимость таких систем для кибератак именно на уровне радиодоступа. Естественным выходом из сложившейся ситуации видится использование других частотных диапазонов, где отсутствуют указанные негативные явления.

Целесообразно выбирать радиорешения, работающие в беспомеховом радиодиапазоне 60 и 70/80 ГГц (соответственно, V-band и E-band)

Сделайте правильный выбор

Другими словами, наличие диапазона 60 и 70/80 ГГц является спасением в сложившейся ситуации. У них есть неоспоримые веские преимущества. Во-первых, они бесплатны для работы и не требуют частотных разрешений, во-вторых, в них невозможно кому-то помешать непреднамеренно или со злым умыслом создать помеху, потому что используются остронаправленные антенны (ширина луча антенны – один градус и меньше). В-третьих, отсутствует какая-либо возможность для несанкционированного доступа в сеть и последующих кибератак.

Для большинства развертываний систем безопасности и видеонаблюдения ненадежная и уязвимая беспроводная сеть недопустима.

От современных сетей безопасности требуется постоянное соединение без помех и интерференции, при помощи которого картинка в реальном времени передается в сторону ядра сети (VMS). Напомним, что важной надстройкой описанной сети является ПО видеоаналитики. А видеоаналитика эффективна тогда, когда обеспечена именно онлайн-работа со стабильным подключением, возможностью моментально указывать и быстро реагировать на тревожные события.

Практика показала, что при плотном городском планировании радиосети (наличие множества источников излучения), когда большое количество технологий конкурируют на одних и тех же радиочастотах (точки доступа Wi-Fi, радиомосты), другие беспроводные сети на частоте ниже 5 ГГц не обеспечивают надежность и появляется риск серьезного сбоя сети безопасности

Видеонаблюдение без волокна? Поставьте E-band – гигабит по радио!

Появление на рынке систем безопасности новинок радиорешений в совершенно другом частотном диапазоне (миллиметровый) несколько лет назад стало началом революции. Получившие признание у операторов связи России радиолинки типа "точка-точка" (PtP) и рвущаяся на рынок новейшая технология "точка-многоточка" (PtMP) работают в целом неиспользуемом "океане" миллиметрового спектра (70/80 и 60 ГГц, соответственно, E-band и V-band) с узким лучом антенны, который серьезнейшим образом защищен от помех. Это определенно можно назвать физическим иммунитетом от радиоинтерференции. Технология PtP обеспечивает мультигигабитную пропускную способность (за счет широкого используемого спектра свободных частот) и в то же время надежную защиту от кибератак (просто нет возможности на физическом уровне по радиоинтерфейсу "достучаться" до устройства). Описанная технология V-band и E-band уже нашла широкое распространение во многих умных городах по всему миру. Сегодня видим их активное использование на культмассовых мероприятиях (таких как фестивали под открытым небом, спортивные соревнования), в инфраструктурных объектах (транспорт/каналы для трафика Wi-Fi в умных парках), радиозащищенное видеонаблюдение в морских портах, аэропортах, на удаленных умных парковках и в коттеджных поселках. Данный вид связи обеспечивает высокую скорость передачи данных и бесперебойное соединение, как у оптоволокна, для систем видеонаблюдения и IoT, что уже повсеместно используется при подключении датчиков умных/безопасных городов в проектах безопасности по всему миру. Для примера посмотрите реализацию одного из проектов безопасного города (см. рис.).

City Buena Park, CA – подключение видеонаблюдения и колонны экстренного вызова (Emergency Call Box – Code Blue)

Диапазон E-band – "король" всей беспроводки

Из всех беспроводных технологий системные интеграторы все чаще обосновано выделяют одну – частотный диапазон E-band 70/80 ГГц и V-band 60 ГГц. Именно эта технология обладает серьезными преимуществами при выборе средств подключения видеокамер наблюдения:

- частоты бесплатны и не зашумлены;
- не требуется получать разрешение на использование частот;
- кристальная чистота спектра (благодаря особым условиям распространения радиоволн);
- отсутствие интерференции и помех (благодаря очень узким лучам антенн – менее одного градуса);
- можно обеспечить передачу широкого потока данных (от 1 до 10 Гбит/с), что невозможно на других частотных диапазонах ввиду их ограниченности.

Построенные на этой технологии радиолинки снискали популярность в качестве радиомостов для подключения видеокамер и построения сетей в умных городах.

Монтаж радиосистемы типа E-band системные интеграторы назвали простым, и его может выполнить один человек. Встроенная техническая возможность таких комплектов позволяет пропускать через себя питание по Ethernet (PoE), что в итоге делает весь процесс развертывания высокоскоростной системы видеонаблюдения оперативно быстрым.

Системные интеграторы, даже те, кто пока незнаком с оборудованием, работающим в указанном частотном диапазоне, с легкостью могут проектировать и монтировать такие сети без специального обучения, добиваясь значительной скорости развертывания, закладывая высокую надежность и пропускную способность.

На рынке России можно найти радиорелейное оборудование, оптимизированное специально под задачи видеонаблюдения. Здесь необходимо обращать внимание на полезный функционал: наименьшие весогабариты, низкое энергопотребление (желательно стандартный PoE 25 Вт), возможность управлять и пропускать питание PoE через себя для запитывания камер. Это дает планировщикам сети бóльшую свободу действий, удешевляет стоимость конечного решения (например, экономия на аутдорных PoE-инжекторах). Данный сценарий подключения наиболее часто встречается на рынках США, Англии, некоторых стран Европы.

Если ваши сети работают на частотах V-band, E-band, вы можете забыть о потере важных эпизодов видео, которые не были записаны из-за помех в сети или чьего-то преднамеренного злого умысла. Благодаря производительности как у волокна и беспроводной гибкости такие радиосети безопасности являются идеальным решением для передачи видео в реальном времени и потока данных с датчиков систем безопасности умного города: они одинаково просты для планирования, разворачивания и доступны по бюджету. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

ПАК "Астра" – комплексная IoT-платформа для получения, хранения, обработки и визуализации данных

Представляет ЗАО "НТЦ "ТЕКО" www.teko.biz

Приоритетные возможности

Комплексная открытая многофункциональная IoT-платформа ПАК "Астра" позволяет внедрять цифровые технологии в различные сферы жизни.

- **ПАК "АСТРА" для ЖКХ ("Цифровое ЖКХ")**. Обеспечение контроля и управления инженерными системами, сбор данных с узлов учета о расходе ресурсов. Выгода – в своевременном реагировании и предотвращении нештатных ситуаций, контроле, прогнозировании и экономии расхода воды, энергоресурсов.
- **ПАК "АСТРА" для безопасности ("Безопасный город").** Мониторинг и управление персональными и общественными охранными системами. Польза – обеспечение защищенности жизненно важных интересов жителей, социальных групп, а также инфраструктуры города от возможного нанесения ущерба.
- **ПАК "АСТРА" для удобства ("Умный дом").** Создание комфортной среды для отдыха, реабилитации и проживания. Преимущество – повышение уровня удовлетворенности жизнью.

Новый подход к решению задач

ПАК "Астра" решает ряд важных задач из сферы ЖКХ.

- **Учет ресурсов.** Комплексная автоматизированная подсистема включает в себя различные компоненты для сбора, доставки, хранения и обработки данных с узлов учета с последующей передачей информации о потребленных ресурсах во внешние информационные системы, а также индивидуальным пользователям. Удобная альтернатива "походам" по квартирам, офисам, техническим этажам и помещениям. Помогает предотвратить чрезвычайные ситуации (прорыв канализации, водоснабжения, утечку газа или превышение уровня контролируемых параметров – давление, углекислый газ и т.д.), так как сбор и передача данных с технологических датчиков происходят в едином диспетчерском центре. Внутренние алгоритмы и сценарии, реализованные в коде платформы ПАК "Астра", вовремя и в автоматическом режиме перекрывают водоснабжение, подачу газа, включают вытяжную вентиляцию, не допускают развитие чрезвычайной ситуации и материальный ущерб. Накапливание и анализ полученных данных (Big Data) позволяют с помощью нейросетей предотвращать техногенные аварии до их возникновения. Альтернатива выездам служб реагирования по факту события.
- **Диспетчеризация.** Отображение в реальном времени контролируемых параметров, оповещение о нерасчетных режимах и параметрах, выходящих за пределы нормы, дистанционное управление исполнительными устройствами (насосы, освещение, шлагбаумы, замки, ворота и т.д.).
- **Безопасность.** Обеспечение пожарной безопасности и контроль доступа в охраняемые помещения. Кнопки-браслеты для вызова персонала и тревожной сигнализации для пожилых людей и детей. Речевое и светозвуковое оповещение при чрезвычайных ситуациях на территориях города, района, жилого комплекса. Передача тревоги в единый диспетчерский центр МЧС и полиции. Визуальный контроль ситуации с помощью удаленного подключения к видеокамерам, размещенным на территории жилых комплексов.

При реализации всех задач ПАК "Астра" позволяет уменьшить объем рутинного, неквалифицированного труда либо устранить его совсем. Открытость платформы обеспечивает интеграцию со всевозможными системами и устройствами различных производителей.

Конкурентные преимущества

Главным преимуществом ПАК "Астра" можно считать открытость для сторонних разработчиков и производителей. Программный интерфейс приложения (API) и набор средств разработчика (DevKit) позволяют внедрить и локализовать платформу в информационные системы и бизнес-процессы. Надежность умных устройств собственного производства (более 100 изделий различного назначения) проверена временем и подтверждена многочисленными сертификатами и наградами. Программное обеспечение прошло экспертизы и включено в реестр Минкомсвязи России и ФКУ НИЦ "Охрана" Росгвардии, что позволяет использовать платформу на территории РФ для задач повышенной важности.

На базе дата-центра, который соответствует требованиям Uptime TIER III и аттестован согласно требованиям PCI DSS, функционируют два равнозначных публичных сервера ПАК "Астра", между которыми реализована репликация данных в реальном времени, что обеспечивает доступность сервисов 99,98% времени. Использование публичного сервера и клиентского ПО бесплатное. При необходимости имеется возможность развернуть собственный облачный сервер на базе платформы ПАК "Астра" в комплекте с бесплатным обновлением системы и расширенной технической поддержкой на всех этапах.

Технические особенности

1. Масштабируемость. Объединение и управление с мобильного устройства 1 млн умных приборов различного назначения.
2. Производительность и безопасность. Поддержка до 300 тыс. одновременных сессий с шифрованием 128-битными ключами.
3. Технологии. Платформа применяет уникальную систему передачи данных в постоянно открытом TCP-канале. Это означает, что оборудование постоянно поддерживает открытый асинхронный канал связи с сервером и готово к обмену в любой момент времени, независимо от того, кто является инициатором обмена. При этом данный функционал обеспечивается без дополнительных VPN, туннелирования, открытия IP-портов на оконечных устройствах, а также без применения "белых" IP-адресов.

Экономическая эффективность

Внедрение ПАК "Астра" на базе телекоммуникационных компаний дает возможность сократить издержки благодаря автоматизации внутренних бизнес-процессов, увеличить базу абонентов на 10% за счет внедрения новых услуг и тарифов, повысить на 20% коэффициенты APRU/APRA и тем самым увеличить прибыль компании.

Совокупный экономический эффект от внедрения в России технологий IoT в электроэнергетике, здравоохранении, сельском хозяйстве, логистике, а также в сегментах умного города и умного дома составит около 2,8 трлн рублей к 2025 г. Таковы данные исследования компании Pricewaterhouse-Coopers (PwC). В нем уточняется, что подобные показатели могут быть достигнуты за счет уменьшения затрат на техническое обслуживание и ремонт производственных активов, повышения энергоэффективности производств, эффективности производственных процессов и т.д. ■

см. стр. 128 "Ньюсмейкеры"

Потребители

ЖКХ, безопасный город, умный дом

Проекты

ПАО "МГТС", АО "Уфанет", ПАО "Таттелеком", "Липецкие Информационные системы", компания "Теле-Плюс", Управление вневедомственной охраны Росгвардии, более 50 частных охранных предприятий РФ и стран СНГ

Появление на рынке	Декабрь 2017 г.
Ценовой сегмент	Низкий

Досмотровый комплекс THERZ-7A: технология исследования галактик для безопасности пассажиров в метро

Представляет "ОКБ "Астрон"
www.astrohn.com, www.astrohn.ru

АСТРОН

Технология сканирования терагерцового излучения в данном виде была впервые представлена Европейским космическим агентством в начале 2000-х гг. Использование терагерцовых волн при сканировании космоса позволяет ученым лучше понять этапы формирования далеких галактик и звезд

Новый подход к решению задач

Система THERZ-7A сканирует пассажиров на предмет естественно излучаемых их телами терагерцовых волн, частоты которых находятся в промежутке между инфракрасным и сверхвысокочастотным микроволновым диапазонами. Если у человека есть запрещенный предмет (металлический или неметаллический, оружие или взрывчатка), он блокирует излучение и позволяет обнаружить себя. Терагерцовое излучение, в отличие от рентгеновского, является неионизирующим. Различные биологические ткани обладают разным поглощением в данном диапазоне, что обеспечивает контрастность снимков. По сравнению с видимым и ИК-излучением терагерцовое менее подвержено рассеянию. В этом диапазоне прозрачны многие сухие диэлектрические материалы (ткани, дерево, бумага, пластмассы), поэтому терагерцовое излучение предпочтительно использовать для сканирования больших потоков людей в метрополитене.

Появление на рынке	2019 г.
Ценовой сегмент	средний

Конкурентные преимущества

Система THERZ-7A позволяет охранному персоналу проводить быстрые и эффективные проверки потока людей без физического контакта. Данный комплекс может быть легко приспособлен к имеющейся системе безопасности и не влияет на ее производительность. Устройство не облучает объекты и не создает опасности для здоровья людей, в том числе имеющих кардиостимуляторы или беременных женщин. Система полностью открыта и не вызывает клаустрофобии. Устройство не отображает анатомические подробности, тем самым защищая личную неприкосновенность, не нарушая нормы морали. Система THERZ-7A работает в реальном времени, ее установка не создает длинных очередей на входе и выходе.

Принцип действия

Система THERZ-7A работает на основе терагерцового сканера, который обнаруживает скрытые объекты, различая естественную энергию (излучение) человеческого тела в миллиметровом диапазоне и излучение неживых предметов, таких как взрывчатые вещества и оружие, даже если они спрятаны под одеждой. Алгоритм обнаружения обводит рамкой потенциально опасный объект и включает тревогу, которая оповестит охрану о возможной проблеме, чтобы сотрудники службы безопасности могли дополнительно проверить подозреваемого или же выключили сигнал тревоги. Система точно определяет изделия из металлов, керамики, пластмасс, композитных материалов, жидкости и гели.

Приоритетные возможности

Применение данного комплекса на объектах позволит достичь следующих эффектов:

- заблаговременное дистанционное обнаружение скрытых предметов на подходе к объекту;
- обнаружение неметаллических скрытых предметов;
- повышение эффективности оперативных организационно-технических мероприятий;
- безвредность для людей;
- неинвазивность (без отображения анатомического строения);
- возможность организации качественного и эффективного дистанционного досмотра людей (в комплексе реализована возможность выгрузки результатов во внешние информационные системы контроля для распознавания лиц и др.).

Технические особенности

- Время хранения записанной видеоинформации – 30 суток. Предусмотрена возможность записи хранимой информации на внешние носители (съемный жесткий диск или твердотельный носитель информации).
- THERZ-7A работает от общепромышленной сети переменного тока напряжением 220 В (±10%), частотой (50±1) Гц.
- Общая электрическая мощность не превышает 150 Вт.
- Диапазон рабочих температур – от +5 до +40 °С внутри отапливаемых помещений без конденсирования влаги, степень защиты оболочки – IP20.
- Габаритные размеры блока камер – 660x650x245 мм.

Экономическая эффективность

Дальность обнаружения крупных предметов (скрытых под одеждой) составляет не менее 15 м. Пропускная способность в режиме прохода объекта досмотра – не менее 150 человек/час. Максимальное время, в течение которого выдается результат контроля, наличие или отсутствие предметов (при условии неподвижности объекта досмотра) не превышает 2 с.

Результаты досмотра, представленные оператору THERZ-7A на экране монитора, визуализируют скрытый предмет с его привязкой к месту нахождения на досматриваемом объекте.

THERZ-7A имеет возможность как автономной (самостоятельной) работы, так и в составе интегрированного комплекса технических средств охраны по каналу Ethernet. ■

см. стр. 127 "Ньюсмейкеры"

Камеры AXIS P1377/-LE и AXIS P1378/-LE: прицельное наблюдение за большими территориями

Представляет Axis Communications
www.axis.com

Приоритетные возможности

Новые сетевые камеры AXIS P1377/-LE и AXIS P1378/-LE оснащены фиксированным корпусом и обеспечивают быстрое реагирование на заданные сценарии, например несанкционированное проникновение в закрытую зону. Модели предназначены для высококачественной съемки объектов и людей в аэропортах, общественном транспорте, на складах. Могут выступать в качестве сдерживающего фактора для потенциальных злоумышленников.

Их можно установить как в помещении, так и на улице. Они отличаются превосходной детализацией изображения при разрешении 5 Мпкс и 4K.

В них используется чип нового поколения ARTPEC-7, который повышает производительность встроенного ПО и расширяет функции кибербезопасности оборудования.

Появление на рынке	февраль 2020 г.

Экономическая эффективность

1. Axis Forensic WDR гарантирует высокое качество изображения, даже когда в кадре имеются яркие и темные участки.
2. Благодаря Axis Lightfinder камеры выдают четкое цветное изображение в том числе при плохом освещении.
3. Модели оснащены технологией Axis Optimized IR и отлично работают даже в полной темноте.
4. Технология Axis Zipstream с использованием форматов сжатия H.264 и H.265 снижает требования к пропускной способности сети и объему дискового пространства.

Технические особенности

Возможность смены объективов и поддержка моторизованных объективов i-CS позволяют адаптировать камеры под конкретные требования объекта и ситуации.

Сетевые камеры для наблюдения в помещении AXIS P1377 и AXIS P1378 не содержат хлорированных и бромированных антипиренов, что повышает их работоспособность и производительность и при этом уменьшает негативное воздействие на окружающую среду. ■

см. стр. 128 "Ньюсмейкеры"

Умный двор доступен каждому с платформой KtoTam

Представляет "НПП Беверд"
www.beward.ru

BEWARD

Новый подход к решению задач

Решение является комплексной системой обеспечения доступа и видеонаблюдения на всей контролируемой территории. Административный интерфейс позволяет гибко настраивать права доступа жильцов, авто и журналировать вход жителей.

Платформа KtoTam112 помогает экстренным службам получать оперативный автоматический доступ на необходимую территорию.

Потребители

Решение эффективно для основных участников и субъектов сферы ЖКХ: жильцов, компаний, предоставляющих услуги домофонии, управляющих компаний, провайдеров услуг

Проекты

Пилотный проект KtoTam112 совместно с Департаментом информационных технологий города Москвы запущен в одном из московских дворов

Появление на рынке	IV квартал 2019 г.
Ценовой сегмент	Средний

Конкурентные преимущества

В настоящий момент это уникальное решение на российском рынке.

Технические особенности

1. Бесшовная интеграция в системы "Безопасного города".
2. Автоматическое открытие двери или шлагбаума при обнаружении авторизованного устройства.
3. Удаленное управление неограниченным количеством подключенных устройств в одной платформе.
4. Несколько удобных сценариев доступа на территорию, включая автоматический доступ экстренных служб.

Экономическая эффективность

Жильцы могут управлять доступом с мобильного устройства и настраивать базовый функционал под себя без дополнительных затрат.

Управляющая компания и операторы могут монетизировать дополнительные возможности платформы и внедрять различные варианты платных услуг. ■

см. стр. 127 "Ньюсмейкеры"

"Приток-А КОП-01" исп. 1-3 – современная классика

Представляет ООО ОБ "СОКРАТ" www.sokrat.ru

Появление на рынке	Ноябрь 2019 г.
Ценовой сегмент	Средний (до 12 000 руб.)

Потребители

Собственники квартир и частных домов

Решаемые задачи

"Приток-А КОП-01" предназначен для построения охранной и тревожной систем сигнализации. Три исполнения и возможность работы с беспроводными извещателями позволяют в короткие сроки оборудовать любую квартиру или дом.

Конкурентные преимущества

Комбинация работы с защищенными от копирования идентификаторами "Приток-NFC" и классической силиконовой клавиатурой для лучшего тактильного контакта при работе с устройством.

Технические особенности

1. До 128 шлейфов сигнализации (при использовании МРШ).
2. Исполнения с литиевыми и свинцовыми АКБ.

Экономическая эффективность

В данном устройстве разработчики отказались от пожарной сигнализации (хотя это можно решить и с помощью внешнего модуля мрш-02), которая не нужна в большинстве квартир. Такое решение позволило снизить стоимость отдельно взятого прибора. ■

см. стр. 128 "Ньюсмейкеры"

Универсальный солдат "Приток-А КОП-02.6"

Представляет ООО ОБ "СОКРАТ" www.sokrat.ru

Появление на рынке	Ноябрь 2019 г.
Ценовой сегмент	Средний (15 000 руб.)

Потребители

Любой сегмент. Частные дома (коттеджи) с интеграцией в систему видеонаблюдения и СКУД, квартиры, посты охраны в торговых (офисных) центрах

Решаемые задачи

Охранно-пожарный контроллер "Приток-А КОП-02.6" позволяет органично объединить наиболее интересные аспекты таких сфер, как видеонаблюдение, контроль и управление доступом и охранно-пожарная сигнализация. При тревоге он способен автоматически вывести на экран изображение с ближайшей IP-камеры, в том числе с включением исполнительного устройства (например, прожектора на нарушаемом участке периметра).

Конкурентные преимущества

Решение отечественного производства с оптимальным соотношением "цена/качество".

Технические особенности

1. Сенсорный дисплей 7".
2. До 128 шлейфов сигнализации (при использовании МРШ).
3. Просмотр изображения с IP-видеокамер. ■

см. стр. 128 "Ньюсмейкеры"

26-я Международная выставка
технических средств охраны
и оборудования для обеспечения
безопасности и противопожарной защиты

securika Moscow

a Hyve event

Москва, Крокус Экспо

13–16 апреля 2020

Видеонаблюдение

Контроль доступа

Охрана периметра

Противопожарная защита

Сигнализация и оповещение

Автоматизация зданий

Hyve

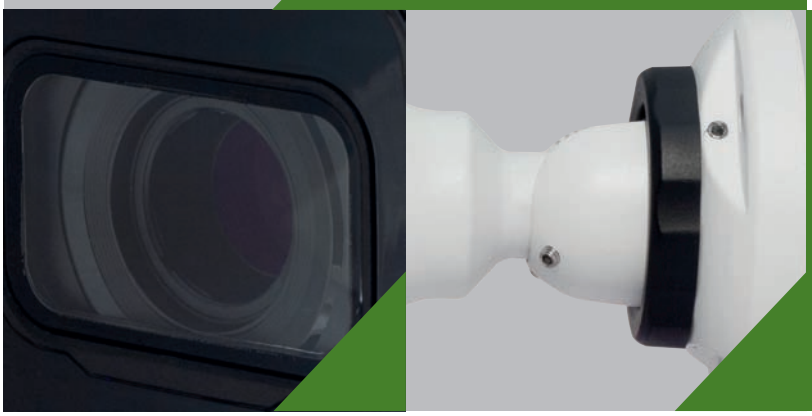
securika-moscow.ru

Бесплатный билет по промо-коду:

sec20pE

ТЕСТ

Видеокамеры 4–5 Мпкс с моторизованным объективом



Разрешение сенсоров, использующихся в видеонаблюдении, непрестанно увеличивается. В отличие от камер мобильных устройств, для решаемых в видеонаблюдении задач важно не номинальное количество пикселей, а детализация изображения. Реальное разрешение съемки зависит от сенсора, оптики, мощности вычислителя, освещенности... В итоге камеры с мегапиксельным сенсором могут показывать менее детализированную картинку, чем модели с меньшим количеством пикселей.

Такая ситуация наблюдается, когда на рынке только появляются камеры, оснащенные сенсорами с более высоким разрешением. Технология производства новых моделей еще не идеальна, используются некоторые компоненты предыдущего поколения, еще нет оптимальных алгоритмов обработки видеосигнала. При этом характеристики старых моделей продолжают улучшаться. Новаторские устройства обычно существенно дороже привычного оборудования. Конечно, спустя какое-то время новые модели начинают практически во всем превосходить старые.

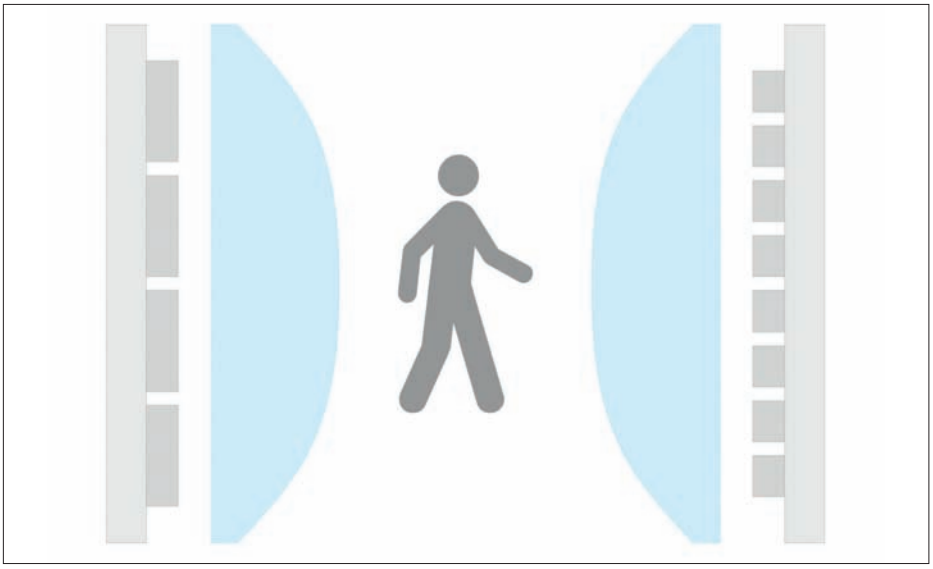
Сейчас подобное происходит среди видеокамер с сенсорами 2 Мпкс и 4–5 Мпкс. Разрешение у камер 4 Мпкс, при прочих равных условиях, превосходит разрешение FullHD-моделей. Чувствительность устройств массового сегмента сравнялась. Разумеется, для камер с более высоким разрешением приходится использовать и более емкий видеоархив, но модернизация алгоритмов сжатия видеосигнала сглаживает и это различие.

Тестирование проведено и предоставлено независимой тестовой лабораторией CCTVLAB

Все решает объектив

Когда речь заходит о реальном разрешении камеры, важно понимать большое влияние объектива на эту характеристику. Камера может оснащаться видеосенсором с любым количеством мегапикселей и объективом, предназначенным для сенсора 1 Мпкс. В этом случае реальное разрешение видео не превысит 1 Мпкс. Обычно моторизованные объективы дороже, но позволяют более точно подобрать угол обзора, чем фиксированные. Камеры с моторизованными объективами сейчас доступны практически у любого производителя.

В предыдущем тесте[1] в камерах 2 Мпкс мы проверили разрешение, чувствительность и характеристики объективов. В этот раз мы решили посмотреть, что в тех же условиях покажут модели с разрешением 4–5 Мпкс.



Съемка одного объекта разными камерами с близкими физическими размерами сенсора (слева с меньшим разрешением сенсора, справа – с большим)

Почему сенсор с меньшим разрешением может оказаться лучше

В определенных ситуациях камеры 2 Мпкс снимают с лучшим реальным разрешением, чем модели, использующие сенсор с большим номинальным разрешением. Это может быть обусловлено технологическим развитием процесса изготовления и применением более качественных компонентов.

Но есть и фундаментальная причина. Камеры фиксируют происходящее перед объективом за счет светочувствительных элементов в видеосенсоре. По сути, это и есть пиксели камеры. Их количество определяет итоговое разрешение матрицы. При других равных параметрах светочувствительность матрицы высокого разрешения меньше, чем матрицы низкого разрешения. Это связано с тем, что эффективная светочувствительная площадь с ростом количества пикселей уменьшается за счет увеличения площади "мертвых зон" между ними.

В обычных условиях освещенности реальное разрешение камер достигает практически максимального значения. Оно больше в камерах, оснащенных сенсорами с большим количеством пикселей. При снижении освещенности реальные разрешения могут оказаться значительно меньше максимальных значений. Получается, что камеры с меньшим числом пикселей могут фиксировать сцену с большей детализацией, в особенности если речь идет о сенсорах с одинаковым физическим размером.

С величиной видеопотока камеры ситуация более сложная. Современные видеокодеки максимально эффективно сжимают видео с неподвижными сценами, а большую часть времени камеры снимают именно такие сцены. В этом случае различие между 4 и 2 Мпкс будет практически незаметно. А вот при постоянном движении в кадре битрейт в моделях 4 Мпкс больше, чем в камерах 2 Мпкс. Конечно, битрейт при снижении реального разрешения тоже закономерно уменьшится.

Что тестируем?

Мы решили проверить видеокамеры с высоким разрешением и ограничились следующими характеристиками:

- **разрешение – 4–5 Мпкс;**
- **уличное исполнение;**
- **моторизованный объектив.**

Предоставленные модели

В результате в лаборатории оказались следующие образцы:

- **BEWARD SV3210RZ2;**
- **Bolid VCI-140-01;**
- **Novicam PRO 48.**

Еще мы взяли одну недешевую камеру 2018 г. Эта модель оснащена сенсором 4 Мпкс старого поколения OV4689 разработки 2013 г. Обозначим ее как Noname и посмотрим, как она будет выглядеть рядом с современными вариантами.

Удобным для теста оказалось то, что все модели имеют схожее разрешение по горизонтали, а значит результаты измерений вполне можно будет сопоставить для всех устройств. Разрешение по вертикали будет просто больше у камер с большим разрешением сенсора.

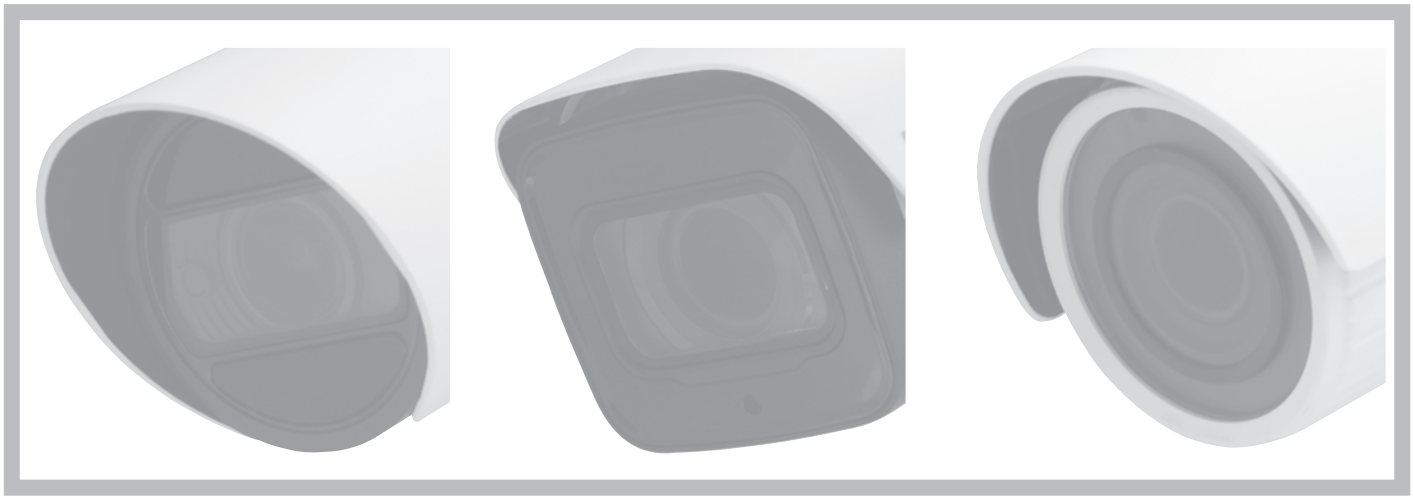
Как проводятся измерения

Измерим реальное разрешение камер при помощи специальных тестовых таблиц. Установим влияние освещенности на разрешение камер, или их чувствительность. Для этого измеряем разрешение при уменьшении освещенности со 100 до 0,1 лк.

Выясним, насколько меняется разрешение камер при изменении фокусного расстояния объектива.

Определим углы обзора, измерив видимую камерой область при минимальном и максимальном фокусном расстоянии объектива.

Определим быстродействие объектива как измеренное время изменения угла обзора от минимального до максимального значения.



1 Тестирование "Видеокамеры 2 Мпкс с моторизованным объективом" // Системы безопасности. 2019. № 6. С. 46–50.

BEWARD SV3210RZ2

Предоставлена компанией НПП "Бевард"

Единственная модель в тесте с разрешением 5 Мпкс. Обладает наилучшей чувствительностью. Лидирует по стабильности разрешения при изменении кратности объектива. Имеет один из самых быстрых объективов.

Производитель подчеркивает, что в модели применяется современный высокочувствительный сенсор Sony Starvis. В IP-камере, по словам производителя, включена поддержка восьми функций интеллектуального видеоанализа (по лицензии). Указан диапазон температур эксплуатации от -40 до +60 °С. Заявленная степень защиты электрооборудования от влаги и пыли соответствует классу IP67. Камера может питаться как от сети 12 В, так и по PoE, причем гер-

метичное подключение осуществляется внутри корпуса.

Производитель отмечает, что для эффективного кодирования видеопотока в камере реализована поддержка кодека H.265 и режима Smart Stream. Для более качественной съемки в модели заявлена поддержка двукратного WDR до 120 дБ и цифровая стабилизация изображения. Модель поддерживает SIP-протокол и ONVIF profile S.

Bolid VCI-140-01

Предоставлена компанией ЗАО НВП "Болид"

Является лидером по величине разрешения при максимальной освещенности. Лидирует по ширине диапазона регулирования угла обзора и скорости его изменения от максимального до минимального значения.

В модели есть аудиовход и аудиовыход для подключения дополнительного звукового оборудования.

В камере реализована поддержка кодека H.265.

Заявляется водонепроницаемый пылезащищенный корпус с классом защиты IP67.

Производитель отмечает, что камеру можно эксплуатировать при температурах от -65 до +60 °С. Кроме того, кожух камеры

имеет антивандальное исполнение с заявленной степенью защиты IK10.

Модель оснащена встроенным адаптером PoE для питания по кабелю сети Ethernet. Заявлен расширенный динамический диапазон 120 дБ для одновременного отображения ярких и темных участков одного кадра.

NOVIcam PRO 48

Предоставлена компанией NOVIcam

Входит в число лидеров по чувствительности, показывая достаточно хорошую стабильность разрешения при снижении освещенности. Обладает одним из самых широких диапазонов регулирования угла обзора.

Производитель отмечает, что связка мегапиксельного сенсора и высокопроизводительного процессора превращает камеру в мультифункциональное устройство. Мегапиксельный моторизованный объектив с ИК-коррекцией позволяет выбрать угол обзора без необходимости разбора камеры. Заявлен температурный диапазон работы от -45 до +60 °С и корпус с классом защиты IP67. Производитель подчеркивает наличие встроенной

грозозащиты 2кВ и защиты от переходного напряжения.

Поддержка технологии PoE позволит использовать один кабель для передачи питания и данных. Отмечается, что камера обладает широким динамическим диапазоном WDR 120 дБ, поддерживает бесплатный облачный сервис P2P и стандарт ONVIF. Модель обеспечивает совместимость со всем оборудованием линейки NOVIcam PRO.

Таблица. Характеристики камер

Камера	Разрешение сенсора, Мпкс	Максимальное разрешение съемки, пкс	Скорость съемки при максимальном разрешении, кадр/с	Объектив, мм	ИК-подсветка, м	Стоимость, руб.
BEWARD	5	2560x1944	20	2,8–12	45	22 900
Bolid	4	2688x1520	30	2,7–13,5	50	25 424
NOVIcam	4	2560x1440	20	2,8–12	40	15 411
Noname	4	2688x1512	30	2,8–10	50	40 000

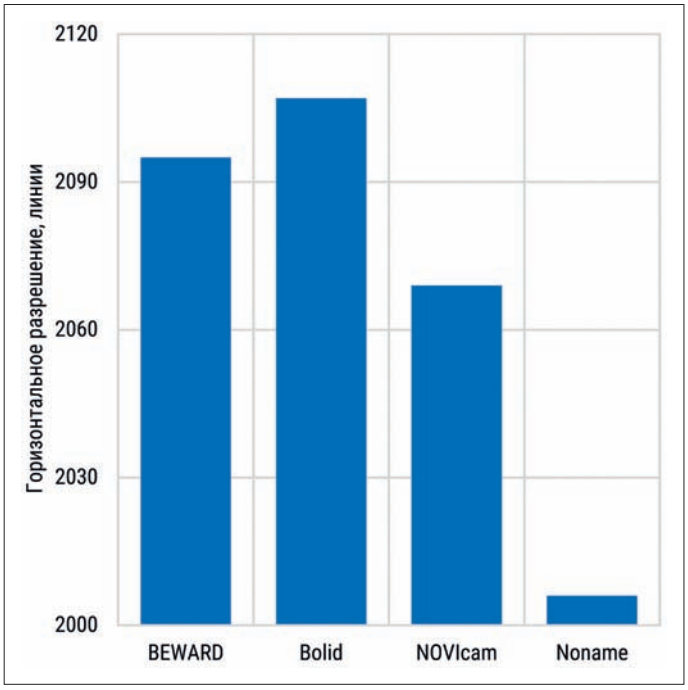


Рис. 1. Разрешение камеры по горизонтали при максимальной освещенности

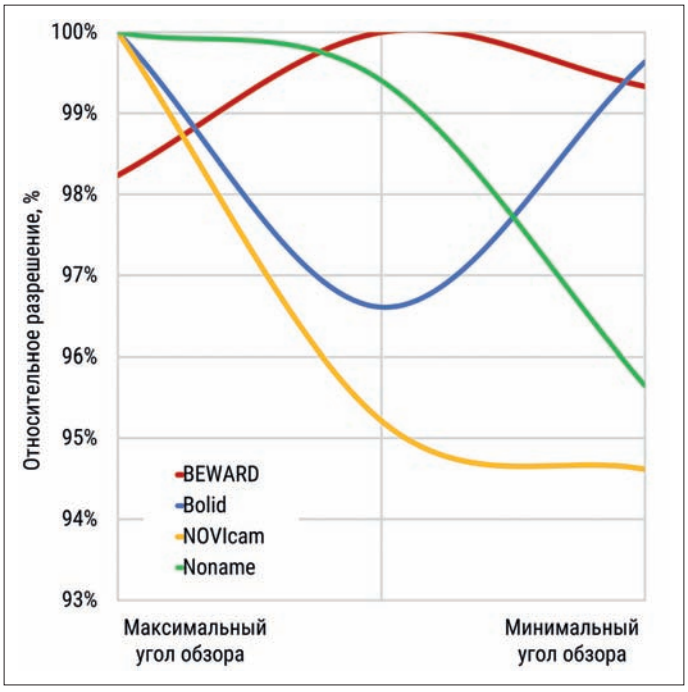


Рис. 2. Стабильность разрешения камеры по горизонтали при изменении угла обзора при максимальной освещенности (больше – лучше)

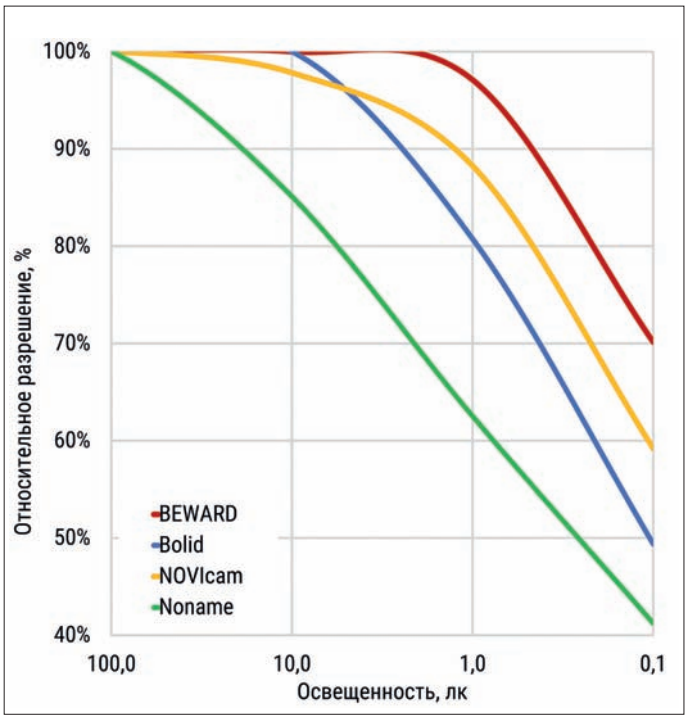


Рис. 3. Стабильность разрешения камеры по горизонтали при уменьшении освещенности (больше – лучше)

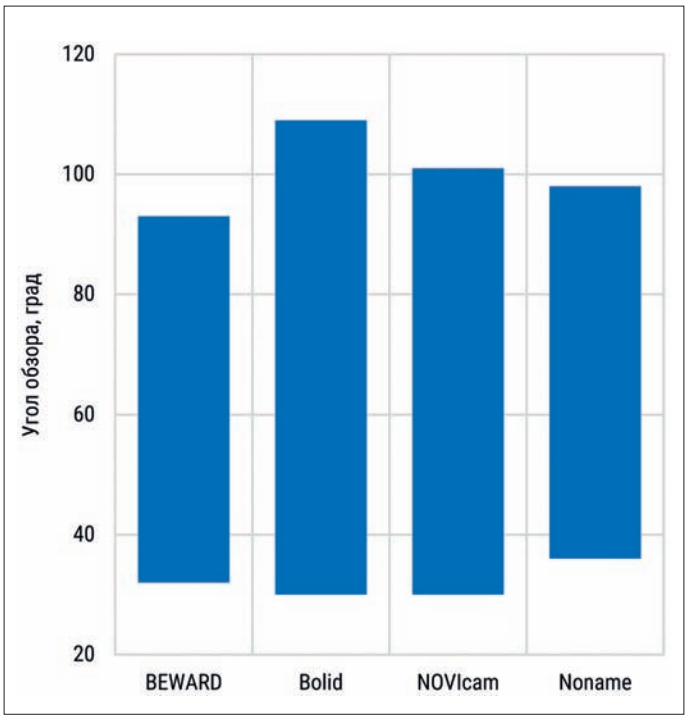


Рис. 4. Диапазон регулирования углов обзора камеры

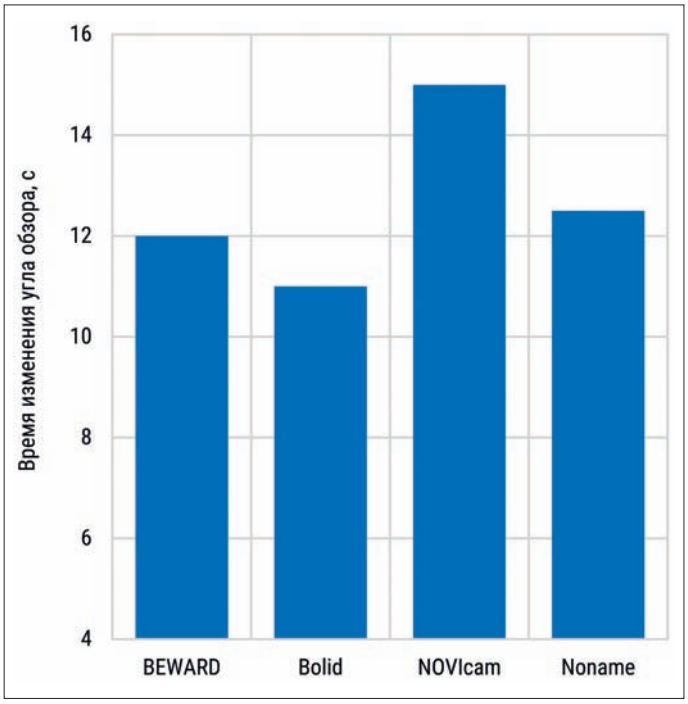


Рис. 5. Время изменения угла обзора камеры от минимального до максимального значения

Камеры фиксируют происходящее перед объективом за счет светочувствительных элементов в видеосенсоре или, говоря привычным языком, в пикселях. Их количество определяет итоговое разрешение матрицы. В двух матрицах с абсолютно одинаковыми параметрами, за исключением числа пикселей, светочувствительность матрицы с высоким разрешением окажется меньше, чем у матрицы с низким разрешением. Это связано с тем, что эффективная светочувствительная площадь с ростом количества пикселей уменьшается за счет увеличения площади "мертвых зон" между пикселями с ростом их числа соответственно

Когда речь заходит о реальном разрешении камеры, важно понимать высокое влияние объектива на эту характеристику. Камера может оснащаться видеосенсором с любым количеством мегапикселей и объективом, предназначенным для 1 Мпкс сенсора. В этом случае реальное разрешение видео не превысит 1 Мпкс.
На видеосенсор с высоким разрешением будет приходить размытая картинка с объектива, не приспособленного для съемки с высокой детализацией

Результаты теста

Все камеры показали сравнимое значение максимального горизонтального разрешения при максимальной освещенности, и это значение практически не зависит от конкретного фокусного расстояния моторизованного объектива. А вот уменьшение освещенности приводит к заметному уменьшению реального разрешения камер.

Камеры имеют достаточно широкие диапазоны регулирования углов обзора, причем время изменения угла обзора от минимального до максимального значения будет практически незаметно при эксплуатации камеры в реальных условиях.

Заметные преимущества

Все камеры показали хорошее разрешение во всех режимах, превосходящее результат моделей 2 Мпкс. Применение камеры с разрешением выше FullHD действительно позволит получить существенное увеличение детализации картинки. А ведь стоимость моделей 4 Мпкс уже сравнима с ценой некоторых камер 2 Мпкс. Однако за увеличение разрешения закономерно придется платить увеличением битрейта и глубиной архива, необходимого для хранения. Не стоит забывать, что технологии видеонаблюдения развиваются и при появлении новых алгоритмов сжатия видео проблема хранения становится менее критичной. Поэтому для конкретного проекта выбор между камерами 2 Мпкс и 4 Мпкс уже не столь очевиден, а в ближайшем будущем мультимегапиксельные модели получат еще большее распространение. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Что должен знать продавец систем видеонаблюдения и как от этого выигрывает заказчик

Алена Швецова
Независимый эксперт
(#cctvMadonna)

Продавец (английские эквиваленты Seller, Salesperson) – это человек, который за соответствующее вознаграждение от имени компании/организации продает клиентам товары или услуги. С целью убрать устоявшуюся коннотацию слова "продавец" из сферы торговли потребительскими товарами в современном бизнесе системной интеграции человека, отвечающего за продажи, называют "менеджер по продажам". Продажи в сфере ИТ, инженерной инфраструктуры и систем безопасности способствуют прогрессу и распространению новых технологий среди конечных заказчиков и в конечном итоге – внедрению Индустрии 4.0 (четвертой промышленной революции)

Высший пилотаж продаж в сфере систем безопасности – это способность менеджера продавать комплексные или интегрированные решения. Один комплексный проект может включать в себя:

- систему видеонаблюдения с видеоаналитикой;
- систему контроля и управления доступом;
- охранную сигнализацию;
- систему охраны периметра;
- системы пожарной безопасности и противопожарной защиты;
- ИТ-инфраструктуру и т.д.

Для продавца это "входной билет" в сложные и крупные проекты, а значит самые престижные и значимые перспективы для компании и новые возможности для своего карьерного роста. Теме компетенций такого менеджера по продажам и посвящена данная статья.

Бизнес-пары в продажах систем безопасности

Позиция человека, отвечающего за продажи систем видеонаблюдения (СВН) и систем безопасности (СБ), называется "Менеджер по продажам систем безопасности" (Security Systems Sales Manager). Сотрудник, руководящий продавцами, может работать на должности "Начальник отдела продаж" (Head of Sales Department). А тот, кто отвечает за развитие бизнеса и финансовый результат продаж, может называться "Директор по продажам" (Sales Director), "Коммерческий директор" (Commercial Director), "Директор по развитию бизнеса" (Business Development Director) и т.д.

Бизнес-парой у конечного заказчика являются менеджер по закупкам/снабжению/логистике, начальник отдела закупок, финансовый директор, директор по логистике и закупкам и т.д.

Задачи участников бизнес-пары совершенно противоположные. Задача менеджера по продажам – наиболее выгодная продажа СБ конечному заказчику (критерий успеха – маржа). Задача менеджера по закупкам конечного заказчика – наиболее выгодная покупка (критерий – самая низкая цена, снижение первичной балансовой стоимости приобретенных товаров и получение максимальной гарантии на комплексное решение).

Залогом успеха при выполнении этих важных задач для обоих менеджеров является их техническая компетенция и соответствующая финансовая квалификация для принятия объективного решения.

Рождение менеджера по продажам систем безопасности

Внимательно посмотрев на специальности, которые формирует сфера среднего специального и высшего образования в странах СНГ, оказывается, что в технических вузах не учат продавать, а в коммерческих вузах не учат необходимым техническим знаниям в области систем безопасности. Следовательно, ни государственные, ни коммерческие организации не могут получить сразу готового и компетентного менеджера по продажам.

Если изучить требования многочисленных вакансий "менеджер по продажам систем безопасности", то работодатели хотели бы видеть специалиста с рынка систем безопасности или ИТ с минимальным опытом работы 1–3 года, владеющего навыками успешных переговоров, знаниями MS Office, грамотной устной и письменной речью, коммуникабельностью, нацеленностью на результат, способностью к самостоятельным решениям, желанием развиваться, а также обязательным выполнением плана продаж.

Между желаемым идеальным кандидатом и реальностью после окончания вузов – пропасть. Поэтому путь менеджера по продажам СБ в системной интеграции начинается, как правило, еще на старших курсах вузов с совмещения учебы и работы, например на позиции помощника менеджера по продажам, проектировщика, инженера или монтажника. В результате:

1. Опыт работы помощником менеджера по продажам СБ дает быстрое понимание экономической составляющей продажи, поскольку продажа – это грамотно оформленные финансовые и юридические документы; заказчики, важные заказчики, договоры, документы, деловые письма, встречи, переговоры, счета, акты, сроки, поставка оборудования, себестоимость, маржа, дистрибьюторы, вендоры, форс-мажор, штрафные санкции, претензии, гарантия на работы и услуги, инженеры, проектировщики, монтажники, руководство и т.д.
2. Опыт работы инженером-проектировщиком СБ дает важную теоретическую базу для продаж, так как грамотное проектирование – фундамент будущего проекта и его продажи: нормативные документы, правила, паспорта, документация, спецификация оборудования и материалов, задания смежным организациям, авторский надзор и т.д.
3. Опыт работы инженером СБ дает важную теоретическую и практическую техническую базу для продаж, поскольку проданное техническое решение должно быть умным и работать на 100%: паспорта, руководства по настройке

и эксплуатации, документация вендоров, проектировщики, спецификация оборудования, сертификационное обучение, пусконаладка, пилотный проект, тестовая и опытная эксплуатация и т.д.

4. Опыт работы монтажником СБ дает важную практическую техническую базу для продаж, потому что грамотный монтаж – лицо системного интегратора: проектная документация, проектировщики, кабельный журнал, наряд-допуск, охрана труда, нормо-часы, акт приема-передачи оборудования, акт выполненных работ, провода и кабели, аксессуары, заземление, молниезащита, дорогое оборудование, паспорта на оборудование, материальная ответственность и т.д.

Помощник менеджера знает, как документально и финансово выглядит продажа. Инженер знает, какое оборудование и материалы нужны, чтобы продать решение и/или чтобы проданное решение заработало. Монтажник знает, сколько сил, времени и сверхурочных потребует реализация той или иной продажи. Этот совершенно разный первичный опыт менеджера по продажам СБ определяет его компетенции, карьерные возможности, успех в продажах проектов и долгосрочные отношения с заказчиками.

Эволюция менеджера по продажам СБ

На встрече с представителем заказчика опытному менеджеру по продажам СБ достаточно двух минут общения, чтобы понять, кто перед ним (технарь, ИТ-специалист, маркетолог или финансист) и как нужно построить эффективные коммуникации, чтобы переговоры завершились успешно и был сделан следующий конструктивный шаг в продажах – договор на консалтинг, аудит, проектирование, создание комплексного решения или сервисное обслуживание. От стратегии переговоров, подготовки и компетенций менеджера по продажам СБ зависит очень многое. Он выступает в роли хорошего "доктора", который внимательно слушает "пациента". Да, конечно, очень важно "подтвердить диагноз", сделать "анализы" и собрать "симпозиум" из коллег, но умение слышать заказчика на встречах и конструктивно вести коммуникации практически сразу определяет успех будущей продажи.

Чтобы вести с заказчиком переговоры на любом уровне, менеджер по продажам СБ должен:

- уметь создавать и проводить презентации;
- доносить преимущества своей компании и ценности предлагаемых брендов;
- пользоваться профессиональной терминологией;
- владеть знаниями по системам безопасности;
- обладать грамотной устной и письменной речью;
- уметь общаться с заказчиком на одном языке;
- уметь объяснять сложные понятия и профессиональные термины простыми словами.

Для этого менеджеру по продажам СБ необходимо пройти соответствующие тренинги по следующим темам:

- навыки эффективной презентации;
- B2B- и B2C-продажи;
- управление временем;

Рис. 1. SWOT-анализ

- личная эффективность;
- успешные переговоры;
- управление проектами и т.д.

Свою главную задачу при продаже комплексных проектов менеджер решает с привлечением команды профильных специалистов своей компании (руководители проектов, проектировщики, пресейлы, инженеры, отдел внедрения, логисты и т.д.), взаимодействуя с командой специалистов заказчика самых различных уровней (технические работники, финансовые подразделения, отдел закупок и т.д.).

Этапы продажи комплексных проектов по системам безопасности

В крупных компаниях-интеграторах работу менеджеров по продажам СБ всегда координируют руководители отделов/департаментов продаж. Как правило, менеджеры по продажам СБ сфокусированы на определенной вертикали рынка, например государственных заказчиках, промышленности, ритейле, банках и т.д. Знания специфики, проблематики и нормативных требований в конкретной отрасли делают менеджера более эффективным. Часто опытный менеджер по продажам СБ является одновременно и проектным менеджером, который ведет заказчиков и координирует проекты.

Стратегию продаж руководитель отдела/департамента СБ всегда начинает с создания бизнес-плана, в основу которого часто ложатся результаты SWOT-анализа. SWOT-анализ – это метод стратегического планирования, включающий в себя анализ внутренних и внешних факторов, влияющих на деятельность компании (в частности, на направление систем безопасности) по четырем критериям:

1) Strengths (сильные стороны);
2) Weaknesses (слабые стороны);
3) Opportunities (возможности);
4) Threats (угрозы).

От каждого менеджера по продажам СБ требуют аккаунт-план (Account Plan) – это документ, где описаны потенциальные заказчики и конкуренты, работающие с этими заказчиками. Из аккаунт-плана по итогам коммуникации появляются перспективные заказчики, или лиды (Leads), с которыми начинается работа по проектам. Далее следует самый важный этап подготовки к продаже – создание воронки продаж (Sales Pipeline, или Sales Tunnel) – перечень проектов, сформированных по запросам от заказчиков.

Задача менеджера по продажам СБ – строить коммуникацию с заказчиками и управлять своей проектной командой таким образом, чтобы постоянно увеличивать вероятность

Рис. 2. Пример воронки продаж комплексных проектов по СБ

Переговоры с заказчиком определяют успех будущих продаж

продажи с момента возникновения запроса. Это делается с помощью презентации возможностей, оценки бюджета, проведения пилотного проекта или технической демонстрации решения, проектирования, подачи коммерческого предложения, прохождения тендерных процедур до момента заключения договора, получения предоплаты и размещения заказов, а также полного закрытия сделки и подписания актов выполненных работ по проекту. Вовлеченность менеджера по продажам СБ будет существенно меняться, если интегратор участвует в проекте частично (например, проектная документация уже создана или тендер уже объявлен).

Соотношение количества проданных проектов по отношению к общему числу просчитанных проектов и поданных коммерческих предложений называется конверсией и выражается в процентах. К примеру, конверсия 10% по системам распознавания лиц означает, что из 100 просчитанных проектов было продано 10 проектов (а 90 проектов отработано "в корзину").

Для системного интегратора нормальным показателем конверсии в год является параметр 20–30%, хорошим – 40–50%. Каждый руководитель департамента продаж в компании-интеграторе знает средний показатель конверсии и методом обратного расчета может оценить, насколько эффективно работает менеджер, пополняя воронку продаж за интересующий период (обычно – квартал). Конверсия проектов является объективным показателем персональной эффективности менеджера по продажам и оценкой его компетенций в умении управлять продажами.

Менеджеры по продажам СБ "живут" кварталами. Ежеквартальный анализ проектов в работе называется Pipeline Review (проверка состояния воронки продаж), а список проектов с вероятностью более 60% – Forecast (прогноз продаж). Чем больше проектов попадает в Forecast в будущий период, тем выше вероятность выполнения плана продаж в этот период.

Цикл продажи систем безопасности в комплексных проектах

Полный цикл продажи комплексного проекта – это время от первого контакта менеджера по продажам СБ и запроса на проект (появление проекта в воронке продаж) до момента полного выполнения интегратором условий договора, сдачи проекта и подписания актов выполненных работ. Циклом продаж также могут называть время от момента появления проекта в воронке продаж до момента заключения договора.

Независимо от формы собственности объекта заказчика единицей финансового изменения времени является финансовый год и соответствующее годовое бюджетирование. Если у заказчика на текущий год выделен бюджет на покупку нового решения СБ или модернизацию существующего, у интегратора есть шанс сделать продажу в текущем году и цикл продажи может составить от полугода до 1 года. Если бюджет не выделен – цикл продажи составит не менее 1,5 лет.

Усредненные показатели полного цикла продажи крупных проектов по СБ для системной интеграции составляют 2–3 года, средних проектов – 1–1,5 года, мелких проектов – от нескольких месяцев до полугода. Все это время менеджер по продажам СБ будет вовлечен в процесс продажи, коммуникацию с заказчиком и сопровождение проекта.

Что должен знать менеджер по продажам систем видеонаблюдения и видеоаналитики

Деятельность менеджеров по продажам систем пожарной безопасности и охранной сигнализации за последние 10 лет практически не изменилась. Эти классические системы безопасности достаточно консервативны, их продажа, создание и внедрение находятся в жесткой правовой области со множеством норм и правил.

С появлением различных типов камер (аналоговые, IP, SD-HDI), кодеков записи (MJPEG, H.264, H.265), способов передачи видеосигнала (проводной, беспроводный), скоростей передачи видеоданных (100 Мбит/с, 1 Гбит/с, 10 Гбит/с), способов хранения видеоинформации (DVR, NVR, серверы, RAID, NAS и т.д.) и форматов экспорта видеоархива (avi, mkv и т.д.) требования к квалификации менеджеров по продажам систем видеонаблюдения за последние 10 лет, наоборот, стали более высокими. Помимо появления в странах СНГ четкой нормативной базы по СВН, приведенной к международным стандартам, данностью стали требования заказчиков о наличии в СВН интеллектуальных функций (распознавание автомобильных номеров, лиц и др.).

Поэтому эффективный и успешный менеджер по продажам современных СВН должен обладать компетенциями "три в одном": видеонаблюдение, ИТ и видеоаналитика.

Развитие бизнеса

С точки зрения развития бизнеса менеджер по продажам СВН в системном интеграторе обязательно должен знать историю, философию, ценности и достижения своей компании и при общении с заказчиком:

1) уметь демонстрировать преимущества своей компании;

2) представить свою команду, их компетенции и примеры успешно реализованных проектов;

3) объяснить разницу между брендами и OEM-брендами, преимущества брендов для заказчика[1];

4) показать ценность качества и философию предлагаемых брендов (в чем они выдающиеся, чем лучше конкурентов, что сделали для рынка видеонаблюдения, почему для бизнеса конкретного заказчика они подойдут лучше всего);

5) объяснить, что такое TCO (Total Cost of Ownership), или совокупная стоимость владения проектом, а также связь между первичной стоимостью проекта и эксплуатационными затратами;

6) объяснить, что такое ROI (Return On Investment) и как это работает в видеонаблюдении и видеоаналитике;

7) уметь объяснить разницу между гарантией 1 год, 3 года, 5 лет на оборудование от вендора (завода-изготовителя) и просто гарантией от интегратора/дистрибьютора/дилера;

8) показать, что ждет заказчика через 1 год после окончания гарантии на работы от интегратора и почему важен сервисный договор;

9) объяснить понятие "гарантия на работы или комплексное решение", зону ответственности и обязанности интегратора, а также его права (например, если на объекте нет заземления и вдруг сгорит сервер, то…);

10) показать, что ждет заказчика через 5 лет при выборе бюджетных решений, какова будет стоимость ремонта/замены, выезда специалистов и стоимость негарантийных работ.

При правильных коммуникациях с заказчиком и предоставлении ему полезной и объективной бизнес-информации менеджер по продажам СВН на старте отсекает конкурентов, работающих по принципу "купи – продай", стремящихся любой ценой (демпингом, акцентом на дешевизну и доступность) продать товар заказчику.

[1] *Швецова А. Вендор. Дистрибьютор. Интегратор. Третий лишний? // Системы безопасности. 2019. № 5. С. 52–53.*

Повышение конкурентоспособности

С точки зрения повышения конкурентоспособности своей компании менеджер по продажам СВН в системном интеграторе обязательно должен знать:

1) как оценить целесообразность/стоимость внедрения проекта на камерах разных видов (аналоговые, SD-HDI, IP);

2) как объяснить заказчику экономический смысл покупки IP-камер (правильное разрешение IP-камеры – экономия, неправильное – затраты);

3) как показать заказчику стоимость требований "время хранения архива должно быть не менее 30 дней", "скорость не менее "25 кадр/с" и других параметров (разрешение IP-камер, скорость записи, частота кадров, глубина хранения);

4) как объяснить заказчику, что самое дорогое, а что – самое дешевое в проекте СВН (IP-камеры, аксессуары, серверы, системы хранения данных, сети, рабочие станции, мониторы и т.д.);

5) как донести до заказчика, что выбор СВН – это не только выбор IP-камер;

6) как объяснить заказчику, что экономия на IP-камерах – это общепринятый миф, который удорожает, а не удешевляет TCO проекта (IP-камеры – это "глаза" проекта, а "слепые глаза" – это бесполезная система);

7) что такое параметр наработки на отказ, или MTBF (Mean Time Between Failures), и как он влияет на ROI проекта;

8) как объяснить заказчику, что СВН будет функционировать так, как будет работать ее "мозг" – программное обеспечение на оптимальной ИТ-инфраструктуре (оценка стоимости СВН по критерию стоимости программного обеспечения не имеет экономического смысла, это тоже общепринятый миф, который удорожает, а не удешевляет TCO проекта);

9) удельный вес и влияние ИТ-инфраструктуры (сеть, серверы, система хранения данных) на TCO проекта;

10) важность внедрения политик кибербезопасности как для существующей, так и для новой СВН (стоимость утечки данных от IP-камер, несанкционированного экспорта видео, отсутствия контроля за действиями администраторов и операторов);

11) как объяснить заказчику, почему важно начать проект с проекта (проектирования);

12) как продемонстрировать заказчику целесообразность и практический смысл аудита существующей СВН, если на систему уже закончилась гарантия или ее делал другой интегратор.

При правильных коммуникациях с заказчиком и предоставлении ему экономических фактов, основанных на технической экспертизе, менеджер по продажам СВН выделит свою компанию на фоне конкурентов (которые готовы сделать то и так, "как скажет заказчик", и не взять на себя ответственность, потому что "заказчик нам так сказал сделать"). Работоспособное решение и ответственность за результат – это важные составляющие репутации системного интегратора.

Уникальные преимущества компании

С точки зрения создания уникальных преимуществ своей компании менеджер по продажам СВН в системном интеграторе обязательно должен знать, какие истинные цели ставит перед собой заказчик, говоря о внедрении видеоаналитики, и уметь ему объяснить:

1) разницу в терминах "видеоаналитика на IP-камере" или "видеоаналитика на сервере";

2) реальные факты о видеоаналитике в ответ на популярные заблуждения и мифы;

3) сколько будет стоить требование "хотим расширить функционал существующей системы модулями видеоаналитики" при покупке новой системы или модернизации существующей;

5) что такое охранная видеоаналитика и бизнес-аналитика, на конкретных примерах;

6) что такое пригодность изображения для распознавания номеров автомобилей/лиц/подсчета посетителей и т.д.;

7) целесообразность и практический смысл аудита существующей СВН с целью будущего внедрения видеоаналитики;

8) целесообразность и преимущества проведения пилотного проекта по видеоаналитике[2].

При правильных коммуникациях с заказчиком, развенчании общепринятых мифов и проведении пилотных проектов менеджер по продажам СВН заметно выделит свою компанию среди конкурентов как авторитетного эксперта в области видеонаблюдения и видеоаналитики. Конструктивный диалог интегратора с заказчиком и позиция эксперта в отрасли – ключ к большим и многолетним проектам.

Менеджеры по продажам СВН и СБ должны обязательно пройти сертификационные обучения по тем вендорам и решениям, которые они будут продавать, и под руководством более опытных и мудрых наставников уметь трансформировать полученные технические знания в свои истинные профессиональные ценности и убеждения. Вера в то, что он/она продает, – важное профессиональное качество менеджера, создающее доверие к нему/ней, компании-интегратору, предлагаемым решениям и ведущее к продаже. Если менеджер не верит в то, что он/она продает, это всегда очень заметно и коллегам, и руководству, и заказчикам

Как от компетенций менеджера по продажам систем видеонаблюдения выигрывает заказчик

Развитие и внедрение Индустрии 4.0 в области систем безопасности ставит заказчика перед сложным выбором: сфокусироваться на составлении задания на проектирование/ТЗ, чтобы отдел закупок смог провести конкурс на проектирование/закупку и реализацию всего решения, или быть вовлеченным во весь проект от момента возникновения потребности и анализа существующих вариантов решений на рынке до предварительного бюджетирования и финальной подготовки технических требований для проведения тендера.

При правильных коммуникациях с заказчиком и предоставлении ему экономических фактов, основанных на технической экспертизе, менеджер по продажам СВН выделит свою компанию на фоне конкурентов (которые готовы сделать то и так, "как скажет заказчик", и не взять на себя ответственность, потому что "заказчик нам так сказал сделать"). Работоспособное решение и ответственность за результат – это важные составляющие репутации системного интегратора

Первый путь – это "звездный час" отдела закупок заказчика. Менеджеры по продажам СБ различных интеграторов в сжатые сроки с привлечением своих команд подготовят и подадут предложение на тендер, а менеджеры по закупкам выполнят свою бизнес-роль в выборе поставщика по критерию самой низкой цены. Этот процесс можно сравнить с покупкой личного автомобиля, например, вашими коллегами по выданным вами характеристикам с лимитированным финансовым бюджетом. Результат такой покупки может вас неприятно удивить.

Второй путь – это тяжелый труд команды специалистов как внутри компании заказчика, так и внутри компании-интегратора (интеграторов), так как заказчик практически никогда не прорабатывает проект только с одним интегратором. Этот процесс можно сравнить с созданием большого "корабля" (комплексной системы безопасности) с множеством "отсеков" (конкретных систем безопасности). Над каждым "отсеком" может работать своя команда, но при этом все "отсеки" должны быть правильно состыкованы и работать как единое целое. До финального "спуска на воду" необходимо провести все тесты и испытания, чтобы убедиться, что "корабль" будет соответствовать требуемым характеристикам. "Командиром" команды со стороны системного интегратора является менеджер по продажам СБ. Он знает, что должно быть построено, управляет и контролирует процесс, вдохновляет свою команду на новые свершения и все время сверяет с заказчиком ориентиры и параметры.

Выбор грамотного и компетентного командира со стороны системного интегратора, которым является менеджер по продажам СВН или СБ, определяет для заказчика возможность и успех реализации проекта по параметрам, помогающим ему развивать свой бизнес: критерий "цена/качество", инновации и лидерство в отрасли, снижение операционных затрат, возврат инвестиций и многие другие. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

[2] Швецова А. Как пилотный проект по видеонаблюдению поможет интегратору выиграть, а заказчику – получить работающее решение // Системы безопасности. 2019. № 6. С. 43–45.

Активисты в эпоху диджитализации

Часть 1. GDPR-террористы

Этой статьей автор начинает серию публикаций под общим названием "Активисты в эпоху диджитализации. Влияние и последствия для организаций". В них будут изложены имевшие место в период 2018–2020 гг. неизвестные факты из мировой и отечественной практики, подтверждающие существование организованных групп активных граждан и иллюстрирующие их деятельность в реальном и виртуальном пространстве, сопряженную с нанесением имиджевого, финансового и иного материального ущерба различных организациям

Алексей Плешков
Независимый эксперт
по информационной безопасности

GDPR-террористы. Какие ассоциации возникают, когда вы в первый раз проговариваете про себя это словосочетание? Евросоюз, комплаенс, опасность, фанатизм, а может быть – абсурд, шутка, игра слов. По мнению автора, каждая из этих ассоциаций по-своему верна.

Термин "GDPR-террорист" является второй производной от более мягкого "GDPR-активист", вошедшего в обиход граждан Евросоюза (далее – ЕС) после вступления в силу в 2018 г. регламентирующих документов под общим названием General Data Protection Regulation (далее – GDPR).

"GDPR-активист" – это термин, обозначающий члена организованной группы лиц, критически настроенной против обработчиков персональных данных, работающих на территории ЕС, действия которых субъективно нарушают, и это подтверждено активистами документально, основные требования GDPR, в том числе права и свободы граждан ЕС – владельцев персональных данных (в терминах GDPR). При этом, до вмешательства активистов, со стороны регуляторов и правоохранительных органов в отношении нарушителей GDPR не было предпринято должных мер воздействия или юридического преследования.

Суждение о нарушении обработчиками GDPR носит сугубо экспертный характер, на первом досудебном этапе оно ничем не подтверждено. Однако GDPR-активисты не стесняются

General Data Protection Regulation (генеральный регламент по защите персональных данных) – серия директив (регламент (EU) 2016/679, директива (EU) 2016/680), введенных в действие 25 мая 2018 г. на всей территории Евросоюза. Целями GDPR являются:

- **защита персональных данных граждан ЕС в любом виде и в любом объеме;**
- **защита прав и свобод граждан ЕС в защите их данных;**
- **ограничение перемещения персональных данных в рамках ЕС.**

После введения в действие GDPR усиливает существующие и вводит новые права для граждан ЕС, а также дает им инструменты контроля над своими личными данными (обрабатываемыми в любом виде), а именно:

- **легкий доступ к их данным, включая предоставление обработчиками подробной информации о том, как именно и где обрабатываются эти данные;**
- **право на переносимость данных: применение формализованных правил передачи персональных данных граждан ЕС между поставщиками услуг;**
- **право на удаление персональных данных: если гражданин ЕС больше не хочет, чтобы его персональные данные обрабатывались и у обработчика нет законных оснований для хранения и дальнейшей обработки персональных данных гражданина ЕС, то данные должны быть незамедлительно отовсюду удалены;**
- **право знать, если данные гражданина ЕС были несанкционированно скомпрометированы: компаниям и организациям придется незамедлительно информировать граждан ЕС – владельцев персональных данных в случае нарушения информационной безопасности их данных, по факту инцидента они (обработчики) также обязаны в кратчайшие сроки уведомить соответствующий орган в ЕС по надзору за защитой персональных данных и выполнению требований GDPR.**

Кроме того, GDPR предоставляет гражданам ЕС рабочие инструменты для реализации своих прав, упрощая механизмы обращения в надзорные органы, например жалобы в электронном виде и пр.

Под действия GDPR попадает полностью или частично автоматизированная обработка физическими или юридическими лицами, государственными органами и другими институтами и организациями персональных данных граждан ЕС на территории ЕС и за его пределами. Любая некоммерческая деятельность (в том числе безвозмездное оказание услуг гражданам ЕС), связанная с обработкой персональных данных, также попадает под действие ст. 2 и 3 GDPR, который имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим персональных данные граждан ЕС, независимо от страны нахождения такой компании

Персональные данные в терминах GDPR

Персональные данные – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъекту данных), по которой прямо или косвенно можно его определить. К такой информации относятся в том числе фамилия, имя, отчество субъекта, данные его фактического местоположения, онлайн-идентификаторы, технические реквизиты и параметры сессии, один или несколько факторов и параметров, характеризующих генетическую, культурную, религиозную, социальную идентичность субъекта данных. При таком подходе даже MAC-адрес сетевого адаптера мобильного устройства и динамический IP-адрес ноутбука могут быть признаны персональными данными субъекта

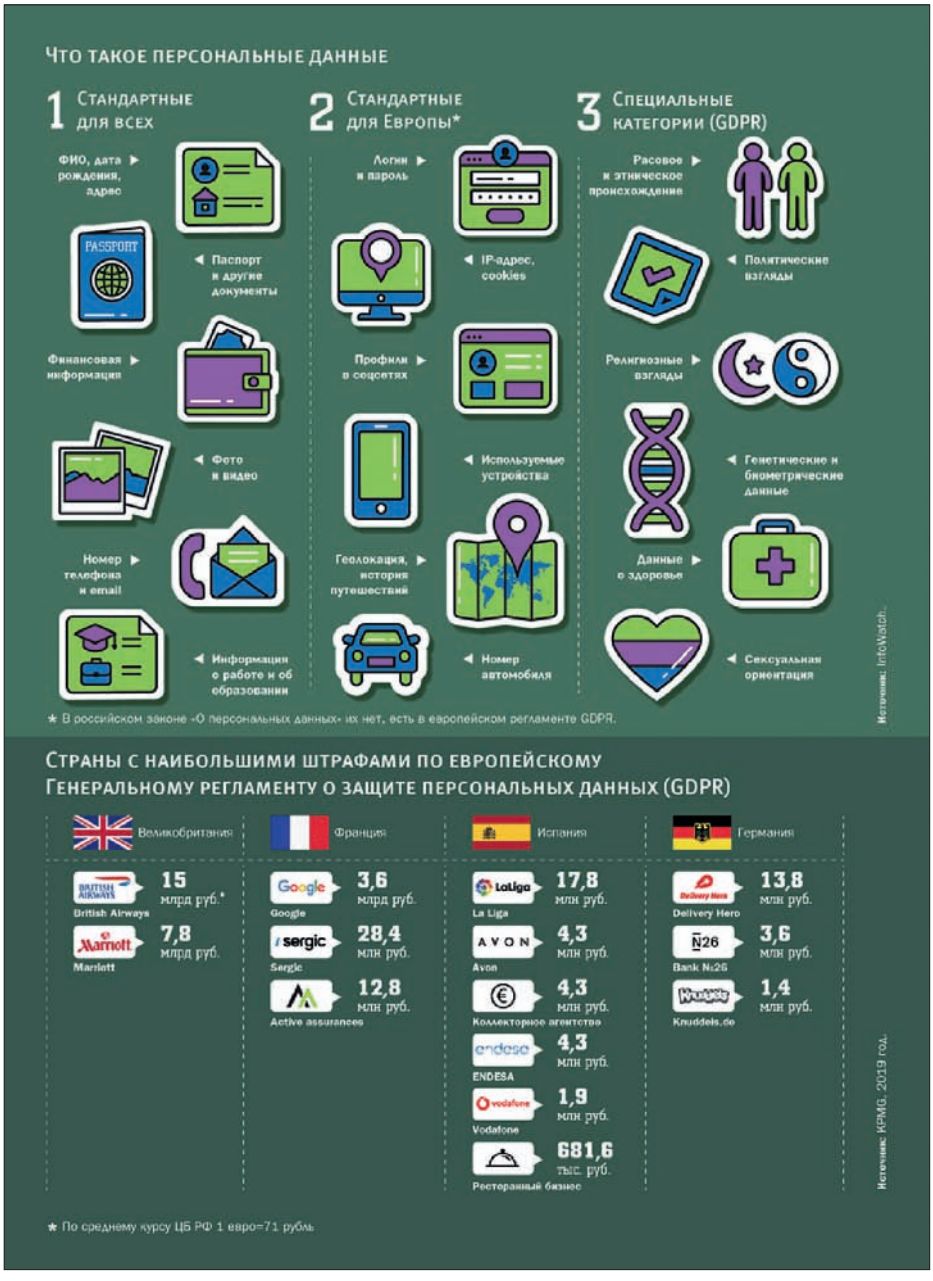
Согласно первому обзору Европейского Совета по защите данных (European Data Protection Board, EDPB) по реализации GDPR, с момента вступления в силу данного регламента надзорными органами в 31 стране ЕС за первые девять месяцев было зарегистрировано 206 326 нарушений.

По статистике европейских регуляторов, в 2019 г. общая сумма штрафов, собранная с нарушителей требований регламента GDPR, составила более 405 млн евро.

Топ-5 штрафов за нарушение GDPR в 2019 г.:

- **British Airways – 204,6 млн евро;**
- **Marriott International – 110,3 млн евро;**
- **Google LLC – 50 млн евро;**
- **Austrian Post – 18 млн евро;**
- **Deutsche Wohnen SE – 14,5 млн евро.**

В контексте деятельности GDPR-активистов интересен кейс № 3 с Google LLC. В январе 2019 г. GDPR-активист из Франции обратился к представителям уполномоченного по GDPR французского надзорного органа (Commission nationale de l'informatique et des libertés, CNIL) с заявлением о массовых нарушениях правил прозрачности (в том числе отсутствии достаточных правовых оснований), допущенных Google при демонстрации целевой рекламы для граждан ЕС – пользователей Android. В результате длительного расследования компания Google признала нарушение и была оштрафована на огромную сумму



в публичном выражении своей позиции в Интернете, на стихийных пикетах и митингах, в европейских печатных СМИ. Некоторые размещают обращения об имевших место нарушениях в открытом доступе на YouTube-каналах и закрытых telegram-сообществах, другие по запросу демонстрируют текстовые и видеоматериалы, доказывающие факты нарушений. Работают GDPR-активисты слаженно и последовательно, юридически грамотно и выверенно формулируя свои претензии к третьим лицам. Многие имеют высшее техническое или юридическое образование и богатый опыт взаимодействия с европейскими регуляторами. Назвать их любителями или непрофессионалами своего дела нельзя. Поэтому и ущерб от их деятельности для юридических лиц, резидентов и нерезидентов ЕС, можно измерить миллионами евро.

В отличие от активистов, GDPR-террористы действуют более радикально, используют все доступные методы и средства информационной войны для достижения своих не всегда однозначно прослеживаемых целей. Ведь деятельность террористов не обязательно направлена на физическое устранение кого-либо. Иногда достаточно любыми средствами, но вовремя убрать крупную фигуру из сложной политической партии, чтобы нанести непоправимый вред государству и его гражданам в будущем.

Деятельность GDPR-террористов

Если погрузиться в тему GDPR глубже, то можно обнаружить, что для контроля за соблюдением GDPR практически в каждой стране – члене ЕС официально созданы и укомплектованы штатом, оборудованием и бюджетом национальные надзорные органы. Для них разработаны, локализованы и внедрены нормативно распорядительные документы, а также методики проведения проверок выполнения требований GDPR. Однако, по мнению GDPR-активистов, институт GDPR в Европе по состоянию на конец 2019 г. работает недостаточно эффективно в части систематического выявления нарушений и привлечения юридических лиц к справедливой ответственности. А формальные санкции и штрафы размером 20 млн евро или 4% от годового оборота нарушителя лишь слегка ограничивают крупные компании, такие как Google, Amazon или Facebook, и не гарантируют соблюдение прав и свобод граждан ЕС в цифровом пространстве Интернет. В этой ситуации единственным вариантом действий для GDPR-активистов становится противостояние (открытое или скрытое) активных граждан ЕС выявленным и доказанным нарушениям.

Открытое противостояние выражается в подготовке и написании в различные инстанции ЕС обращений с информацией об имевших место в компаниях массовых нарушениях. За два года GDPR-регуляторам поступило более полумиллиона таких обращений. К примеру, для открытого противостояния с нарушителями GDPR одним из основателей движения GDPR-активистов в Европе Максом Шремпсом создан некоммерческий проект Not Your Business

(NOYB, в переводе с английского "Не твое дело"). Подробнее об этом проекте чуть-чуть дальше.

Скрытое противостояние нарушителям (и здесь в полной мере мы видим нарушение требований по защите конфиденциальной информации в организациях) заключается в поиске и подкупе источников внутри организации – потенциального нарушителя GDPR, которые добудут и предоставят необходимые в качестве доказательства материалы по формату/запросу активистов или представителей регуляторов. При реализации подобных сценариев подтвержденные действия инсайдеров фактически являются нарушением внутренних политик конфиденциальности компании и могут повлечь за собой юридические последствия, вплоть до судебного преследования.

К примеру, в списке выше топ-5 штрафов за нарушение GDPR в 2019 г. в позиции № 4 упоминается прецедент с австрийской почтовой компанией Österreichische Post AG. В октябре 2019 г. австрийская коммерческая компания Austrian Post получила штраф за нарушение GDPR в части несанкционированного профилирования своих клиентов. Сотрудники почты много лет создавали в автоматизированной системе класса CRM профили своих клиентов, содержащие ФИО, информацию об адресах, личных предпочтениях в печатных изданиях, в том числе комментарии по политической принадлежности клиентов. Суммарно база содержала более 3 млн записей по клиентам. Затем эти данные были проанализированы и в определенный момент проданы почтой в различные политические партии Австрии и коммерческим компаниям. Указанные действия Austrian Post были классифицированы австрийским регулятором как нарушение ст. 5 и 6 GDPR. Интересен тот факт, что первичную информацию о нарушении GDPR, которая легла в основу расследования, регулятор получил из анонимного источника, близкого к Osterreichische Post AG, в разгар очередной политической битвы в Австрии.

Принципы работы GDPR-активистов

Разберем отдельные активности GDPR-террористов на примере некоммерческой организации NOYB. Официально зарегистрированные в Австрии как юридическое лицо ID#1354838270, они ни от кого не скрываются. Информация о NOYB доступна на сайте местного регистратора http://zvr.bmi.gv.at/. Основываясь на материалах сайта https://noyb.eu, можно самостоятельно сделать вывод о схеме работы и основных принципах, лежащих в основе деятельности подобных организаций. Хештеги, звучащие как лозунги на демонстрациях, недвусмысленно дают понять, чем руководствуются GDPR-активисты в своей деятельности.

#MakePrivacyReal
Воплотим в реальности требования европейского законодательства по защите персональных данных
#StrategicandEffectiveEnforcement
Добьемся эффективного правоприменения к нарушителям GDPR
#CollaborativeEffort
Совместно с другими группами активистов достигнем синергетического эффекта в борьбе
#CrucialMoment
С принятием GDPR в ЕС наступил переломный момент, наступила эра конфиденциальности
#ExperiencedTeam&Members
Представляем собой опытную команду экспертов-единомышленников с компетенциями в различных областях
#FocusonCommercialPrivacy
Сфокусируем свою деятельность на нарушениях конфиденциальности крупными корпорациями
#EuropeanScopeGlobalImpact
Правоприменение GDPR в ЕС в конечном итоге повысит уровень конфиденциальности персональных данных во всем мире
#SupportingBusiness
Поддержим европейские компании, которые готовы, хотят и соблюдают GDPR, защитим их от недобросовестной конкуренции со стороны крупных корпораций – нарушителей GDPR
#InvestInPrivacy
Готовы к сотрудничеству с людьми, которые ценят право неприкосновенности своих персональных данных, своей частной жизни и собственного выбора

Таким образом, не только европейские компании сталкиваются с деятельностью GDPR-активистов. Экстерриториальность GDPR открывает перед желающими возможность воздействовать прямо или косвенно практически на любую компанию, в деятельности которой на территории ЕС GDPR-активисты усмотрели нарушения своих прав.

А как с GDPR-активистами в России?

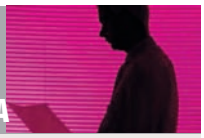
По состоянию на февраль 2020 г. автору неизвестно о существовании/регистрации в российском юридическом пространстве организаций, подобных по своей сути и направлению деятельности проекту NOYB. Возможно, что они уже кем-то созданы, но пока не вышли на такой уровень публичности, чтобы открыто заявить о своих успехах в борьбе с нарушителями GDPR в России.

Начиная с 2018 г. в открытых источниках и СМИ достаточно регулярно появляются комментарии и публикации на тему присутствующих в деятельности крупных российских компаний нарушений отдельных статей GDPR. В 2018 г. ВКонтакте (ВК) столкнулся с проблемой, связанной с политикой конфиденциальности: белорусский активист Кристиан Шинкевич, постоянно проживающий на территории Польши, официально и публично со ссылкой на нормы GDPR запросил у российского проекта ВК предоставить ему все касающиеся его персональные данные, которые он ранее разместил на своей странице или страницах своих друзей в ВК. ВК недостаточно детально, по мнению активиста, удовлетворил данное требование, предоставив не всю информацию. В то же время ВК нашел причину, чтобы приостановить доступ активиста к его ВК-странице. Полученный от ВК ответ лег в основу статей и публикаций в Интернет, вызвал множество споров и побочных ветвей для обсуждения.

Но отсутствие реальных прецедентов из правозащитной практики GDPR-террористов в России ни в коем разе не подтверждает пассивность отечественных активистов в вопросах соблюдения конфиденциальности персональных данных. Федеральные законы, такие как 152-ФЗ, и подзаконные акты предоставляют широкое юридическое поле для деятельности. К примеру, 13 февраля 2020 г. мировой судья судебного участка № 374 Таганского района г. Москвы, рассмотрев на открытом судебном заседании материалы дела № 5-168/2020 об административном правонарушении в отношении иностранного юридического лица Facebook, Ink. и материалы дела № 5-167/2020 об административном правонарушении в отношении иностранного юридического лица Twitter Inc., постановила: признать обе иностранные компании виновными в совершении административного правонарушения, предусмотренного ч. 8 ст. 13.11 Кодекса РФ об административных правонарушениях, и назначить наказание каждой из компаний в виде штрафа в размере 4 млн рублей. Как и в случае с Austrian Post, базой для проведенного регулятором расследования (в данном случае – Роскомнадзором) послужили материалы, опубликованные в открытом доступе пользователями сети Интернет с активной жизненной позицией. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

КОЛОНКА ЭКСПЕРТА



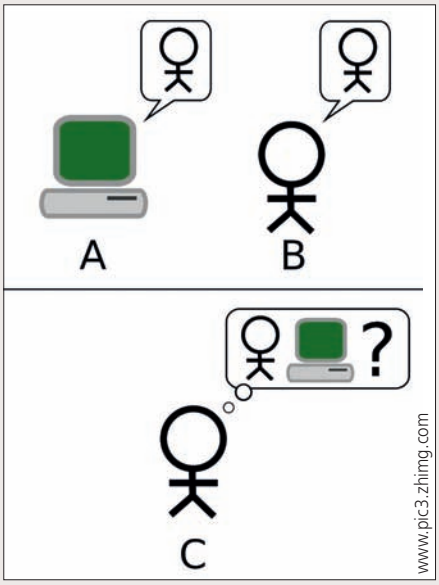
О RobBee, Meema и эпохе эмоционального искусственного интеллекта

В первые месяцы нового года произошло множество событий, достойных внимания

В предыдущем номере мы говорили о возрастающем влиянии государства на регулирование технологий и влиянии технологий на жизнь общества в целом. И вот 15 января президент России Владимир Владимирович Путин в послании Федеральному Собранию предложил сделать бесплатным доступ к основным государственным и социально значимым ресурсам. Если его предложения будут реализованы, то Россия станет первой страной в мире, где доступ к основным информационным ресурсам всем гражданам будет гарантирован законом. К сожалению, этот революционное событие еще не осознано обществом и незаслуженно находится в тени.

Бухгалтер RobBee может заменить 120 сотрудников

Интересную новость сообщила компания "Билайн" о результатах внедрения робота-бухгалтера RobBee: компания сократила расходы на 50 млн рублей, робот перевыполнил план на 40% и окупился менее чем за год. RobBee взял на себя проверку более 90% кассовых документов, снизил трудоемкость в четыре раза и увеличил скорость работы на 30% без найма дополнительных сотрудников. Планируется, что скоро RobBee научится создавать закупочные документы и будет выполнять работу, сопоставимую с работой 120 сотрудников. Как мы видим, внедрение систем искусственного интеллекта идет полным ходом, в том числе и у нас в стране, и уже приносит первые значимые результаты.



Стандартная интерпретация теста Тьюринга

Робот-бухгалтер может заменить 120 сотрудников

Тест Тьюринга – эмпирический тест, идея которого была предложена Аланом Тьюрингом в статье "Вычислительные машины и разум", опубликованной в 1950 г. в философском журнале Mind.
Тьюринг занимался проблемой машинного интеллекта по меньшей мере с 1941 г. и к моменту публикации статьи уже на протяжении многих лет рассматривал возможность создания искусственного интеллекта

Становится все сложнее распознать, кто разговаривает с вами – человек или бот

Исследования не прекращаются. Google представила нового чат-бота Meena, который поддерживает беседу очень похоже на человека. Чат-бот может разговаривать на разные темы, при этом сохраняет контекст разговора в течение всего диалога. Но чтобы что-то оценить, нужно вначале оцифровать результат, и для этого Google разработала новую метрику "Средняя осознанность и конкретность" (Sensibleness and Specificity Average), которая позволяет определить, насколько осознанным и конкретным был ответ. Так, средний человек по этой метрике получил 86%, а Meena получил 79%. То есть сейчас уже практически нельзя распознать, кто вам отвечает в чате – человек или бот. Ближайшие конкуренты, боты Mitsuku и Cleverbot, набирают по этой метрике всего 56%. Чтобы добиться столь впечатляющих результатов, компания использовала нейросеть с более 2,6 млрд параметров, для ее обучения было загружено более 341 Гбайт текстовых данных (1 Гбайт текстовых данных – это примерно около тысячи книг, то есть небольшая районная библиотека) и построены связи между 40 млрд комбинаций слов. Сеть тренировалась в течение 30 дней на суперкомпьютере с 2048 ядрами.

Человечность ИИ все ближе

В 2014 г. компьютером впервые был пройден тест Тьюринга, когда соответствующая программа, отвечая на вопросы, смогла убедить судей, что она является 13-летним мальчиком из Одессы. Прошло всего пять лет, и уже ответы человека и чат-бота при беседе становятся неразличимы. Это гигантский прогресс, который позволяет приблизить эпоху эмоционального искусственного интеллекта, создавать чат-боты психологической поддержки, делать роботов, специализирующихся на продажах, полноценных персональных ассистентов и многое другое. Например, при достаточном количестве звуковых записей голоса и подключении чат-бота можно создавать имитацию разговора с близким человеком, которого уже нет с нами... ■

Алексей Коржебин
Директор по продукту AggreGate Edge компании Tibbo Systems

Видеонаблюдение и AI: тенденции развития

Системы видеонаблюдения сегодня являются основным технологическим инструментом обеспечения безопасности, при этом задачи безопасности уже не единственная функция камер видеонаблюдения. С развитием вычислительных мощностей непосредственно железа и интеллектуальных возможностей программной составляющей на рынке растет спрос на многофункциональность и интеллект

Дамир Алиуллов
Pre-sale инженер
Hikvision Russia

Аналитика и искусственный интеллект в системах безопасности, в частности в сегменте видеонаблюдения, изначально разрабатывались для того, чтобы научить устройства реагировать на определенные события и тем самым оптимизировать работу оператора-человека

По оценкам аналитиков IHS Markit, к 2021 г. во всем мире будет установлено около 1 млрд устройств для мониторинга и видеосъемки (для сравнения: на конец 2019 г. их количество оценивалось в 770 млн). Такой массив камер и данных, которые они генерируют, требует эффективного управления и точного анализа для быстрого решения возникающих вопросов.

Аналитика и искусственный интеллект в системах безопасности, в частности в сегменте видеонаблюдения, изначально разрабатывались для того, чтобы научить устройства реагировать на определенные события и тем самым оптимизировать работу оператора-человека. Начиналось все с примитивного анализа кадра для детекции движения, фактов пересечения виртуальной линии, контроля входа/выхода, выявление оставленных или исчезнувших предметов. С появлением нейросетевых технологий на базе глубокого обучения (Deep Learning) возможности стандартного видеонаблюдения существенно расширились, и сегодня многофункциональные системы можно встретить в ритейле, транспортном сегменте, медицине, финансовом секторе и т.д., где камеры не только следят за безопасностью объектов и людей, но и решают задачи сбора и анализа статистических данных, анализа маркетинговых активностей, управления транспортными потоками и многие другие.

Расширяя границы безопасности...

Стоит отметить, что до настоящего момента большинство камер видеонаблюдения, работающих с AI-алгоритмами, могли использовать небольшое количество интеллектуальных функций (часто не более одной-двух) из-за ограничений в производительности процессора. То есть за один сеанс камера способна работать только с одной сложной интеллектуальной функцией, например распознать человека или номер автомобиля. Совершенствование компонентов железа и рост производительности процессоров обеспечивает увеличение вычислительных мощностей AI-видеокамер, поэтому на рынке постепенно будет появляться все большее количество устройств, способных выполнять несколько интеллектуальных задач одновременно.

Таким образом, рынок постепенно приходит к тому, что традиционная Security (безопасность) трансформируется в Smart Security (умная безопасность) и далее – в Business Intelligence (бизнес-аналитика и автоматизация бизнес-процессов). Обеспечить растущие запросы клиентов в сегментах Smart Security и Business Intelligence возможно только с помощью развитых AI-алгоритмов. Популярность таких решений, даже несмотря на их довольно высокую стоимость, будет расти, так как грамотно выстроенные AI-алгоритмы в устройствах создают дополнительную ценность для оборудования и в целом повышают инвестиционную привлекательность проектов на базе интеллектуальных решений.

Как следствие, на рынке ожидается настоящий бум: станет увеличиваться не только количество аналитических продуктов, но и компаний-разработчиков, задача которых будет заключаться в удовлетворении растущего спроса. Согласно оценкам аналитического агентства MarketsandMarkets, мировой рынок видеоаналитики в среднем растет на 21,5% ежегодно. Главным драйвером сегмента традиционно выступают специализированные интеллектуальные решения для обеспечения безопасности (в том числе в рамках проектов Safe City и Smart City): распознавание лиц и эмоций, автомобильных номеров, модели, цвета и типа транспортного средства, анализ потоков людей и транспорта, детекция опасных предметов, прогнозирование различных ситуаций и т.д. Растет также количество кейсов внедрения промышленной аналитики: контроль соблюдения техники безопасности на производственных и промышленных предприятиях и объектах (наличие каски, защитных костюмов и т.д.), контроль опасных зон, мониторинг потенциально опасных факторов, которые могут повлиять на работу предприятия, и прогнозирование нежелательных событий (например, мониторинг уровня подземных вод в шахтах).

...И не только

Как уже было отмечено ранее, обеспечение безопасности – далеко не единственная задача, которую заказчик возлагает на системы видеонаблюдения, особенно в коммерческом сегменте. Законодателем мод в этом случае выступает бизнес и его запросы, например проведение маркетингового анализа, сбор статистических данных, анализ целевой аудитории и ее интересов, составление тепловых карт, работа с таргетированной рекламой и т.д. Этот сегмент особенно важен для рынка видеонаблюдения и AI-решений с точки зрения повышения эффективности бизнеса.

Цифровизация и стремительное развитие технологий напрямую влияют на отношения продавца/поставщика и потребителя. В эру Интернета и повсеместной информатизации клиент четко осознает, какие задачи ему необходимо решить с помощью той или иной технологии,

Традиционная Security трансформируется в Smart Security и далее – в Business Intelligence. Обеспечить растущие запросы клиентов в сегментах Smart Security и Business Intelligence возможно только с помощью развитых AI-алгоритмов. Популярность таких решений будет расти, так как грамотно выстроенные AI-алгоритмы в устройствах создают дополнительную ценность для оборудования и в целом повышают инвестиционную привлекательность проектов на базе интеллектуальных решений

приобретаемых товаров и услуг. Как результат – растут потребительские ожидания. Интеллектуальная видеоаналитика с этой точки зрения выступает незаменимым инструментом для развития бизнеса и работы с клиентом, анализа его поведения, выявления ожиданий и предпочтений. Яркий пример – персонифицированный маркетинг, когда под конкретного клиента подбирается лучшее для него предложение, с учетом индивидуальных потребностей. База для такого маркетинга создается с помощью AI-алгоритмов и развитой нейросетевой аналитики.

На борту и за бортом

Существенное влияние на развитие систем видеонаблюдения оказывает видеоаналитика на борту камеры. Главным преимуществом такого решения является децентрализация системы и снижение нагрузки на ядро системы (сервер). В этом случае камера не зависит от главного сервера и его удаленности, пропускной способности сети и перебоев в работе каналов связи. Современный уровень развития встроенных аналитических модулей позволяет эффективно обрабатывать явления, которые требуют быстрого реагирования оператора. На борт камеры можно вынести фиксацию автомобильных номеров в проектах управления парковками, маркетинговую аналитику (подсчет посетителей, поведенческая аналитика, контроль очереди и т.д.), фиксацию тревог на удаленных объектах, где не требуется постоянное видеонаблюдение. В последние годы набирает популярность пожарная видеоаналитика на базе тепловизионных модулей – в интеллектуальных тепловизорах и двухспектральных камерах видеонаблюдения. С их помощью можно измерять температуру людей, предметов, выделенных зон, фиксировать появление огня или дыма, отправлять тревожные сигналы ответственному оператору и запускать противопожарные системы.

Бортовая аналитика позволяет высвободить мощности сервера для более значительных задач, связанных с анализом Big Data, для работы с базами, а самое главное – для развития самообучающихся AI-алгоритмов.

Кроме видеофайлов и информации об инцидентах современная система видеонаблюдения накапливает огромные объемы метаданных, которые также можно анализировать с помощью AI-технологий. Чем больше таких данных проходит через алгоритм, тем больше он накапливает статистики и полезной информации, на их основе и происходит обучение алгоритма. Это позволяет повышать уровень достоверности идентификации событий и распознавания объектов, прогнозирования явлений. В конечном счете повышается надежность всей системы.

Прогулка в облаках

Говоря об искусственном интеллекте и видеонаблюдении, невозможно не упомянуть облака и облачные сервисы. Развитие Интернета вещей (IoT) повлекло за собой стремительный рост количества подключаемых устройств, в том числе и устройств безопасности, которые стали неотъемлемой частью IoT. На этом фоне переход в облако также выступает одним из ключевых трендов всей индустрии безопасности. Облака дают большие преимущества частным пользователям, малому и среднему бизнесу с точки зрения эффективности работы систем видеонаблюдения, их гибкости и рентабельности. "Видеонаблюдение как сервис" (VSaaS) особенно привлекает эти группы пользователей своей простотой эксплуатации, поскольку им не нужно устанавливать локальный сервер, проводить сложную настройку оборудования на объекте. Гибкие системы тарифов, которые предлагают операторы облачных сервисов, позволяют пользователям оптимально распределять расходы в течение всего срока действия контракта, оплачивать только актуальные и необходимые услуги.

Широкие возможности облачных технологий привлекают и крупных заказчиков из корпоративных сегментов. Системные интеграторы используют корпоративные облака для построения развитой информационной инфраструктуры. На ее базе возможно создать распределенную систему безопасности, что упрощает подключение большого количества камер к центральному серверу и их администрирование с назначением прав доступа к отдельным ресурсам для каждого конкретного пользователя. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА ЭКСПЕРТА

Аналог мертв, да здравствует аналог!

Технологии, в частности IoT, все усложняются, ширится область их применения. Приставку "смарт" скоро можно будет добавлять к каждому предмету в квартире или офисе: их становится больше, они становятся доступнее. Но становятся ли они понятнее? Да, молодым людям, которые зачастую не знают многих исторических фактов, но все могут моментально загуглить, достаточно просто во всем разобраться. Но что делать поколению людей с кнопочными телефонами? Как разобраться и использовать интернет-технологии без Интернета?

На ум приходят устройства с аналоговыми интерфейсами – простые и большие панели, где у каждой кнопки есть четкое предназначение, которое на этой кнопке крупно написано. Ведь история развивается циклично и вполне может быть, что на данном этапе технологиям нужно сделать небольшой виток и уйти от сенсорных экранов (Touch Screen) к более простым и понятным физическим интерфейсам, в которых разберется человек не только 20+, но и 60+.

Сенсорные мониторы в автомобилях отвлекают от проезжей части

Простой пример эволюции технологий, которая ухудшила потребительские свойства товара, – сенсорные мониторы в автомобилях. Ранее можно было, не отрывая глаз от дороги, на ощупь найти любую нужную кнопку, сейчас же от проезжей части придется отвлечься: вызвать на Touch Screen меню, подменю, несколько секунд всматриваться в экран. А ведь эти секунды могут быть роковыми...

Поэтому давайте вместе отвлечемся от цифрового мышления и пропустим через призму аналогового восприятия все новинки в области безопасности и IoT, чтобы понять, как на самом деле человеку удобнее и эффективнее с ними взаимодействовать. Вдруг мы откроем новые горизонты синергии аналогового восприятия человека и цифровых технологий в век беспроводного Интернета?!

Евгений Ерошин
Директор по маркетингу
ООО "БайтЭрг"

КОЛОНКА РЕДАКТОРА

Востребовано рынком

Внимательный читатель заметил, что название нашего раздела изменилось и теперь звучит как "Видеонаблюдение и видеоаналитика". Видеоаналитика – наиболее перспективный, динамичный раздел видеонаблюдения. Рынком особенно востребованы такие инструменты, как системы распознавания образов, определения разнообразных тревожных ситуаций, ряд бизнес-приложений для ритейла, складов и производств.

Большое влияние на развитие видеоаналитики оказывают маркетологи всех мастей. Именно в этой области производитель может выделиться, придумав свой собственный "детектор чего-то", чтобы отличаться от конкурентов.

Инструменты видеоаналитики призваны автоматизировать процесс принятия решений и заменить оператора видеонаблюдения. Некоторые программные модули уже сейчас выполняют свою работу лучше и быстрее человека. Примером могут служить системы распознавания номеров автомобилей, несущихся по многополосному ночному шоссе. На горе нарушителям автоматизация в данном случае зашла очень далеко. Можно сколько угодно сокрушаться по поводу засилья камер на дорогах, но приходится признать, что именно благодаря им мы в целом стали ездить аккуратнее и меньше нарушаем правила дорожного движения.

Большую помощь службам безопасности ритейла оказывают системы распознавания лиц. Особенно эффективно они работают в тандеме с базой данных нежелательных лиц. Очень удобны умные алгоритмы поиска событий в архивах. Пока еще ждут своего звездного часа разнообразные детекторы драк и других правонарушений.

Действительно, любую тревожную ситуацию можно алгоритмизировать, дело лишь в вычислительной мощности процессоров и в мастерстве программистов. Судя по всему, лет через двадцать профессия оператора видеонаблюдения уйдет в прошлое, будучи вытесненной электронным искусственным интеллектом.

Более того, алгоритмы распознавания, разработанные специалистами видеонаблюдения, могут быть востребованы в областях, далеких от безопасности, например в беспилотных автомобилях.

Михаил Арсентьев
Редактор раздела "Видеонаблюдение", коммерческий директор ООО "Артсек"

Независимый рейтинг видеокамер по бренду, разрешению и форм-фактору

Представляем набор рейтингов, диаграмм и статистик, который показывает популярность разных брендов камер видеонаблюдения, камер различного разрешения, а также других показателей, относящихся к этому рынку. Рейтинги составляются на основе обезличенных статистических данных, собранных программным обеспечением IP Video System Design Tool для планирования и проектирования систем видеонаблюдения, которым в течение последних 12 месяцев пользовались более 50 тыс. установщиков и проектировщиков

Максим Шумейко
Генеральный директор компании IPICA Software

Анастасия Хорина
Ведущий специалист по работе с клиентами компании IPICA Software

Объем выборки, представленной в статье для построения мировых рейтингов и статистики по разрешающей способности камер и типам камер, превышает 65 тыс. записей. По основным регионам доли записей распределились следующим образом:

- Западная Европа – 18,2%;
- США – 16,6%;
- Россия – 6,1%.

Позиция в рейтинге отражает данные о популярности брендов камер в самой программе для проектирования систем видеонаблюдения, а не рыночную долю брендов камер видеонаблюдения или лучшую марку

Первый набор диаграмм (рис. 1) иллюстрирует рейтинг производителей за 2019 г. в мире, России и Западной Европе, который основан на процентном соотношении камер, добавляемых в проекты видеонаблюдения в программе. Второй (рис. 2) отражает популярность камер различных разрешений в разных регионах. Диаграмма третьего блока (рис. 3) отображает статистику использования камер различных типов.

Обзор брендов

К концу 2019 г. мировые лидеры зафиксировались на своих позициях (рис. 1). Основные изменения начинаются уже во второй половине списка (двойные стрелки отображают изменение позиции производителя более чем на два пункта к концу 2019 г. по сравнению с II и III кварталами 2019 г.).

Как видно из инфографики, лидирующие позиции в мировом рейтинге занимает Hikvision. В России за счет популярной линейки камер HiWatch совместная доля Hikvision и HiWatch на рынке все еще примерно в два раза выше, чем в среднем по миру, хотя этот процент начинает снижаться. При этом доля камер примерно одинакова: на HiWatch приходятся 17,7% от выбранных камер, на Hikvision – 20,3%.

По сравнению с II и III кварталами, в которых было заметно тяготение отечественных установщиков к бюджетным камерам, к концу 2019 г. ситуация немного изменилась. AXIS, находящийся на лидирующих позициях в Западной Европе, Северной Америке и общемировом рейтинге, по итогам года поднялся на 6-е место с 10-го по итогам II и III кварталов.

Выделим производителя Dahua, который занял 3-е место в общемировом рейтинге и вошел в первую пятерку по всем регионам.

Компания Hanwha Techwin, производящая камеры под брендом Wisenet, сохраняет 7-е место в России и весьма популярна на мировом рынке, не опускаясь ниже 4-го места в Западной Европе и Северной Америке.

Из собранной статистики заметна склонность российских установщиков к выбору отечественных брендов. Так, в первой двадцатке находятся DSSL (DSSL, ActiveCam, Trassir), Optimus, RVi, Beward, Satvision, BOLID, IPTRONIC, Polyvision и LTV.

В общемировом рейтинге заметно соревнование китайских (Hikvision, Dahua, Uniview) и западных (AXIS, BOSCH, Honeywell, Mobotix) производителей. Стоит отметить, что на 7-м месте в миром рейтинге находится популярный в Бразилии бренд Intelbras.

Мир

№		Бренд	Рейтинг
1	=	Hikvision	21,8
2	=	Axis	11,8
3	=	Dahua	11,1
4	=	Hanwha Techwin	9,1
5	=	Bosch	4,6
6	=	IDIS	2,7
7	=	Intelbras	2,5
8	=	Uniview	2,3
9	=	Avigilon	1,6
10	=	Vivotek *	1,5
11	▲	Honeywell	1,4
12	▲	Mobotix	1,3
13	▼	Sony	1,2
14	▼	Panasonic	1,1
15	▲	Ivideon (Nobelic)	1,0
16	▲	FLIR	0,9

Россия

№		Бренд	Рейтинг
1	=	Hikvision+HiWatch	38,0
2	=	Dahua	9,6
3	=	DSSL	6,0
4	▲	Optimus	3,3
5	▼	RVi	3,2
6	▲	Axis	3,1
7	=	Hanwha Techwin	2,9
8	▲	Beward	2,8
9	▲	Uniview	2,2
10	▼	Satvision	2,1

Западная Европа

№		Бренд	Рейтинг
1	=	Axis	19,5
2	=	Hikvision	14,8
3	=	Hanwha Techwin	11,2
4	=	Dahua	7,7
5	=	Bosch	7,7
6	=	Mobotix	3,4
7	▲	Vivotek *	2,5
8	▼	Interlogix	2,4
9	▼	IDIS	2,1
10	▼	Santec	1,7

* Рейтинг камер Vivotek может быть выше, так как в представленной инфографике используется статистика только основного ПО и не включены данные по использованию камер в OEM-версии ПО для Vivotek

Рис. 1. Рейтинг брендов камер в 2019 г.

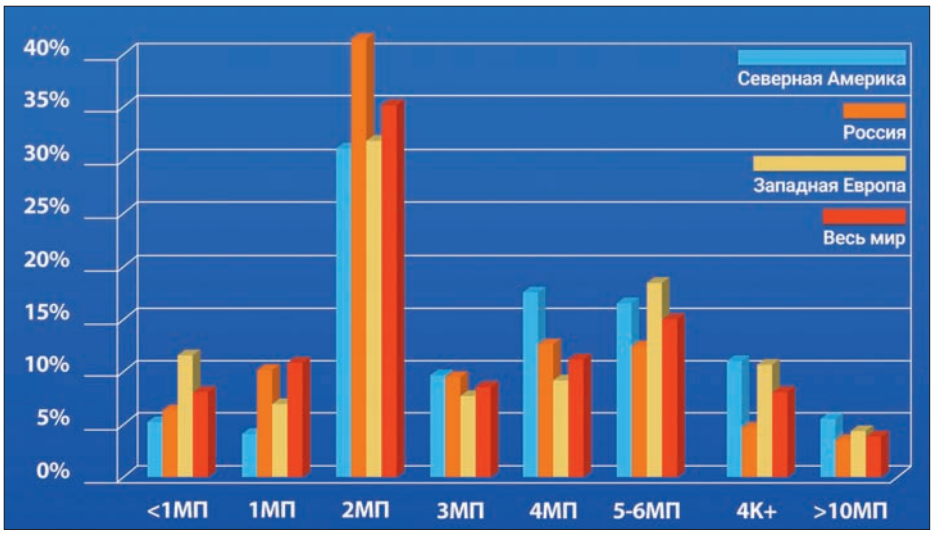


Рис. 2. Рейтинг использования камер различного разрешения в 2019 г.

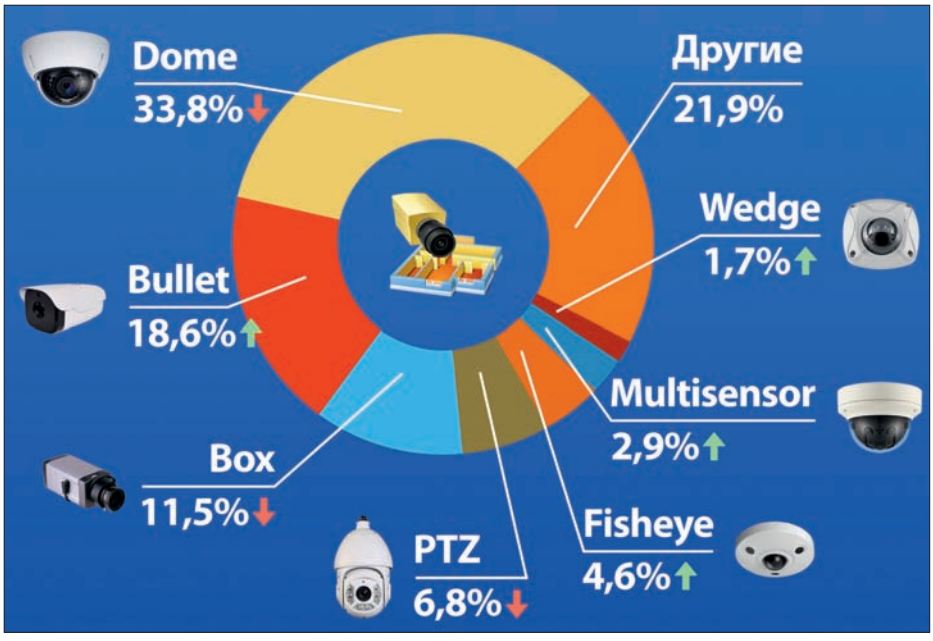


Рис. 3. Рейтинг типов камер в 2019 г.

В США и Западной Европе четверка лидеров одинакова: AXIS, Hikvision, Hanwha, Dahua. Китайский бренд к концу 2019 г. занял 4-е место в США, вытеснив Arecont Vision.

Рейтинг камер разного разрешения

Следующим параметром аналитики стали популярные разрешения камер видеонаблюдения (рис. 2). К концу 2019 г. повсеместно лидирующую позицию все еще сохраняют камеры с разрешением 2 Мпкс. 35% выбранных камер имели такое разрешение, а это каждая третья камера видеонаблюдения из добавленных в проекты в программе. В России доля камер 2 Мпкс составляет около 40%, а к концу 2019 г. заметен рост использования камер от 5 Мпкс и выше (в среднем на 0,5%).

По внедрению 2- и 3-мегапиксельных камер в 2019 г. Россия обходит Западную Европу и среднемировой уровень. Но процент камер с разрешением выше 5 Мпкс пока еще сильно ниже среднемирового.

Заметный процент камер с разрешающей способностью менее 1 Мпкс в Западной Европе и в общемировом рейтинге можно объяснить распространением камер-тепловизоров с низким разрешением.

В Северной Америке наблюдается стабильный прирост в использовании камер с разрешением выше 4K (примерно на 17,5%), что отличает данный регион от всех остальных.

Статистика по типам применяемых камер

Анализ использования камер видеонаблюдения разных типов (рис. 3) показывает плавное снижение популярности купольных (Dome), наклонно-поворотных (PTZ) камер и формата Box. При этом наблюдается рост внедрений малогабаритных Bullet- и Wedge-камер и камер типа Fisheye (с объективом "рыбий глаз"). Увеличивается популярность довольно дорогих мультисенсорных камер, что говорит о смене вектора развития рынка видеонаблюдения. Современные проектировщики либо отдают предпочтение лаконичному и простому дизайну с использованием Bullet-камер, либо постепенно начинают пользоваться функциональными устройствами с большим количеством возможностей.

Возможные погрешности

Точность рейтинга в значительной степени зависит от того, какое количество пользователей установило вышеуказанное программное обеспечение в конкретном регионе. На результаты также может влиять разный уровень популярности программы проектирования среди пользователей отдельных брендов и опубликованные пресс-релизы об интеграции камер в программу.

Статистика собирается только тогда, когда пользователь выбирает опцию "Отправить анонимную статистику использования" при установке программы или соглашается участвовать в программе повышения качества.

Рейтинг формируется с апреля 2019 г. и обновляется ежеквартально. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

КТОТАМ 112 – уникальная система пропуска спецтранспорта на придомовую территорию

Появление возможности ограничения доступа на придомовую территорию предоставило жильцам новые удобства и существенно повысило безопасность на всем огороженном участке. Простейший забор и калитка со шлагбаумом и цифровым замком – уже "серьезная" система контроля доступа. Но обратной стороной этого нововведения стало заметное увеличение времени прибытия на вызов экстренных служб. Теперь человека, ожидающего помощь, отделяет от специалиста еще большее количество устройств и закрытых проходов. Частично проблему сглаживает повсеместное распространение видеокамер и умных домофонов. Но несмотря на это, специальным службам все еще приходится ожидать открытия проезда

Доступ во дворы, оборудованные шлагбаумами, в лучшем случае осуществляется через операторов, в подъезды – через консьержей или компанию, предоставляющую домофонные услуги. А такой режим взаимодействия затрачивает драгоценные минуты сотрудников служб специализированной помощи. В этих условиях важной задачей, для которой пока еще не было разработано полноценного решения, становится обеспечение автоматического доступа экстренных служб на придомовую территорию.

Проблемы физических ключей доступа

При использовании физических ключей сотрудники экстренных служб могут их потерять или скопировать. Кроме того, для их полноценного использования требуется применение дополнительного оборудования, что ведет к соответствующим затратам.

Есть вариант с установкой радиометок на спецтранспорте, но и это сделает систему еще дороже и сложнее в эксплуатации.

В то же время использование мобильного устройства не требует установки дополнительного оборудования и позволяет связать аккаунт в приложении с конкретным пользователем и смартфоном. И компания BEWARD успешно решила эту задачу.

Уникальная разработка BEWARD

В кратчайшие сроки была разработана уникальная система – платформа KtoTam 112, позволяющая автоматически управлять устройствами ограничения доступа и предоставлять "зеленый коридор" для экстренных служб.

Пилотный проект уже реализован в самом обычном дворе. Это абсолютно типичный современный двор, оборудованный шлагбаумом на въезде и координатно-матричным домофоном на каждом подъезде. Существующая инфраструктура подверглась серьезным аппаратно-программным усовершенствованиям, а жильцы по-прежнему пользуются всеми возможностями старой системы, но с уже значительно большим функционалом.

При помощи оборудования BEWARD шлагбаум и домофоны были оснащены устройствами видеонаблюдения и подключены к цифровой системе, которая уже интегрирована с ЦОД и может быть легко внедрена во всю систему "Безопасный город". Масштабируемость решения позволяет применять его и в более крупных проектах.

Удобный сервис для специальных служб

Сотрудники спецслужб получили доступ к эффективному решению через приложение KtoTam 112, которое можно установить на любое мобильное устройство на платформе Android или iOS. Программное обеспечение обладает удобным и понятным интерфейсом. Все необходимые действия осуществляются в едином окне – автоматически или в один клик.

Система позволяет через приложение открыть нужный шлагбаум, находящийся в заданном радиусе от спецтранпорта

При приближении спецтранспорта система автоматически открывает ему шлагбаум

В процессе работы приложения координаты транспортного средства определяются на смартфоне со спутника. На карте на экране устройства в радиусе действия отображаются все доступные для открытия шлагбаумы. При приближении автомобиля они автоматически активируются и открывают проезд. Шлагбаум может быть открыт и в ручном режиме.

Доступ к возможностям приложения предоставляет администратор системы и только персоналу, которому он необходим для выполнения служебных обязанностей. Возможности создать аналог мастер-ключа просто нет.

На самом шлагбауме устанавливается антивандальная видеовызывная панель, позволяющая связаться с диспетчером, если есть какие-то проблемы со смартфоном, например разрядился аккумулятор или пропала связь с GPS. Диспетчер по видеотрансляции в режиме реального времени примет решение об открытии шлагбаума.

Модернизация затронула и старые домофоны в подъездах. После входа сотрудников специальных служб во двор домофоны, подключенные к цифровой системе, открываются автоматически при их приближении. Они могут быть открыты в ручном режиме из приложения или осуществлять видеовызов диспетчера.

Антивандальная панель, установленная на шлагбаум, с круглосуточной видеофиксацией и прямой связью с оператором

Платформа KtoTam

KtoTam 112 – это дополнительная часть более крупной системы KtoTam, разработанной компанией BEWARD. Платформа KtoTam предназначена для повышения удобства жильцов и предоставления новых функциональных бизнес-возможностей жилищным компаниям.

Новые базовые функции для жильцов:

- применение мобильного устройства вместо координатно-матричной трубки;
- запись и просмотр архива вызовов посетителей;
- переадресация вызова на любой телефон и управление доступом;
- просмотр полного видеоархива с домофона;
- онлайн-видео по запросу;
- автоответчик;
- открытие двери по распознаванию лица;
- администрирование списка номеров автомобилей для открытия шлагбаума на въезде во двор;
- предоставление разового временного гостевого пропуска для номера автомобиля;
- добавление и редактирование ключей RFID;
- добавление и редактирование индивидуального пароля на вход;
- СМС-оповещение по событию (посетитель, открытие ключом, распознавание и т.д.);
- журналирование событий.

Новые функциональные возможности для жилищных компаний и провайдеров услуг:

- монетизация коммунальных услуг и расширение методов мониторинга;
- монетизация услуг сверх базового функционала (в виде набора тарифных планов либо добавления и оплаты услуг по отдельности);
- предоставление услуг муниципалитету в системе "Безопасный город";
- предоставление услуг МЧС. ■

Системы видеонаблюдения. Итоги десятилетия

Часть 1

Десятилетие – это достаточно большой период времени для такой высокотехнологичной отрасли, как системы видеонаблюдения, тем более в обстановке все ускоряющегося технического прогресса. Особенно это относится к области ИТ и общей цифровизации, непосредственно примыкающей к сегменту систем безопасности и видеонаблюдения

Николай Чура
Технический консультант
компании "Фирма "Видеоскан"

За 10 лет существенно изменились как предлагаемое оборудование, так и участники рынка. Усилилась монополизация среди производителей, поставщиков и инсталляторов. Как ни странно, в нашей стране монополизация произошла и среди потребителей, постоянно вымывая частный сегмент личного потребления, индивидуального и малого бизнеса. На рынок вышли крупные ИТ-компании и мобильные операторы, а крупные концерны и банковские структуры становятся квазипроизводителями, определяющими направление технической политики.

Аналоговое и IP-видеонаблюдение в начале десятилетия

В начале десятилетия основная масса оборудования в российском сегменте рынка была аналоговой, на основе стандартного телевидения (4:3, 576 строк, PAL). Вместе с тем уже предлагались IP-системы с разрешением до FullHD, однако стоимость подобных камер и систем регистрации значительно превышала цену на аналоговые образцы. Кроме того, чувствительность применяемых CMOS-сенсоров, тем более для форматов HD и FullHD, в те времена была намного ниже аналоговых CCD. Некоторые производители тогда применяли в IP-камерах типовые чересстрочные CCD, что сохраняло привычную потребителю чувствительность. Но это лишало возможности ожидаемого роста разрешения и создавало проблему интерлейсинга при демонстрации. Такие решения были особенно характерны для видеокамер известных тайваньских и южнокорейских брендов, еще находящихся почти полностью в аналоговом сегменте.

IP-наблюдение как основной тренд

За прошедшее десятилетие IP-системы стали приоритетным направлением в видеонаблюдении. Кроме того, ИТ-решения открыли широкие возможности построения протяженных интегрированных систем безопасности. Кроме наблюдения и регистрации изображений, в них теперь включаются функции контроля доступа, учета рабочего времени, аналитики перемещения людей, товаров и транспортных средств и их идентификации. Домофонные системы сейчас также строятся по технологии IP и входят в общую систему безопасности здания, микрорайона, а иногда и города. Сюда же подключаются и модули инженерного оборудования, создавая единую систему Интернета вещей IoT.

Видеонаблюдение как услуга

Развитие облачных сервисов создало новое направление индивидуального и корпоративного наблюдения с использованием технологии VSaaS – видеонаблюдения как услуги. Это позволяет вообще не закупать оборудование, а ограничиться арендой или покупкой только видеокамер, осуществляя видеоконтроль и просмотр архива на собственном смартфоне. На рис. 1 показаны примеры подобных "бытовых" IP-видеокамер. Как ни странно, подобная технология стала востребованной и для очень больших систем безопасности (например, города или крупной корпорации), когда более оптимально использовать услуги профессиональной организации с ее системой видеонаблюдения.

Комплекты "домашнее наблюдение в чемодане"

Укрупнение поставщиков и инсталляторов создало потребность в небольших законченных комплектах оборудования для "домашнего наблюдения в чемодане", ориентированных на конечного частного потребителя. Пример подобного комплекта показан на рис. 2. Сейчас это обычно аналоговые HD-камеры с гибридным регистратором и просмотром на смартфоне потребителя.

Технологии распознавания

За прошедшее десятилетие были хорошо отработаны технологии распознавания регистрационных номеров, а затем и человеческих лиц. Сейчас они широко применяются в крупных городах и на автомагистралях.

Для эффективного использования этих технологий необходимо только качественное изображение при любых погодных условиях. Естественно, для регистрации обстановки на автомагистралях и автомобильных номеров применяются специализированные камеры, зачастую с импульсной ИК-подсветкой.

Стали популярными телевизионные методы контроля скоростного режима. Правда, подобный способ регистрации "мгновенной" скорости в точке измерения сильно зависит от пространственного положения камеры. Эта методика чревата большими ошибками, иногда умышленными, что подтверждает огромное количество жалоб.

Новое назначение камер

За годы появились камеры и оборудование с новым назначением и конструктивом, например:

- носимые "нательные" камеры с непосредственной или удаленной регистрацией для работников безопасности и охраны порядка (на рис. 3 представлен образец подобного изделия);
- огромный сегмент автомобильных видеорегистраторов, которые не относятся напрямую к видеонаблюдению, однако в каком-то смысле служат безопасности;
- специализированные системы наблюдения с автономной или удаленной регистрацией для общественного транспорта, включая железные дороги. Чаще всего эти камеры имеют повышенную вандалозащищенность и встроенную ИК-подсветку. Для таких моделей, как правило, применяется конструкция "глазное яблоко", представленная на рис. 4;
- видеосистемы для контроля кассовых операций, охраны и учета посетителей в ритейле и т.п.

Появились и стали довольно популярными панорамные камеры с объективами "рыбий глаз" или панаморфной оптикой. Они позволяют одной камерой вести наблюдение довольно обширных пространств, перекрестных проходов и т.д. при размещении ее на потолке и визировании сверху вниз.

В наружных камерах, особенно в поворотных вариантах (PTZ), стали использовать лазерную подсветку и подсветку с согласованным с кадром полем и переменным углом.

И наконец, все чаще стали предлагаться тепловизионные камеры или даже гибридные варианты на их основе. Особенно приятно, что в основном это модели с рабочим диапазоном

Рис. 1. IP-видеокамера для домашнего наблюдения

подъездный домофон

домофон на площадке

IP PORTAL
DK103M
BEWARD

интернет

одноквартирная вызывная панель

многоквартирная вызывная панель

поддержка

доступные опции

www.beward.ru

Рис. 2. Комплект видеонаблюдения для самостоятельной установки

Рис. 3. "Нательная" видеокамера

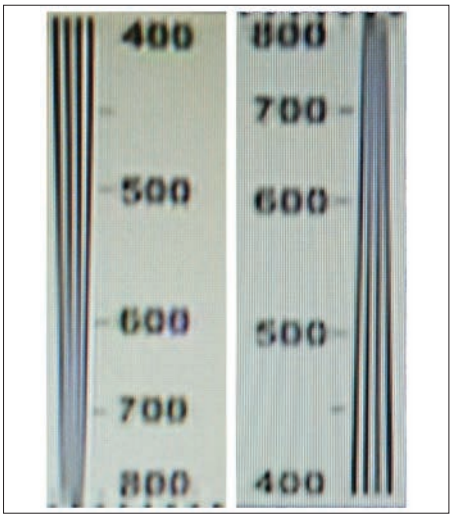


Рис. 5. Горизонтальное разрешение видеокамеры 960H

8–13 мкм, максимально отвечающим реальному температурному "рельефу" окружающего ландшафта. Применение детекторов на основе неохлаждаемых микроболометров на оксиде ванадия и неохлаждаемых термических объективов, а также увеличение выпуска этих приборов несколько снизили цены на подобную технику.

Параметры, определяющие успех видеонаблюдения

Очевидно, что важнейшие характеристики, определяющие качество изображения, получаемое системой наблюдения, – это разрешение и чувствительность видеокамеры. Используемый чересстрочный телевизионный стандарт (PAL или NTSC) к тому времени сильно ограничивал рост качественных характеристик наблюдения. Это противоречие требовало своего разрешения.

Формат 960H: маркетинг или "заря новой жизни"?

На рубеже десятилетий компания SONY, практически основной разработчик и производитель видеосенсоров, предложила "улучшенный" телевизионный формат с повышенным горизонтальным разрешением 960H. Для оцифровки и обработки видеосигнала с расширенным спектром были представлены три видеопроцессора семейства Effio – S, E, и P. Они имели различную функциональность и возможности. Через короткое время появились и специальные регистраторы, обеспечивающие запись изображения с повышенным горизонтальным разрешением 960H (960x576 пкс). Объективные измерения разрешения по телевизионной таблице однозначно подтверждали лучшее горизонтальное разрешение типового значения. Результат этих измерений показан на рис. 5. Однако это безусловное достижение совершенно не улучшило общее качество картинки в сравнении с типовым разрешением (720x576 пкс).

Теперь эту многолетнюю маркетингово-технологическую операцию по увеличению стоимости оборудования можно рассматривать по-разному. Но в итоге нам в наследство остался именно этот формат (960x576 пкс) в качестве базового стандартного аналогового изображения.

Рис. 4. Видеокамера с ИК-подсветкой – "глазное яблоко"

Наблюдение по принципу "пиксель в пиксель"

Потребность серьезно улучшить качество изображения, без перехода в сегмент IP-наблюдения с пакетной передачей, привела к появлению нового формата HD-SDI, предложенного альянсом HDcctv во главе с Тоддом Рокоффом.

Этот формат базировался на типовом интерфейсе, используемом в профессиональном телевидении. Он обеспечивает последовательную цифровую передачу несжатых изображений 720p (1280x720 пкс) и 1080p (1920x1080 пкс) по принципу "пиксель в пиксель". Пожалуй, это самый качественный принцип передачи изображений для видеонаблюдения.

Основными "знаменами", под которыми шло внедрение этого формата, были:

- простота эксплуатации, аналогичная типовой аналоговой системе;
- потенциальная возможность применения существующей коаксиальной структуры при модернизации системы наблюдения;
- привычные методы монтажа системы и методики наблюдения операторов.

К сожалению, эти факторы оказались не столь значительными, чтобы компенсировать относительно высокую стоимость оборудования, серьезные требования к качеству коаксиальной линии и даже соединительных элементов. Видимо, надежды на применение существующей кабельной сети систем наблюдения основывались на предположении практически повсеместного использования в нашей стране кабелей RG-59. Но воображение заканчивалось на кабелях класса КВТ-2 и ШГЭС. Кроме того, дальность передачи сигнала HD-SDI даже для качественных линий RG-59 и RG-6 не превышала 100–150 м.

Другими словами, предложенный формат, несмотря на исключительное качество передачи несжатого изображения, не нашел широкого применения.

Развитие систем HD-SDI

В середине десятилетия было предпринято несколько попыток реанимировать это направление. Почти одновременно с появлением аналоговых HD-форматов был предложен цифровой формат EX-SDI, или HD-VLC. В нем скорость последовательного видеопотока SDI в 1,5 Гбит/с снижалась до 270 Мбит/с. Это увеличивало дальность передачи до 400–500 м. Однако, судя по спецификации, в технологии использовалось покадровое JPEG-сжатие, очевидно, не очень значительное, поскольку заметного глазом ухудшения качества на стандартных изображениях не было.

Через некоторое время корейским производителем был предложен еще один вариант интерфейса, почему-то названного им 3G-SDI. Следуя описанию, он не имеет ничего общего с типовым телевизионным 3-гигагерцевым вариантом 3G-SDI (SMPTE 424M). Благодаря использованию сжатия H.264 видеопоток, даже с раздельной передачей информации о яркости и цветности, существенно снижен по битрейту. Это позволило увеличить дальность передачи до 500 м по коаксиальному кабелю и до 2000 м по витой паре. Здесь фактически утрачен принцип несжатой передачи. Примечательно, что камеры с выходом EX-SDI распространены значительно шире варианта 3G-SDI.

К сожалению, сейчас уже можно констатировать, что форматы на основе технологии HD-SDI "не пошли", а если и применяются, то исключительно для специальных задач. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

На борту или за бортом? Камеры со встроенной видеоаналитикой

Мнения экспертов

Камеры со встроенной видеоаналитикой дают ощутимый экономический эффект в деятельности самых разных объектов,не только повышая уровень безопасности, но и автоматизируя многие типовые события и бизнес-процессы. Они позволяют снизить нагрузку на сетевую инфраструктуру и серверы, упростить контроль объекта и перевести внимание оператора только на тревожные уведомления. Для каких задач встроенная видеоаналитика подойдет идеально, а когда лучше все-таки сохранить ее на сервере? Эксперты из компаний Faceter Russia, Ivideon и Vidau Systems рассказали о самых популярных модулях встроенной видеоаналитики, привели примеры реальных кейсов и оценили перспективы этого класса камер

Эдуард Костырев
Исполнительный директор компании Faceter Russia

Заур Абуталимов
Директор по продуктам сервиса облачного видеонаблюдения и видеоаналитики компании Ivideon

Александр Снегирев
Директор по техническому развитию компании Vidau Systems

Какие модули встроенной видеоаналитики наиболее популярны сегодня?

Эдуард Костырев, Faceter Russia
На сегодняшний день наиболее популярными типами аналитики, встроенной непосредственно в камеры наблюдения, является детекция движения или ее более продвинутый вариант – не просто обнаружение движения в кадре, но и его анализ в виде пересечения заданной границы или покидания заданной области.
Набирает популярность аналитика, связанная с детекцией исчезновения или появления новых предметов в заданной области. Развиваются опции, позволяющие детектировать наличие дыма или огня в кадре, а также разного рода антивандальная аналитика (реакция на изменение положения камеры, закрытие объектива или расфокусировку, сильную засветку и т.д.). Отдельно можно отметить распознавание номерных знаков.
Детекция силуэтов и лиц пока встречается реже и ограничивается именно детекцией (реже детекцией + идентификацией) без персонализации, которая может быть выполнена уже сторонним ПО.

Заур Абуталимов, Ivideon
Наиболее высокий спрос приходится на модули детекции людей и подсчета посетителей. В последнее время повышенное внимание бизнес проявляет к технологии распознавания лиц.

Александр Снегирев, Vidau Systems
На первый план выходят следующие модули видеоаналитики:
1. Фейс-контроль с созданием баз лиц для дальнейшей аналитической обработки.
2. Подсчет пассажиров и статистическая обработка перемещения людей.
3. Определение номеров транспортных средств.
4. Определение забытых вещей, а также вновь появившихся в кадре.

Устойчивый рост рынка

Исследовательская компания Tractica прогнозирует устойчивый рост рынка видеоаналитики в ближайшие пять лет. В 2025 г. выручка должна достигнуть 4,5 млрд долларов.
Усовершенствование алгоритмов компьютерного зрения, растущие вычислительные мощности и увеличение разрешения камер наблюдения позволили сделать более точными результаты видеоаналитики. Это, в свою очередь, способствует более широкому внедрению технологий анализа видеоданных.
По данным Tractica, выручка на рынке видеоаналитики в 2019 г. увеличилась до 1,5 млрд долларов, тогда как в 2018 г. она составила 1,1 млрд долларов. В 2020 г. показатель приблизится к 2 млрд долларов, а в 2023 г. преодолеет отметку в 3 млрд долларов

По материалам DailyComm

В каких областях применение данных модулей может принести максимальную пользу?

Эдуард Костырев, Faceter Russia

Из наиболее понятных с точки зрения применения и практических кейсов можно назвать сферы безопасности и маркетинга.

Например, детекция движения в целом или в заданной области кадра позволяет упростить работу при контроле охраняемых зон. Детекция посторонних предметов в заранее заданной зоне понятным образом ускоряет реакцию персонала на потенциально опасные для общественного порядка события. Распознавание номеров уже достаточно широко применяется на объектах контрольно-пропускного режима для автомобилей и позволяет практически полностью автоматизировать некоторые самые типовые кейсы. С помощью детекции силуэтов и лиц (и здесь в полной мере достаточно только детекции) можно вести общий подсчет посетителей и строить тепловые карты их перемещения в торговой зоне. Хотя решения для данного типа аналитики сегодня чаще находятсяв сфере внешнего ПО, нежели камеры.

Во всех упомянутых кейсах аналитика из антивандальной области поможет быстрее отреагировать на изменение условий съемки для камер наблюдения (а это особенно важно, когда на аналитику завязан какой-то бизнес-процесс).

Заур Абуталимов, Ivideon

Видеоаналитика – безотказный помощник в вопросах безопасности и сравнительно дешевый способ сбора Big Data. Широкие возможности, которые дают камеры со встроенной аналитикой, применимы практически в любой области, будь то контроль доступа на режимный объект или изучение посетителей сети магазинов в маркетинговых целях.

- Детекция людей. Технология, способная качественно заменить детекцию движений, к работе которой на рынке остаются вопросы. Детекция движений работает по принципу анализа последовательных кадров – реагирует на любое изменение в картинке. Получается, что движение веток дерева от ветра или тень на стене от прошедшего мимо человека может вызвать ложное срабатывание системы безопасности. В этом плане модуль распознавания конкретного объекта – человека позволяет существенно снизить процент ложных детекций и повысить уровень безопасности.
- Подсчет посетителей. Одна из ключевых метрик, которая напрямую влияет на выручку конкретной точки и успешность бизнеса в целом. Если раньше считать трафик предпринимателям приходилось вручную, то теперь получать подробную статистику можно в автоматизированном режиме. Это позволяет управляющим оперативно принять меры, если трафик в один момент, например, резко снизился. На количество клиентов мог повлиять начавшийся у входа в магазин ремонт дороги, и в таком случае волноваться не стоит, вопрос со временем решится сам. Но могут сыграть роль и проблемы в бизнес-процессах, которым нужно уделить повышенное внимание.
- Распознавание лиц. Безусловный тренд видеоаналитики. Рост спроса на технологию связан с запуском в конце прошлого года первых в России облачных модулей для распознавания, которые привели к упрощению подключения и значительному снижению стоимости системы. Несмотря на растущий спрос, нельзя сказать, что технология используется повсеместно. Пока бизнес делает только первые видимые шаги в сторону практического применения таких модулей.

В первую очередь распознавание лиц помогает в вопросах безопасности. С помощью черных списков можно сформировать базу лиц, которые ранее были замечены за кражей или нарушениями порядка в магазине. "Узнав" такого человека, камера отправит уведомление ответственным за безопасность сотрудникам.

Применение распознавания лиц, эмоций, пола и возраста позволит ритейлу персонализировать предложения, а банкам – следить за качеством обслуживания клиентов. Мы знаем кейсы, где распознавание эмоций сотрудников используется для повышения эффективности работы. Руководство компании отслеживает общий эмоциональный фон и в соответствии с ним изменяет систему мотивации, перераспределяет задачи и нагрузку работников.

см. стр. 128 "Ньюсмейкеры"

Александр Снегирев, Vidau Systems

Фейс-контроль может быть использован:

- в системах контроля доступа, когда по определению лица возможен (или нет) доступ на объект, что позволит исключить, например, консьержа или охранника на входе;
- в местах скопления людей (стадионы, эстрадные площадки и т.д.) для выявления разыскиваемых лиц или определения мимики лица неадекватных людей;
- в ритейле, гипермаркетах, где можно использовать базу покупателей для определения ассортимента товара и при повторных посещениях рекомендовать товар.

Подсчет пассажиров и статистическая обработка перемещения людей будут полезны для развития инфраструктуры районов города, транспортной структуры с целью оптимизации трафика. А если объединить все данные в ЦОД, то это поможет городу в целом.

Определение номеров целесообразно при розыске угнанных транспортных средств, а в сочетании со средствами контроля доступа (автоматические ворота или шлагбаумы) упрощает заезд на стоянки и во дворы по допуску, считывая номера.

До какой степени целесообразно автоматизировать реакцию систем на тревожные события видеоаналитики?

Эдуард Костырев, Faceter Russia

Это достаточно сложный и комплексный вопрос. Подходить к его решению лучше с точки зрения экономической эффективности. Нужно понимать, какие у компании возникают риски в связи с ложноположительным или ложноотрицательным срабатыванием системы и во сколько компании будет обходиться ликвидация последствий в таких ситуациях. Это нужно сопоставить с затратами на внедрение и (что немаловажно) сопровождение таких систем.

В целом аналитика на базе видеонаблюдения все же остается скорее вспомогательной и дополнительной к другим автоматизированным системам. Например, пожар достаточно хорошо детектируется специализированными средствами. А вот открытие шлагбаума уже может быть значительно (или полностью) автоматизировано с помощью видеоаналитики (особенно если речь идет о публичном месте и цена ошибки невысока).

Заур Абуталимов, Ivideon

Полная, абсолютная автоматизация систем безопасности любого объекта несет больше рисков, чем пользы. В качестве примера можно взять пассажирский самолет – объект, критически чувствительный к ошибкам. Пилоты проходят долгие часы тренировок, но не вмешиваются в работу системы при штатном полете и не корректируют движение каждую минуту, а время от времени наблюдают за показателями приборов. Большую часть времени самолет управляется автопилотом. Тренировки помогают быстро взять управление на себя и принять стратегически важное решение в редких кризисных условиях, когда автоматика ошибается или не справляется с поставленной задачей.

Александр Снегирев, Vidau Systems

Если классифицировать системы по уровню ответственности за события, то станет понятно, что видеоаналитика, внедренная для реакции на тревожные события, весьма несовершенна.

Так, если внедрять видеоаналитику в системы пожарной безопасности, то надо вводить еще один уровень, так называемый желтый, от ложных срабатываний.

Видеоаналитика, интегрированная в работу экстренных служб, может работать только как вспомогательная система. Решение принимает человек, например ответственный дежурный, иначе может случиться коллапс.

А вот открывание двери вместо консьержа вполне реалистично. Открывание шлагбаума, например, для заезда на стоянку, сложно тем, что трудно увидеть и распознать лицо водителя. Считывание номеров не обезопасит от проникновения на закрытую территорию посторонних лиц. Поэтому лучше и проще использовать средства контроля доступа, радиобрелоки или звонок с мобильного телефона.

см. стр. 128 "Ньюсмейкеры"

Обоснован ли перенос аналитики из серверов в камеры?

Эдуард Костырев, Faceter Russia

Очень многое зависит от конкретной задачи и ситуации. В некоторых случаях использование встроенных в оборудование модулей аналитики целесообразно, а следовательно имеет хорошие перспективы. Например, в случаях, когда на объекте большое количество камер, требуется очень широкий канал для передачи видеопотока на сервер с целью его дальнейшего анализа. Здесь аналитика внутри камер может взять часть задач на себя, сильно сократив объем видеопотока, который требуется передавать на сервер (а в ряде случаев может быть достаточно передачи только ключевых кадров). Не стоит забывать и о сохранности чувствительных персональных данных, когда передача видеопотока куда-то на сторонний сервер может быть нежелательна, а аналитических возможностей софта камеры, скажем, достаточно для решения задачи, и система может быть автономной.

Вместе с тем такая конфигурация менее защищена от взлома или вмешательства в процесс обработки данных извне. В ряде случаев реакция системы на событие должна быть практически мгновенной и задержка даже в 300 мс может быть недопустимой, а при проведении аналитики без использования удаленных серверных мощностей можно свести такие задержки практически к нулю.

В то же время при большом количестве камер и большом объеме проводимой аналитики применение централизованных мощностей может быть гораздо эффективнее экономически. Серверные мощности можно эффективно распределять между данными с камер. Допустим, часть камер на объекте генерирует много данных для аналитики только утром, а другая часть – только вечером. Применение встроенной аналитики означало бы избыточное использование ресурсов, которые простаивают большую часть времени.

Стоит упомянуть, что при постановке задачи интеграции аналитики с какими-то сторонними системами на предприятии она решается гораздо проще при осуществлении аналитики централизованно на сервере.

Заур Абуталимов, Ivideon

Камеры со встроенной видеоаналитикой уже несколько лет присутствуют на рынке. Спрос на них стабилен. Решения подобного класса позволяют экономить на интернет-трафике, что важно при развертывании сети видеонаблюдения на объектах с ограниченной пропускной способностью каналов связи.

Труднодоступные, удаленные объекты, особенно в нефтегазовой отрасли, кабельные сети банкоматов, системы на базе беспроводных сетей чувствительны к объемам трафика. Встроенная видеоаналитика обрабатывает видео в режиме реального времени без подключения дополнительных ресурсов и отправляет на сервер через Интернет лишь готовые "отчеты" – критически важные уведомления, тревожные сигналы, приоритизированные сообщения.

Из минусов можно отметить высокую цену, сложное и дорогостоящее техническое обслуживание. Обновление и масштабирование системы, построенной на базе локальной аналитики, также затруднено. Выход из строя даже одной камеры может вызвать серьезную брешь в периметре безопасности предприятия. У подобных камер от разных производителей возникают проблемы совместимости, что затрудняет удаленный контроль.

Александр Снегирев, Vidau Systems

Поскольку аналитика реализуется функционально-модульно под задачу, нет смысла переносить столь сложное ПО в камеры. Это заметно повысит их стоимость, усложнит схемотехнику, они будут более уязвимы по электропитанию к окружающей среде.

Есть альтернативное решение – Stand Alone NVR, где вся аналитика интегрирована в прошивку регистратора в Linux. Это повышает надежность всей системы и стабильность ее работы, а по стоимости значительно дешевле, чем система на ПК.

см. стр. 128 "Ньюсмейкеры"

МНЕНИЕ ЭКСПЕРТА

Наиболее перспективна нейросетевая аналитика

Дмитрий Калинин
Продакт-менеджер компании DSSL

На сегодняшний день встроенная аналитика еще не получила массового распространения. Играет роль определенный консерватизм заказчиков и нехватка информации о том, какие экономические выгоды можно получить за счет применения инновационных решений. Однако отрасль развивается динамично, и встроенная аналитика все же входит в нашу жизнь. Когда она станет по-настоящему популярной – это только вопрос времени, причем достаточно скорого

На текущий момент наиболее востребованы самые простые функции встроенной видеоаналитики – пересечение линий, вторжение в зону, детекция лиц и оставленных предметов. Спрос определяется в первую очередь невысокой стоимостью данных модулей: цена камер с такой аналитикой не сильно отличается от аналогичных моделей без аналитики. Из новых относительно недорогих решений можно также отметить детекцию людей. За более дорогие решения, такие как распознавание лиц или автомобильных номеров, подсчет людей и определение их атрибутов (цвет одежды, пол, возраст и т.д.), готовы платить пока лишь немногие крупные заказчики, строящие системы видеонаблюдения на эксклюзивных объектах.

С пользой для объекта

Простую аналитику, дополненную функцией детекции людей, будет полезно использовать на большинстве типовых объектов. Ведь наибольший интерес для видеонаблюдения, как правило, представляют именно люди и их перемещения. Конечно, максимальную пользу такие решения принесут на режимных объектах, при охране периметра, контроле производственных площадей и прочих объектах с регламентированным ограничением передвижения в пределах заданной области.

Из сервера в камеру

Главный плюс переноса аналитики из серверов в камеры – разгрузка вычислительных мощностей сервера. Для систем с небольшим числом каналов особого смысла в такой периферийной аналитике нет. Однако чем больше камер, для которых требуется вычислительная мощность, и чем более сложная аналитика используется в системе, тем дороже обходится ее использование на сервере. Во-первых, из-за более дорогой архитектуры самих чипсетов, используемых на серверах. Во-вторых, по причине, условно говоря, простоя оборудования: ведь чем больше смарт-операций производится на сервере, тем меньше камер к нему можно подключить. Соответственно, гораздо выгоднее использовать умные камеры вместо обычных, чем покупать больше серверов. Притом что и сами серверы с умными функциями стоят, конечно, существенно дороже их бюджетных аналогов.

Кроме чисто экономической выгоды, использование периферийной аналитики также является более гибким в плане сетевой архитектуры, обслуживания и управления системой (особенно в случае большой распределенной системы на несколько тысяч камер, например).

Минусом периферийной аналитики на данный момент является все же более низкая точность детекции по сравнению с серверной. Однако после появления в недавнем прошлом нового типа высокопроизводительных (от 500 млрд операций в секунду) чипсетов, так называемых нейросетевых процессоров для видеокамер, данный разрыв по качеству аналитики будет неизменно сокращаться.

Будущее – за автоматизацией

Учитывая современные технологические тренды внедрения искусственного интеллекта во все системы, где это только возможно, надо полагать, что и видеонаблюдение со смежными отраслями (такие как контроль доступа) не должно быть исключением – применение автоматизации позволит кардинально повысить точность срабатывания и полностью устранит человеческий фактор. Есть все основания считать, что ближайшее будущее – за полной автоматизацией таких систем. Конечно, с той оговоркой, что система все же должна предусматривать возможность фонового контроля со стороны оператора, то есть полностью автоматическая работа в штатном режиме с возможностью ручного управления на случай нестандартных ситуаций, как в электромобиле известной марки.

Развитие нейросетевой аналитики

Наиболее перспективна нейросетевая (AI) аналитика, которая сейчас находится на гребне технологического развития. Во-первых, она основана на современных алгоритмах машинного обучения, что позволяет создавать любые сценарии идентификации и структурирования видеоданных. Это дает возможность настроить аналитику под любые, самые специфичные требования заказчика, не привязываясь к традиционным модулям типа распознавания лиц или детекции дыма. Во-вторых, возможности искусственного самообучающегося интеллекта уже сейчас кратно превосходят человеческие. Нейросети, например, могут решать даже такие сложные прикладные задачи, как постановка диагноза – определение некоторых болезней по фотографии пациента. Поэтому и в сфере видеонаблюдения применение нейросетевой аналитики выглядит очень перспективно.

Какие модули видеоаналитики имеют наилучшие перспективы развития?

Эдуард Костырев, Faceter Russia

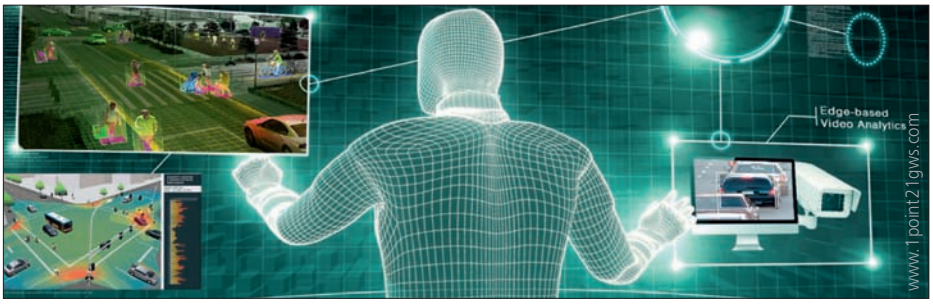
Наиболее перспективны те модули аналитики, для которых уже сложилось более или менее предметное понимание практической применимости. Прежде всего это кейсы безопасности и контроля (детекция движения, детекция лиц и силуэтов, контроль границ или зон в кадре), а также первичной маркетинговой аналитики.

Самой универсальной является антивандальная аналитика. Она может применяться для наиболее широкого круга задач по видеонаблюдению, меньше зависит от сути конкретного кейса и хорошо реализуется внутри самой камеры.

Более сложная аналитика непосредственно на камерах (как, например, идентификация и персонализация лиц) вряд ли будет активно развиваться в ближайшее время, потому что такие кейсы более сложные и гораздо лучше решаются сторонним программным обеспечением, которое к тому же проще кастомизировать под нетиповые задачи.

Заур Абуталимов, Ivideon

Мы видим большой потенциал в развитии распознавания лиц. Компании уже ищут возможности интеграции технологии со своими системами. Думаю, что в 2020 г. мы увидим первые рабочие кейсы применения распознавания лиц не только в целях безопасности, например в



СКУД, но и в маркетинге с дополнительной аналитикой пола, возраста и эмоций.

Еще один перспективный в первую очередь для ритейла продукт, – контроль кассовых операций с помощью камер видеонаблюдения. По статистике, 38% потерь ритейла связаны с действиями покупателей и сотрудников. Проблему двойных пробитий, отмены пробития, незакрытых чеков решит камера с модулем контроля кассовых операций. Сервис, связанный с кассовым аппаратом, "увидит" подозрительную операцию и укажет в отчете, что на нее стоит обратить внимание. Человеку останется только зайти в архив и посмотреть отрезок видео, который автоматически привязан к подозрительному документу – кассовому чеку. Таким образом, у ритейла есть отличная возможность сократить потери выручки от кассовых махинаций практически до нуля.

Александр Снегирев, Vidau Systems

Самые перспективные направления:

- подсчет пассажиров с целью управления пассажиропотоками, развития транспортной инфраструктуры и районов города;
- видеоконтроль с целью обнаружения лиц, разыскиваемых правоохранительными органами, и неадекватных людей в толпе;
- подбор товаров в ритейле, когда продавцы могут помочь гражданам, часто посещающим те или иные крупные магазины. В этом вопросе может помочь аналитика по гендерному и возрастному признаку. Но здесь есть и подводный камень – многие люди считают это вмешательством в их личное пространство.

МНЕНИЕ ЭКСПЕРТА

Читателей билбордов подсчитала камера с видеоаналитикой

Андрей Ивахненко
Продукт-менеджер компании RedLine

Последние несколько лет наиболее распространенными модулями видеоаналитики были обнаружение пересечения линии, контроль периметра, оставленные/исчезнувшие объекты. Однако все чаще и чаще возникает потребность в модулях, отвечающих за распознавание образов – автомобилей, людей, лиц и характеристик человека (пол, возраст, эмоции). Получается, если раньше наиболее востребованными были базовые алгоритмы (пересечение линии), то сейчас потребители хотят более качественного улучшения работы функций за счет применения искусственного интеллекта.

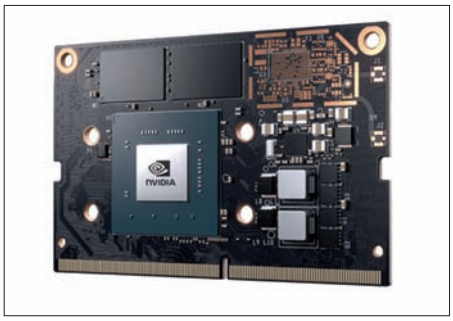
Наиболее полезны встроенные аналитические модули при установке на объектах малого бизнеса. Владельцам небольших организаций очень важно учитывать общую стоимость решения – количество выполняемых функций к общей стоимости системы. Зачастую встроенный модуль видеоаналитики позволяет заменить какую-либо дополнительную систему или службу, что является прямой экономической выгодой. Примером из нашей практики может служить проект с организацией видеоаналитики для компании, занимающейся брокериджем коммерческой недвижимости. Заказчик отвечал за сдачу в аренду коммерческих площадей, расположенных в наиболее проходимых частях города, и нуждался в точном понимании потенциальной аудитории для подбора арендатора. Установка видеокамер и аналитического модуля позволила решить поставленную задачу путем подсчета и анализа половозрастных характеристик проходящих людей, помогла в выборе оптимальных арендаторов и повысила эффективность бизнеса.

В настоящее время можно наблюдать активный перенос аналитики из серверов в камеры. Подобная тенденция, на наш взгляд, является положительной. В качестве плюсов можно отметить снижение нагрузки на сеть в системах с аналитикой, снижение требований к производительности сервера/регистратора. Это особенно важно для распределенных (децентрализованных) объектов. Например, в еще одном нашем проекте установка камер с аналитикой на борту в рекламных щитах была единственным подходящим решением для компании, владеющей бизнесом по сдаче щитов в аренду. В противном случае невозможно было бы обеспечить необходимый канал для связи всех точек и стоимость сервера совместно с ПО была бы слишком высока. Установленные камеры обеспечили возможность проанализировать трафик посетителей и использовать эти данные при формировании тарифов на аренду рекламного места.

Говоря о возможности автоматизации реакции системы на тревожные события видеоаналитики (открывание шлагбаума, пожарная тревога, вызов экстренных служб и т.д.), стоит учитывать, насколько качественно и достоверно работает тот или иной модуль, а также насколько важен и критичен этот объект. По закону, системы пожарной безопасности могут использовать видеоаналитику только в качестве дублирующей системы для видеоверификации тревоги. Пример работы системы контроля доступа на территорию ЖК с распознаванием образов объектов позволил в автоматическом режиме открывать ворота для машин скорой помощи и пожарных служб. Однако такая система контроля доступа должна быть не единственным средством.

Наилучшие перспективы развития имеют модули аналитики, позволяющие принципиально улучшить решение существующих проблем. В первую очередь это касается систем распознавания лиц, эмоций, поведения, а также классификации объектов, модулей, которые позволят автоматизировать процессы и повысить эффективность решения поставленных задач. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru



Новые революционные видеорегистраторы для транспорта от EverFocus

Тайваньская компания EverFocus Corporation анонсировала новейшую серию специализированных видеорегистраторов для транспорта с расширенными возможностями – eIVP (Intelligent Vehicle Platform). Разработчики EverFocus реализовали принципиально новый революционный подход к выполнению требований по обеспечению безопасности на транспорте

Новая серия MDVR представляет собой новую платформу с более гибким подходом к подбору оборудования: исходя из требований проекта, выбранная модель комплектуется индивидуальным аппаратным набором, включая основной процессор (CPU). Модельный ряд представлен четырьмя основными системами.

Продвинутая техническая начинка

В качестве основного источника видеосигнала используются бортовые IP-камеры, подключаемые по PoE. Старшая в модель в линейке eIVP 5600 в зависимости от задачи может комплектоваться Intel® 7th Gen. Core™ i7 Processor или i7-7600U 3.9 GHz. Младшая модель в серии, 4-канальная система eIVP 1300, комплектуется Intel® Atom™ E3845, 1.91 GHz.

Все модели имеют по два сетевых адаптера x 1Gbps, порты RS-485 и RS-232 для управления и подключения к CAN-шине. Серия обладает всеми необходимыми аппаратными возможностями.

Кроме стандартных и обязательных для MDVR подогрева HDD/SSD, предусмотрен подогрев материнской платы и контроль температуры. В основе всех моделей лежит безвентиляторный PC-IXT, а в модели eIVP 5600 есть "горячая замена" (Hot-Swapp) сразу двух HDD/SSD.

В серии предусмотрен стандартный набор модулей беспроводной связи для мобильных решений – модем 4G и Wi-Fi, а навигационный чип ГЛОНАСС/GPS уже установлен в базе на всех моделях, кроме eIVP 1300.

Процессор Intel Movidius для нейросетевых вычислений

Главной отличительной особенностью платформы является возможность подключения модуля Intel Movidius (Intel® Movidius™ Myriad™ 2 2450 TensorFlow, Caffe) и NVIDIA Jetson Xavier. Специализированный процессор Movidius Myriad 2 2450 разработан для обработки изображений с целью различения отдельных объектов подобно тому, как это делает мозг человека. Плата с процессором устанавливается в слот Mini-PCI на системной плате MDVR и взаимодействует с программным обеспечением, беря на себя большую часть ресурсоемких операций по обработке оптических потоков, отдельных кадров или данных телеметрии. По сути, такой модуль является специализированным устройством для нейросетевых вычислений. Модуль построен на базе чипа Myriad 2, содержащего 12 программируемых векторных процессоров.

Модель eIVP 1570 DE является гибридной и может поддерживать видео от AHD камер. Как уже понятно, аппаратной производительности достаточно для обработка сигнала независимо от типа видео. Именно eIVP 1570 DE комплектуется специализированной процессорной сборкой NVIDIA Jetson Xavier для нейросетей.

Мощная аналитика на борту

Основная цель и назначение новой серии eIVP от EverFocus – это реализация аналитических функций и приложений, интегрированных с бортовой системой видеонаблюдения. На базе этой платформы становится возможным построение интеллектуальных самообучающихся бортовых систем, способных работать как автономно, так и в составе сложных городских структур. Становится реальным применение бортового машинного зрения, позволяющего транспорту, работающему в беспилотном режиме, огибать препятствия при движении и др. В случае стационарного использования, например в торговых системах, можно узнавать постоянных покупателей и предугадывать их запросы, подобно поисковым системам.

Больше, чем просто "рекордеры"

Выход новой серии eIVP от EverFocus знаменует собой появление на рынке принципиально нового направления в транспортных и стационарных системах видеонаблюдения – мобильных систем с бортовой аналитикой.

Объединенные в единую транспортную систему, такие регистраторы могут успешно выполнять роль не просто "рекордеров". Это будут автономные передвижные модули "глаз + мозг" на улицах городов, фиксирующие, анализирующие и по необходимости передающие информацию в центр управления.

В случае подключения к CAN-шине транспортного средства становится возможным не только стандартная запись информации с датчиков, но и принятие решений на основе этих показаний. Наличие таких систем способно разгрузить головные центры обработки и анализа данных: eIVP-решения смогут самостоятельно и автономно анализировать и накапливать видео-/аудио-/фото-/метаинформацию, принимать решения на базе анализа и обучаться. С выходом этой серии закладывается прочный фундамент для будущих новых задач и связанных с ними приложений.

На старте продаж

Без преувеличения можно сказать, что эта серия открывает дорогу для применения искусственного интеллекта в реальных транспортных проектах и решениях. В настоящее время серия уже имеет международную сертификацию E-Mark, EN50155, SAE-J1455 и полностью готова к заказам в России.

По всем вопросам обращайтесь в компанию Vidau Systems. Информация о появлении новинок, комплектациях и ценах размещена на сайте www.vidau-cctv.ru. ■

			
eIVP 1300 – 4 канала	eIVP 3300 – 4 канала	eIVP 5600 – 8 каналов	eIVP 1570 – 8 каналов

"Утечка мозгов" в камеру: перспективы развития рынка встроенной видеоаналитики

В ближайшие пять лет рынок видеоаналитики ждет лавинообразный рост. Технологии анализа видеоданных уже давно вышли за рамки вопросов безопасности, завоевывая все новые позиции в самых разных сферах. Число и спектр аналитических задач, решаемых внутри камер, неуклонно растет. Встроенная видеоаналитика набирает обороты и меняет сложившиеся представления о видеонаблюдении. В этой статье я поделюсь своим мнением о перспективах развития данного направления

Евгений Веснин
Технический директор
ООО "Малленом Системс"

Исторически первыми модулями видеоаналитики в видеокамерах были модули обнаружения движения, которые впоследствии получили развитие до модулей определения пересечения линии и обнаружения вторжения в заданную область на кадре.

С ростом вычислительных мощностей процессоров камер появилась возможность выполнять на борту более сложную аналитику – распознавание номеров автомобилей, детекцию лиц, детекцию людей, трекинг объектов и др.

Рынок сегодня: сферы применения и популярные модули

Системы видеонаблюдения в большинстве случаев являются элементом системы безопасности объекта. С ростом доступности и количества установленных видеокамер возрастает нагрузка на оператора системы, что негативно сказывается на эффективности его работы. Использование модулей обнаружения движения позволяет привлекать внимание оператора к тем зонам, где что-то происходит, и не отвлекаться на наблюдение зон без движения.

Обнаружение движения на стороне камеры снижает требования к производительности видеосервера/регистратора и позволяет увеличить глубину видеоархива за счет записи фрагментов с движением в более высоком качестве, в то время как фрагменты без движения могут быть записаны с более низким качеством или вовсе не сохраняться.

Модуль трекинга объектов позволяет при меньшем количестве видеокамер получать изображения интересующих объектов в высоком разрешении. Обычно это подразумевает использование связки нескольких видеокамер. На обзорной фиксированной видеокамере происходит обнаружение движущихся объектов, а согласованная с ней поворотная видеокамера ориентируется на них и формирует крупный план обнаруженных объектов.

В последнее время наблюдается повышение спроса на модули видеоаналитики со стороны ритейла и объектов транспортной инфраструктуры. Интерес представляют задачи подсчета посетителей и определения их половозрастного состава, определение длины очередей, построение тепловых карт посещаемости внутри торгового зала. Пока эти задачи в полной мере не могут быть решены на борту камеры, но некоторые видеокамеры уже имеют модули выделения людей и лиц, результаты работы которых можно использовать в составе специализированных решений.

Камеры с модулем распознавания номеров автомобилей находят применение в ограниченном классе задач. Там, где требуется более комплексная автоматизация, они выступают элементом специализированного решения.

На борту или на сервере

Производительность процессоров видеокамер продолжает расти, в то время как цены на них неуклонно снижаются. С течением времени и увеличением вычислительной мощности камер возможности для размещения постоянно растущего массива аналитических функций также возрастают.

Неоспоримым достоинством переноса аналитики в камеры можно назвать снижение требований к серверу, уменьшение нагрузки на сеть, что в некоторых случаях приводит к удешевлению системы в целом. Однако это актуально при оснащении нового объекта или его модернизации, что сопряжено с существенными капитальными затратами.

Решения на базе сервера позволяют использовать уже установленные видеокамеры и быстро добавлять возможности аналитики в существующие системы. В целом потребности бизнеса в видеоаналитике настолько разнообразны, что, скорее всего, в ближайшие годы наибольшей популярностью будут пользоваться гибридные решения, где часть аналитики будет выполняться на борту камеры, а часть на стороне сервера.

Анализируй, чтобы управлять

Сейчас большинство камер имеет гибкую регулировку реакций на разные события, в том числе от аналитических модулей. Это позволяет настроить реакцию камеры требуемым образом. Из средств для наладки реакции камер чаще всего доступны один-два релейных выхода, которые могут использоваться для управления внешними устройствами (шлагбаум, тревожная сигнализация), и программный сигнал, который может быть обработан внешней системой. Для простых сценариев использования этого достаточно, в более сложных случаях требуемая реакция реализуется на стороне внешней системы.

Точки роста

С учетом того что объектами интереса камер видеонаблюдения в большинстве случаев являются транспортные средства и люди, в первую очередь аналитические модули будут развиваться в направлении выявления и описания этих объектов. Развитие компьютерного зрения и нейронных сетей делает возможным выполнение тегирования видео и распознавание действий на видео, что является также очень перспективным направлением развития аналитических модулей. Нейронные сети могут использоваться для извлечения низкоуровневых визуальных признаков изображений внутри камеры, чтобы впоследствии можно было выполнять анализ изображений для разных задач.

В задачах промышленного контроля ведущие производители смарт-камер машинного зрения предоставляют набор инструментов, позволяющих сконфигурировать видеокамеру для решения различных задач. Возможно, и в области видеонаблюдения мы сможем вскоре увидеть такие конструкторы. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Биометрическая идентификация в офисе Lamoda

Что важно для сотрудников офиса, руководителей и службы безопасности с точки зрения контроля доступа? Как найти компромисс между их желаниями и построить оптимальное решение, устраивающее всех? Рассмотрим на примере проекта внедрения СКУД в офисе Lamoda

Компания Lamoda – ведущая онлайн-платформа в России и СНГ для продажи товаров, связанных с модой и образом жизни. Недавно Lamoda переехала в новый офис в Москве, заняв три этажа крупного бизнес-центра. В связи с переездом встал вопрос проектирования и внедрения новой СКУД, учитывающей все проблемы и нюансы, выявленные при эксплуатации предыдущей системы.

Карты – нет! Биометрия – да!

Одним из пожеланий к новой системе доступа стал отказ от системы электронных пропусков. Несмотря на то, что в компании Lamoda довольно демократично относились к ситуации, когда сотрудник забыл или потерял пропуск, просьбы его заменить создавали ненужные заботы службе безопасности. Это особенно актуально, учитывая, что в базе зарегистрировано 1500 пользователей. Современная альтернатива пластиковым картам – биометрическая идентификация. Преимущества такого подхода очевидны: не нужно носить с собой карты, идентификатор невозможно потерять, скопировать или передать другому лицу.

Особые требования

Какие требования, помимо решения основных задач СКУД, были предъявлены к системе? Прежде всего – стабильная работа при многочисленной базе пользователей (более 1500) и большом количестве точек прохода (40). Одними из приоритетов были удобство идентификации и быстрый бесконтактный проход через точку доступа. При этом требовалось обеспечить интеграцию СКУД Lamoda в единую систему доступа бизнес-центра.

Выбор решения

Для построения новой системы доступа была выбрана биометрическая платформа APACS Bio, разработанная компанией "ААМ Системз", которая поддерживает широкий спектр устройств (считыватели лица, отпечатков пальцев, карт, смартфонов и т.д.). Специализированная российская разработка учитывает большинство потребностей отечественного заказчика (включая функционал УРВ со стандартными формами отчетов), а также обеспечивает:

- интеграцию с внешними системами;
- автоматизацию повторяющихся операций для снижения затрат на поддержку;
- высокий уровень информационной безопасности (доступ к данным, аудит действий операторов);
- оптимизацию для работы с крупными объектами (опыт установки в одной из башен "Москва-Сити" – 1500 точек доступа).

На сегодняшний день система APACS Bio успешно работает на десятках объектов, в том числе в банках, аэропортах, музеях, административных зданиях и на промышленных предприятиях.

Состав оборудования

Всего в офисе Lamoda было организовано 40 точек прохода:

- 20 биометрических точек доступа для прохода в помещения общего пользования (вход и выход по считывателям лица Suprema FaceStation 2);
- 20 точек для ограничения доступа в помещения специального назначения (склады, серверные и т.д.). Доступ в них требуется ограниченному и относительно небольшому числу сотрудников, поэтому с целью сокращения затрат такие помещения были оборудованы считывателями карт Suprema Xpass S2.

Интеграция в единую СКУД бизнес-центра

На турникетах входной группы в бизнес-центр был создан отдельный проход для сотрудников Lamoda. С этой целью на выбранные турникеты были установлены считыватели лица (на вход и выход), подключенные и к единой системе доступа бизнес-центра, и к системе APACS Bio.

Лайфхак для выездных мероприятий

Еще одно преимущество выбранного решения – его гибкость и универсальность. Система может меняться и эволюционировать, подстраиваясь под новые требования и новые задачи.

В качестве примера такой гибкости можно привести использование терминала FaceStation 2 на выездных корпоративных мероприятиях, куда

могут быть приглашены более тысячи сотрудников. Ранее контроль доступа проводил сотрудник службы безопасности путем ручной сверки с ранее подготовленным списком. Это было неудобно, неэффективно и трудозатратно.

На данный момент для выездных мероприятий используется один из считывателей лица FaceStation 2. Его снимают с точки прохода, подключают к автономному источнику питания и устанавливают на мобильный штатив. Сотрудники проходят на мероприятие так же, как и в офис, – по лицу, при этом в автономной памяти считывателя может храниться до 3000 пользователей.

Выиграли все

Стоит ли искать компромисс между удобством для пользователей, уровнем безопасности и экономической эффективностью? В компании Lamoda решили получить все преимущества сразу и выбрали биометрическую систему APACS Bio.

Денис Глушаков, инженер отдела безопасности компании Lamoda, отмечает: "Выиграли все. Сотрудникам не нужно носить карты и искать их по карманам, чтобы войти в офис. Администраторы получили современную систему с удобным интерфейсом, многие функции выполняются автоматически. Сотрудникам службы безопасности не нужно думать о выпуске электронных пропусков. Решением и работой компании "ААМ Системз" мы полностью удовлетворены. Единственный тонкий момент – найти грамотного интегратора для монтажа и настройки системы (у нас был интегратор от офисного центра). В итоге мы получили современное высокотехнологичное решение, соответствующее имиджу компании. Мы не только обеспечили удобство сотрудникам, но и повысили уровень доверия партнеров". ■

КОЛОНКА РЕДАКТОРА

Кто там?..

Цифровые технологии все глубже проникают во все сферы бизнеса и повседневной жизни. Такие глобальные проекты, как "Умный город", "Цифровое ЖКХ", у всех на слуху и стремительно переходят из категории теоретических в практическую область. Цели их понятны: обеспечить автоматизацию процессов, цифровую трансформацию, которая должна в конечном итоге привести к повышению эффективности городской инфраструктуры, повысить безопасность и сделать жизнь людей удобнее. Многие из этих проектов являются составной частью национальной программы "Цифровая экономика", а их реализация зависит от внедрения передовых цифровых и инженерных решений в городской и коммунальной инфраструктуре. Это значит, что системы безопасности и, в частности, СКУД должны встать неотъемлемым элементом данных проектов.

Общая цифровизация нашей жизни существенно сокращает временной интервал от появления новой технологии до ее внедрения в том случае, если данная технология содержит в своей основе реальные преимущества. Поясню на примере: внедрение биометрической идентификации, использование мобильного банкинга и облачных технологий в смартфонах существенно упростило внедрение некоторых давно известных технологий в СКУД. Как ни странно, но появление данных технологий в массовом потребительском сегменте рынка значительно упростило их продвижение в профессиональных приложениях СКУД.

Еще один пример – домофония. Современные домофоны шагнули далеко вперед в количестве и качестве предоставляемых сервисов именно за счет перехода на цифровые технологии. В настоящее время продвинутые модели могут объединять не просто функции спикера и передачу видео на монитор, но также осуществлять идентификацию по картам или биометрическим признакам, связываться с компьютерами в сети предприятия для организации управляющего терминала на любом компьютере и многое другое. Завершая мысль, хочу сказать, что после установки СКУД или домофона у вас не будет необходимости задавать вопрос "Кто там?" при стуке в дверь.

Алексей Гинце
Редактор раздела "Системы контроля и управления доступом", директор по связям с общественностью компании "ААМ Системз"

Умный домофон: удобно для жильцов, выгодно для бизнеса

Исследовательская компания GfK попросила онлайн-пользователей в 21 стране мира, включая Россию, оценить по 7-балльной шкале, насколько они обеспокоены вопросами своей безопасности. Россия с 42% занимает пятое место в списке стран, где больше всего потребителей сказали, что постоянно беспокоятся о личной безопасности. Другими словами, почти половина россиян хочет сделать свою жизнь безопаснее

Александр Детков
Генеральный директор компании Росдомофон

Росту обеспокоенности уровнем безопасности способствует урбанизация, рост городов, расширение спальных районов и постройка многоэтажных жилых комплексов. Родители уже не могут спокойно отправлять детей погулять во двор, а длинные дороги вдоль одинаковых домов не кажутся безопасными ночью даже для взрослых.

Рост мобильного Интернета как фактор влияния на поведение

Технический прогресс не стоит на месте и влияет на паттерны поведения и наши привычки. Основная тенденция последних лет – распространение мобильного Интернета. В городах с населением от 100 тыс. человек мобильным Интернетом пользуются 47,1 млн человек. В исследовании говорится, что это 74% населения, или 89% всех интернет-пользователей в возрасте от 12 лет. В малых городах и населенных пунктах (менее 100 тыс. человек) в Интернет с мобильных устройств заходят 37,4 млн человек – это 64% населения, или 87% всех интернет-пользователей. При этом в малых населенных пунктах доля интернет-пользователей, которые выходят в сеть только с помощью мобильного Интернета, выше, чем в крупных городах – 41% против 27%.

Охват мобильным Интернетом продолжает увеличиваться во всех возрастных группах населения. Число пользователей мобильного Интернета среди людей старшего возрастаза последние два года выросло более чем в два раза[1].

К началу 2019 г. аудитория интернет-пользователей в России среди населения 16+ составила 90 млн человек (+3 млн человек к прошлому году) и достигла отметки 75,4% взрослого населения страны. При этом больше всего растет доля пользователей, которые используют Интернет только на мобильных устройствах. Такие данные опубликовала компания GfK.

К началу 2019 г. доля пользователей Интернета на мобильных устройствах достигла 61%. Годом ранее этот показатель составлял 56%[2].

В эпоху смартфонов и Интернета люди привыкли, что все доступно по одному клику. Так же

Умный домофон позволяет вывести контроль придомовой территории на новый уровень

[1] *https://m.dp.ru/a/2019/09/18/JEksperti_nazvali_kolichest*
[2] *https://www.computerra.ru/234277/61-rossiyan-polzuyutsya-internetom-na-mobilnyh-ustrojstvah/*

и с безопасностью. Им больше недостаточно аналогового домофона на двери подъезда, который к тому же может быть открыт универсальным ключом. Все больше пользователей хотят видеть, кто звонит им в дверь, пришел ли их ребенок домой, что происходит с их машиной на придомовой территории.

80% преступлений происходят на домовой территории

И для этого есть веские основания. Если посмотреть статистику правоохранительных органов, то около 80% преступлений происходят на дворовой территории и совершаются в дневное время, пока люди на работе.

Около трети преступлений происходят в подъезде жилого дома. Это говорит о том, что системы СКУД, широко применяемые в данный момент в жилых домах и на придворовых территориях, пока не в состоянии обеспечить жильцам требуемый уровень личной безопасности и комфорта. Аналоговые домофоны устарели как технически, так и морально, потому что не решают проблему безопасности и не дают чувство защищенности пользователям.

Около трети преступлений происходят в подъезде жилого дома. Это говорит о том, что системы СКУД, широко применяемые в данный момент в жилых домах и на придворовых территориях, пока не в состоянии обеспечить жильцам требуемый уровень личной безопасности и комфорта

Как наличие камер влияет на раскрываемость преступлений

Развитие программы "Безопасный регион" в Москве и Московской области и установка камер наблюдения в общественных местах позволили раскрыть 3 249 преступлений в 2018 г.

Для этих целей государство установило уже 167 тыс. камер, и их количество постоянно растет.

Все большее распространение получают системы видеонаблюдения для контроля событий на придомовой территории. Видеозаписи с камер нередко помогают в расследовании происшествий.

В некоторых регионах России строится централизованная система видеонаблюдения, которая устанавливается в школах, детских садах и подъездах.

Чем может помочь умный домофон?

Внедрение умного домофона позволяет вывести тему контроля придомовой территории на новый уровень для каждого жителя.

Пользователи приложения смогут:

- принимать звонок домофона прямо на мобильный телефон, находясь в любой точке мира, где есть Интернет;
- видеть и слышать того, кто звонит в домофон;
- открыть дверь прямо с помощью мобильного телефона;
- просматривать камеры онлайн в подъезде и на придомовой территории;
- пользоваться архивом (камера фиксирует все события и отправляет в архив);
- через камеру контролировать парковку, детскую площадку или территорию перед подъездной дверью – любую территорию, где установлены камеры.

Любой пользователь получает доступ к зафиксированным событиям, а главное – все эти функции становятся доступны в одном приложении.

Персонализация как тренд

Сегодня всем пользователям предлагается личный тариф сотовой связи, персонализированная подборка музыки, рекомендации по фильмам и сериалам, а таргетированная реклама "догоняет" людей даже в метро. Сервисы сейчас знают о пользователях уже больше, чем их мамы.

Компании уловили спрос на личную безопасность и начали его удовлетворять с помощью различных приложений и услуг, которые можно охарактеризовать как умный домофон.

Собственные решения разрабатывают крупные игроки телеком-рынка, застройщики и, конечно, компании, которые специализируются на услуге "умный домофон". Ведь тренд персонализации не только все еще актуален, но и получил толчок за счет развития искусственного интеллекта и нейронных сетей.

Причины малого количества игроков

Пока в гонку включились не так много игроков, что обусловлено разными факторами.

Далеко не все могут себе позволить создать отдельное подразделение, которое будет заниматься одним приложением. Представьте, сколько ресурсов сюда нужно вложить, развивая услугу с нуля.

Стоимость самостоятельной разработки подобного сервиса может исчисляться миллионами долларов. К тому же современный рынок облачных сервисов предполагает постоянные расходы на программные улучшения, связанные с конкуренцией и меняющимися требованиями рынка. Например, придется ежегодно адаптировать мобильные приложения под новые версии операционных систем от Apple и Google.

Стоимость ежегодной поддержки и развития подобного сервиса сравнима со стоимостью его разработки. Поэтому такие решения недоступны большинству игроков рынка. Однако есть компании, которые специализируются на разработке подобных сервисов и помогают операторам запускать услугу без вложений в разработку дорогостоящего ПО, его поддержание и налаживание инфраструктуры.

Услуга умного домофона – новая для рынка, нет экспертизы в построении и продвижении. Нет также данных о том, как умный домофон помогает увеличению продаж и уменьшению оттока. Это значит, что игрокам сложнее принять решения о крупных вложениях.

И конечно, свою роль в этом вопросе играет инертность, которая вообще свойственна российским рынкам услуг.

Около 80% преступлений происходят во дворах в дневное время

Зачем это управляющим компаниям?

Если с крупным телекомом все более-менее понятно, то зачем умный домофон управляющим компаниям?

Для управляющих компаний мобильное приложение – отличный инструмент для повышения лояльности жильцов и еще один источник заработка. К тому же чем больше доверие к компании, тем выше вероятность, что ее не сменят и будут платить коммунальные платежи вовремя.

Помимо функционала, связанного с безопасностью, современные сервисы предлагают новые способы взаимодействия между жильцами и управляющими компаниями:

1. УК сообщают о важном событии жильцам прямо в мобильном приложении, будь то изменение тарифов ЖКХ или очередное проведение испытаний на теплотрассе.
2. Жители получают дополнительный современный канал взаимодействия через чат в мобильном приложении. В ближайшем будущем через такой чат можно будет запрашивать у УК любую информацию, касающуюся отношений жителя и УК.

Кроме того, появится возможность подключать важные датчики – задымленности, загазованности или состояния входа в технические помещения с обязательным уведомлением всех заинтересованных лиц о таких событиях.

Можно ли отдать такую услугу на аутсорсинг?

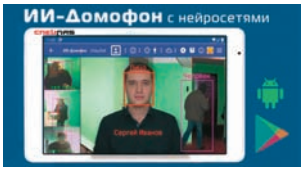
Как ни странно, такую сложную услугу и ее обслуживание можно отдать на аутсорсинг. На рынке присутствуют несколько компаний, которые специализируются только на умных домофонах. Они отличаются списком поддерживаемых домофонов, уровнем сервиса, простотой инсталляции и эксплуатации платформы и, конечно, же размером ежемесячного платежа.

В результате оператор услуги получает еще один источник дохода и канал взаимодействия с клиентами, а пользователи – личную безопасность и удобство для себя и своих близких. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Модель IP-домофона	BEWARD DKS15102	BEWARD DKS15120	BEWARD DS06A
			
Производитель, сайт	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru
Компания, предоставившая информацию, сайт	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru
Тип домофона	Многоабонентский	Многоабонентский	Однооабонентский
Голосовое дублирование действий пользователя	Нет	Нет	Нет
Тип операционной системы домофона	Нет данных	Нет данных	Нет данных
Клавиатура	Механическая	Механическая	Механическая
Датчик приближения	Нет	Нет	Нет
Отдельная кнопка вызова консьержа	Да	Да	Нет
Датчик вскрытия снятия панели	Да	Да	Нет
Характеристики камеры	1/3", 1,3 Мпкс, 3,7 мм	1/3", 1,3 Мпкс, 2 мм	1/3", 1,3 Мпкс, 3,7 мм
Встроенный SIP-сервер	Нет данных	Нет данных	Нет
Количество поддерживаемых абонентов	9999	9999	3
Возможность регулировки встроенной камеры	Да	Да	Да
Реле управления замком	Встроенное	Встроенное	Встроенное
Возможность управления двумя замками	Да	Да	Нет
Поддерживаемые кодеки	H.264, MJPEG, G.711, G.726, дуплекс, эхоподавление	H.264, MJPEG, G.711, G.726, дуплекс	H.264, MJPEG, G.711, G.726, дуплекс, эхоподавление
Поддержка протоколов RTSP/ONVIF	Да	Да	Да
Поддержка протокола SIP, TCP/IP	Да	Да	Да
Поддержка сигнала DTMF	Да	Да	Да
Подсветка (LED/ИК)	ИК	ИК	ИК
Дальность действия подсветки, м	10	10	10
Возможность прохода по цифровому коду	Да	Да	Нет
Тип питания	12 В DC	12 В DC	12 В DC/PoE (опция)
Потребляемая мощность в состоянии покоя	Нет данных	Нет данных	Нет данных
Потребляемая мощность в рабочем режиме	Нет данных	Нет данных	Нет данных
Степень защиты IP	IP66	IP66	IP54
Тип считывателя	EM-Marine, MIFARE	EM-Marine, MIFARE	Нет
Встроенный контроллер для карт	Да	Да	Нет
Поддержка Wiegand 26	Нет, 1-wire	Нет, 1-wire	Нет
Диапазон рабочих температур, °C	-50...+60	-50...+60	-40...+50
Тип установки	Врезной	Врезной	Накладной
Габаритные размеры, мм	262x150x32	262x150x32	73x166x51
Материал/цвет корпуса	Металл	Металл	Металл, черный/серый
Масса, кг	1,1	1,1	0,57
Средний срок службы, лет	Нет данных	Нет данных	Нет данных
Розничная цена, руб.	39 500	39 500	14 300

Модель IP-домофона	BEWARD DS06AP-3L	BEWARD DS06M	ACE-FA01
			
Производитель, сайт	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru	ACE, www.vidau-cctv.ru
Компания, предоставившая информацию, сайт	НПП "Бевард", www.beward.ru	НПП "Бевард", www.beward.ru	"ВИДАУ СБ", www.vidau-cctv.ru
Тип домофона	Однооабонентский	Однооабонентский	Интеллектуальный, на одну дверь, с распознаванием лиц
Голосовое дублирование действий пользователя	Нет	Нет	Да
Тип операционной системы домофона	Нет данных	Нет данных	Linux
Клавиатура	Механическая	Механическая	Монитор Touch Screen, 1200x600 пкс
Датчик приближения	Нет	Нет	Нет
Отдельная кнопка вызова консьержа	Нет	Нет	Да
Датчик вскрытия снятия панели	Нет	Нет	Да
Характеристики камеры	1/3", 1,3 Мпкс, 3,7 мм	1/3", 1,3 Мпкс, 3,7 мм	Две камеры по 2 Мпкс
Встроенный SIP-сервер	Нет	Нет	Нет
Количество поддерживаемых абонентов	3	3	10 000 лиц, 50 000 карт
Возможность регулировки встроенной камеры	Да	Да	Нет
Реле управления замком	Встроенное	Встроенное	Встроенное
Возможность управления двумя замками	Да	Нет	Нет
Поддерживаемые кодеки	H.264, MJPEG, G.711, G.726, дуплекс, эхоподавление	H.264, MJPEG, G.711, G.726, дуплекс	Режим онлайн, запись лиц в базу JPEG
Поддержка протоколов RTSP/ONVIF	Да	Да	Нет
Поддержка протокола SIP, TCP/IP	Да	Да	TCP/IP, FTP
Поддержка сигнала DTMF	Да	Да	Нет
Подсветка (LED/ИК)	ИК	ИК	Да
Дальность действия подсветки, м	10	10	1,5
Возможность прохода по цифровому коду	Нет	Нет	Да
Тип питания	12 В DC/PoE	12 В DC/PoE (опция)	12 В DC
Потребляемая мощность в состоянии покоя	Нет данных	Нет данных	30 мА
Потребляемая мощность в рабочем режиме	Нет данных	Нет данных	До 3 А
Степень защиты IP	IP54	IP54	IP66
Тип считывателя	Нет	Нет	Wiegand 26, Wiegand 34
Встроенный контроллер для карт	Нет	Нет	Да
Поддержка Wiegand 26	Нет	Нет	Да
Диапазон рабочих температур, °C	-40...+50	-40...+50	-20...+65
Тип установки	Накладной	Накладной	Врезная панель
Габаритные размеры, мм	73x166x51	73x166x51	330x140x45
Материал/цвет корпуса	Металл, черный/серый	Металл, черный/серый	Затемненное ударопрочное стекло, алюминий
Масса, кг	0,57	0,57	1,2
Средний срок службы, лет	Нет данных	Нет данных	5
Розничная цена, руб.	16 700	12 500	151 200

Модель IP-домофона	"Скрижаль"	"Скрижаль-мини" (приложение)	2N IP VERSO
			
Производитель, сайт	"Спецлаб", www.speclab.ru	"Спецлаб", www.speclab.ru	2N Telekomunikace, www.2n.cz
Компания, предоставившая информацию, сайт	"Спецлаб", www.speclab.ru	"Спецлаб", www.speclab.ru	2N Telekomunikace, www.2n.cz
Тип домофона	Одноабонентский	Одноабонентский	Одноабонентский, многоабонентский, модульный
Голосовое дублирование действий пользователя	Нет	Нет	Да
Тип операционной системы домофона	Windows 10	Android	Собственная
Клавиатура	Сенсорная	Сенсорная	Сенсорная/механическая/сенсорная комбинированная с RFID EM-Marine + MIFARE
Датчик приближения	Да	Да	Датчик движения
Отдельная кнопка вызова консьержа	Да	Да	Да
Датчик вскрытия снятия панели	Да	Да	Да
Характеристики камеры	4 камеры FullHD	Одна камера FullHD	1280x960 пкс, 2,25 мм
Встроенный SIP-сервер	Нет	Нет	Прямой SIP-вызов: UAC/UAS
Количество поддерживаемых абонентов	100	100	10 000
Возможность регулировки встроенной камеры	Да	Да	Разрешение камеры, цифровое PTZ
Реле управления замком	Да	Да	Встроенное/внешнее
Возможность управления двумя замками	Да	Да	Управление до 60 замками
Поддерживаемые кодеки	H.264, H.265, MJPEG	H.264, H.265, MJPEG	G.711, G.729, G.722, L16/16kHz, H.263+, H.263, H.264, MJPEG, MPEG-4
Поддержка протоколов RTSP/ONVIF	Да	Да	Да
Поддержка протокола SIP, TCP/IP	Да	Да	SIP 2.0 (RFC 3261), TCP/IP v4
Поддержка сигнала DTMF	Нет	Нет	Да
Подсветка (LED/ИК)	Да	Нет	ИК
Дальность действия подсветки, м	10	10	~2
Возможность прохода по цифровому коду	Да	Да	Да
Тип питания	PoE/DC/комбинированный	PoE/DC/комбинированный	PoE/DC/комбинированный
Потребляемая мощность в состоянии покоя	200 мА	200 мА	Макс. 2,124 В
Потребляемая мощность в рабочем режиме	350 мА	350 мА	Макс. 11,568 В
Степень защиты IP	Высшая	Высшая	IP54K, IK08
Тип считывателя	Идентификация лиц	Идентификация лиц	EM-Marine/MIFARE/HID iClass и др.
Встроенный контроллер для карт	Да	Да	Да
Поддержка Wiegand 26	Да	Нет	Да
Диапазон рабочих температур, °С	-40...+60	-40...+60	-40...+60
Тип установки	Накладной	Накладной	Врезной/накладной
Габаритные размеры, мм	Разные	Разные	107x234x28
Материал/цвет корпуса	Разные	Разные	Рама из цинка, цвет черный или никель
Масса, кг	0,23	0,230	Около 1,5 кг (в зависимости от использованных модулей и их количества)
Средний срок службы, лет	5 лет гарантии	Бессрочно	Нет данных
Розничная цена, руб.	24 000	Бесплатно	По запросу

DS-KH8520-WTE1	TI-2750WS	E21A	R20A
			
Hikvision, www.hikvision.ru	TRUE IP, www.true-ip.ru	Akuvox, www.akuvox.com, www.akuvox-rus.ru	Akuvox, www.akuvox.com, www.akuvox-rus.ru
DSSL, www.dssl.ru	DSSL, www.dssl.ru	InPrice Distribution, www.inprice.ru	InPrice Distribution, www.inprice.ru
Нет данных	Нет данных	Одноабонентский	Одноабонентский
Нет данных	Нет данных	Нет	Нет
Linux	Linux	Linux	Linux
Нет данных	Сенсорная	Механическая	Механическая
Нет данных	Нет данных	Нет	Нет
Нет данных	Нет данных	Нет	Нет
Нет данных	Нет данных	Да	Да
Нет данных	Нет данных	1,27", 2 Мпкс (1920x1080 пкс)	1/3", 3 Мпкс (1280x720 пкс)
Нет данных	Нет данных	Нет	Нет
Нет данных	Нет данных	До 10	До 10
Нет данных	Нет данных	Нет	Нет
Нет данных	Нет данных	Встроенное	Встроенное
Нет данных	Нет данных	Да	Да
G.711 U, 64 Кбит/с	H.264, 25/30 кадр/с, G711u	H.264, H.265, G.711a, G.711µ, G.729, G.722	H.264, G.711a, G.711µ, G.729 G.722
RTSP	RTSP	Да	Да
SIP, TCP/IP	SIP, TCP/IP	SIP v1 (RFC2543), SIP v2 (RFC3261), IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP	SIP v1 (RFC2543), SIP v2 (RFC3261), IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP
Нет данных	Да	Да, 3 вида in-band, out-of-band DTMF (RFC 2833), SIP Info	Да, 3 вида in-band, out-of-band DTMF (RFC 2833), SIP Info
Нет данных	Нет данных	ИК	ИК
Нет данных	Нет данных	2	~2
Нет данных	Нет данных	Нет	Нет
12 В DC, 1 А; PoE IEEE802.3af	12 В DC/пассивное PoE	PoE/DC	PoE/DC
Нет данных	<1,5 Вт	Нет данных	Нет данных
⩽6 Вт	<7 Вт	1000 мА	1000 мА
Нет данных	Нет данных	IP65	IP65
Нет данных	Нет данных	Нет данных	EM-Marine, MIFARE
Нет данных	Нет данных	Да	Да
Нет данных	Нет данных	Нет	Да
-10...+55	-10...+55	-20...+65	-20...+65
Накладной	Накладной	Накладной	Врезной/накладной (опционально)
195,8x132,8x17,5	200x136x24	210x120x61	145x85x27,5
PC + ABS, черный	Белый	Сталь, серый	Цинковый сплав, серый
0,66	0,46	0,842	0,573
Нет данных	Нет данных	5	5
25 990	20 990	24 300	14 200

Модель IP-домофона	R26B	R27A	R28A
			
Производитель, сайт	Akuvox, www.akuvox.com, www.akuvox-rus.ru	Akuvox, www.akuvox.com, www.akuvox-rus.ru	Akuvox, www.akuvox.com, www.akuvox-rus.ru
Компания, предоставившая информацию, сайт	InPrice Distribution, www.inprice.ru	InPrice Distribution, www.inprice.ru	InPrice Distribution, www.inprice.ru
Тип домофона	Многоабонентский	Многоабонентский	Многоабонентский
Голосовое дублирование действий пользователя	Нет	Нет	Нет
Тип операционной системы домофона	Linux	Linux	Linux
Клавиатура	Механическая	Механическая	Механическая
Датчик приближения	Нет	Нет	Да
Отдельная кнопка вызова консьержа	Нет	Да	Да
Датчик вскрытия снятия панели	Да	Да	Да
Характеристики камеры	1,27", 2 Мпкс, 1920x1080 пкс	1,27", 2 Мпкс, 1920x1080 пкс	1,27", 2 Мпкс, 1920x1080 пкс
Встроенный SIP-сервер	Нет	Нет	Нет
Количество поддерживаемых абонентов	До 15	Неограниченно	Неограниченно
Возможность регулировки встроенной камеры	Нет	Нет	Нет
Реле управления замком	Встроенное	Встроенное	Встроенное
Возможность управления двумя замками	Да	Да, тремя	Да, тремя
Поддерживаемые кодеки	H.264, H.265, G.711a, G.711μ, G.729, G.722	H.264, H.265, G.711a, G.711μ, G.729, G.722	H.264, H.265, G.711a, G.711μ, G.729, G.722
Поддержка протоколов RTSP/ONVIF	Да	Да	Да
Поддержка протокола SIP, TCP/IP	SIP v1 (RFC2543), SIP v2 (RFC3261), IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP	SIP v1 (RFC2543), SIP v2 (RFC3261), IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP	SIP v1 (RFC2543), SIP v2 (RFC3261), IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP
Поддержка сигнала DTMF	Да, 3 вида in-band, out-of-band DTMF (RFC 2833), SIP Info	Да, 3 вида in-band, out-of-band DTMF (RFC 2833), SIP Info	Да, 3 вида in-band, out-of-band DTMF (RFC 2833), SIP Info
Подсветка (LED/ИК)	ИК	ИК	ИК
Дальность действия подсветки, м	~2	~2	Нет данных
Возможность прохода по цифровому коду	Нет	Да	Да
Тип питания	PoE/DC	PoE/DC	PoE/DC
Потребляемая мощность в состоянии покоя	Нет данных	Нет данных	Нет данных
Потребляемая мощность в рабочем режиме	1000 мА	1000 мА	1000 мА
Степень защиты IP	IP65	IP65	IP65
Тип считывателя	EM-Marine, MIFARE	EM-Marine, MIFARE	EM-Marine, MIFARE
Встроенный контроллер для карт	Да	Да	Да
Поддержка Wiegand 26	Нет	Да	Да
Диапазон рабочих температур, °C	-20...+55	-40...+55	-40...+55
Тип установки	Накладной	Врезной/накладной (опционально)	Врезной/накладной (опционально)
Габаритные размеры, мм	196x110x39,5	280x130x68	280x130x68
Материал/цвет корпуса	Алюминиевый сплав, серый	Цинковый сплав, серый	Цинковый сплав, серый
Масса, кг	0,9	0,913	0,913
Средний срок службы, лет	5	5	5
Розничная цена, руб.	26 700	34 000	46 990

Модель IP-домофона	CIOT-L20M	CIOT-L7FM	MAJOR IP HOME KIT
			
Производитель, сайт	COMMAX, www.commax.com	COMMAX, www.commax.com	MAJOR SECURITY, www.major-security.ru
Компания, предоставившая информацию, сайт	IPDROM, www.ipdrom.ru	IPDROM, www.ipdrom.ru	MAJOR SECURITY, www.major-security.ru
Тип домофона	Многоабонентский	Многоабонентский	Модульный
Голосовое дублирование действий пользователя	Да	Да	Нет
Тип операционной системы домофона	Linux	Linux	Linux
Клавиатура	Механическая	Сенсорная	Сенсорная
Датчик приближения	Да	Да	Да
Отдельная кнопка вызова консьержа	Да	Да	Нет
Датчик вскрытия снятия панели	Нет	Нет	Нет
Характеристики камеры	2 Мпкс, обзор 120 град.	2 Мпкс, обзор 120 град.	2 Мпкс
Встроенный SIP-сервер	Нет	Нет	Да
Количество поддерживаемых абонентов	Нет данных	Нет данных	2
Возможность регулировки встроенной камеры	Да	Нет	Да
Реле управления замком	Да	Да	Встроенное
Возможность управления двумя замками	Нет	Нет	Нет
Поддерживаемые кодеки	H264/G.711	H264/G.711	H.265, H.264, MJPEG/G711-U, G711-A, PCM, G726
Поддержка протоколов RTSP/ONVIF	Нет	Нет	RTSP, ONVIF v.2.4, VPN, HTTP и др.
Поддержка протокола SIP, TCP/IP	TCP/IP	TCP/IP	SIP, TCP/IP
Поддержка сигнала DTMF	Нет	Нет	Да
Подсветка (LED/ИК)	LED	LED	ИК
Дальность действия подсветки, м	1	1	1,5
Возможность прохода по цифровому коду	Да	Да	Нет
Тип питания	DC	DC	Комбинированный
Потребляемая мощность в состоянии покоя	2,1 А	2,1 А	2 Вт
Потребляемая мощность в рабочем режиме	2,1 А	2,1 А	5 Вт
Степень защиты IP	IP54	IP54	IP64
Тип считывателя	RFID/BLE	RFID/BLE	Нет
Встроенный контроллер для карт	Да	Да	Нет
Поддержка Wiegand 26	Нет	Нет	Нет
Диапазон рабочих температур, °С	-40…+50	-40…+50	-10…+70
Тип установки	Врезной	Врезной	Накладной
Габаритные размеры, мм	210x240x81	210x130x45	180x272x25
Материал/цвет корпуса	Металл + пластик, серый	Металл + пластик, серый	Металл
Масса, кг	Нет данных	Нет данных	0,8
Средний срок службы, лет	10	10	10
Розничная цена, руб.	59 900	40 700	27 000

Организация СКУД и УРВ на стороне ERP и других систем

Зачастую решения, представленные на рынке СКУД, – это самодостаточные программные продукты, которые требуют соответствующих затрат: отдельный компьютер, отдельного сотрудника для ввода данных, отдельную базу данных, которую надо резервировать и т.д. В этой статье поговорим о том, как можно сократить такие издержки

Геннадий Демин
Руководитель ИТ-отдела
ЗАО НВП "Болид"

Как правило, на объектах, где внедряется СКУД, имеется множество разнообразных систем, содержащих одинаковые данные, например системы класса ERP со списком сотрудников, штатных подразделений, расчетом заработной платы, бухгалтерским учетом и т.д. В таких случаях возникает необходимость вносить одинаковые данные в разные системы и поддерживать их в одинаковом состоянии. Для упрощения подобных задач разработчики этих систем разрабатывают функционалы экспорта/импорта данных или интеграционные решения. Такие функционалы отвечают за перенос необходимых данных между системами, но в итоге получается несколько копий одних и тех же данных, которые разбросаны по разным местам. Среди них могут быть и персональные данные, хранение и обработку которых надо вести согласно федеральному закону № 152-ФЗ. Кроме того, с разными системами работают и разные люди/подразделения со своими представлениями о том, "как должно быть". Такое разнообразие систем на практике влечет за собой ощутимые затраты, которые неизбежно приведут к издержкам. Но их можно сократить!

Быстро, просто, без дублирования

Типовые СКУД состоят из аппаратной (считыватели, ограничители проходов, контроллеры доступа, источники питания и т.д.) и программной части в виде АРМ и имеют функционалы переноса данных между разными системами. Если с аппаратной частью ничего сделать нельзя, то программную можно перенести непосредственно в ERP-систему заказчика. Такой подход позволит избежать дублирования информации и всех сопутствующих затрат.

В компании "Болид" разработано простое, удобное и доступное решение, которое позволяет реализовать СКУД в существующей и работающей у клиента ERP-системе. Оно состоит из аппаратной части и библиотеки с набором API-функций для работы с аппаратной частью. Далее в ERP-системе настраивается вызов функций данной библиотеки.

Функционал "СКУД и УРВ для 1С:Предприятие".

В России и странах СНГ де-факто самой распространенной ERP-системой является "1С:Предприятие". Поэтому непосредственно для нее в плюс к указанной выше библиотеке был разработан клиентский интерфейс (в терминологии 1С – это внешняя обработка), который в 1С добавляет функционал управления и настройки функций СКУД. Данное решение получило название "СКУД и УРВ для 1С:Предприятие".
Его ключевые возможности:

- Использование штатных справочников подразделений и сотрудников из 1С.
- Контроль физического доступа на территорию (подключение турникетов/дверей/ворот/шлагбаумов для ограничения доступа). Возможен вариант подключения только считывателей без ограничения физического доступа (например, для задачи УРВ).
- Фотоверификация (отображение данных сотрудника и его фотографии в момент прохода).
- Подключение удаленных филиалов (требуется локальная сеть VPN).
- Открытый программный код (алгоритмы расчета рабочего времени и другие фрагменты кода являются открытыми, что позволяет разрабатывать свои отчеты и дорабатывать имеющийся функционал под свои нужды).
- Автономная работа (ключи записываются во все контроллеры доступа, которые подключены к резервированным источникам питания и могут работать без электричества и связи с компьютером, накапливая события проходов в своем буфере – до 64 тыс. событий на каждый контроллер).
- Организация централизованного доступа. Решение о предоставлении доступа принимает не аппаратный контроллер доступа автономно, а запрос отсылается в 1С и решение принимается на стороне ERP.
- Запись кодов ключей в контроллеры доступа из 1С (в качестве ключей используются идентификационные карты стандартов MIFARE и EM-Marin).
- Отображение состояния подключенных контроллеров доступа.
- Автоматический расчет отработанного времени.
- Автоматическое формирование табеля и данных для расчета зарплаты.
- Контроль посещаемости и отклонений от графика работы (опоздания, ранние уходы, переработки и т.д.).

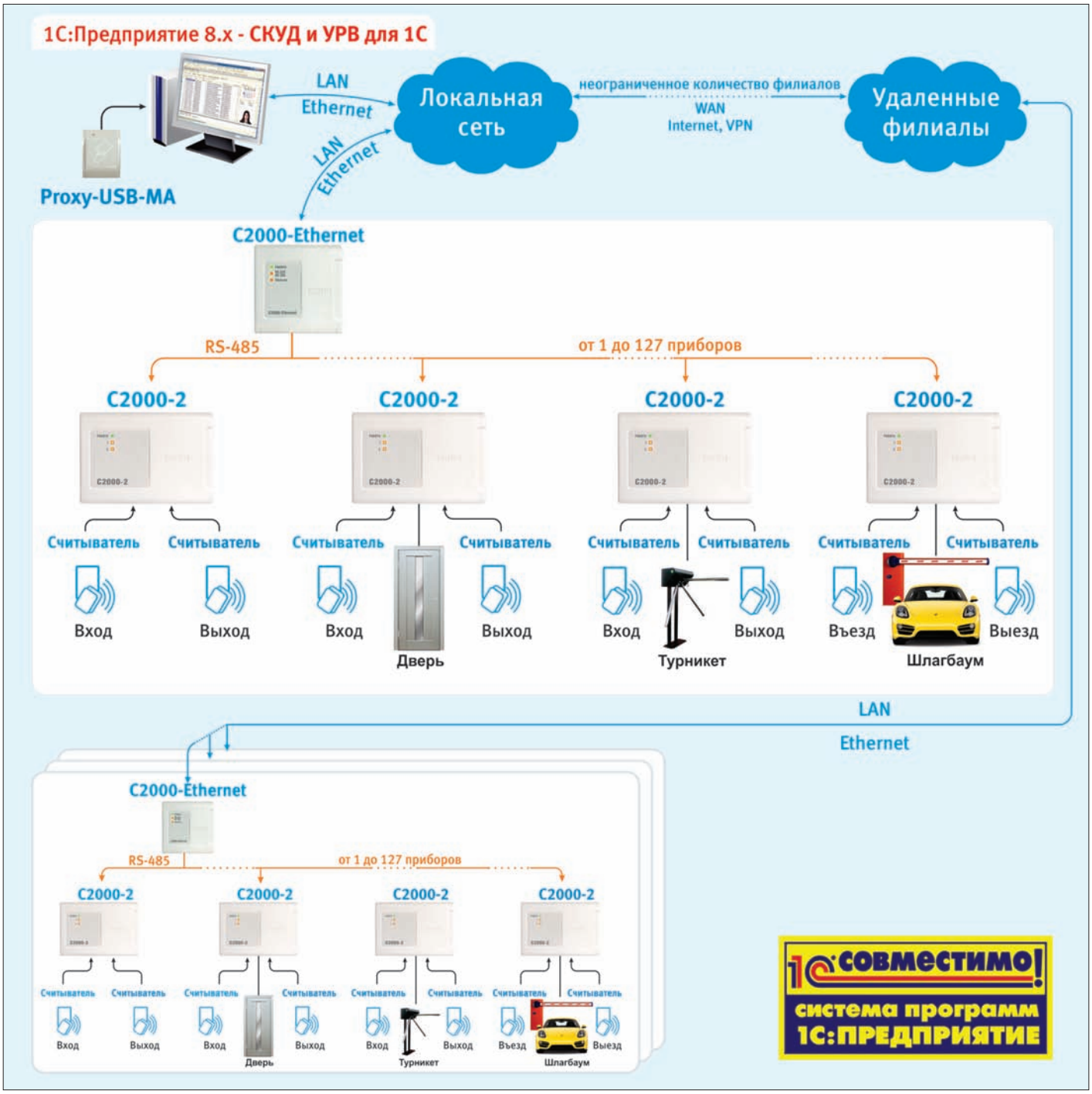
Пользователь на языке 1С может написать сценарий обработки запроса доступа, который вернет результат – разрешить/запретить (например, можно проверить факт оплаты парковки, остаток по депозиту на браслете и т.д.).
Пример пользовательского сценария указан на рис. 1.

```
// Пример пользовательского сценария
// обработки события "Инициатива управления (Запрос доступа)"

Access = Ложь; // изначально доступ запрещен

// Проверка существования считанного "кода ключа" в базе
МойОтбор = Новый Структура;
МойОтбор.Вставить("КодКлюча", KeyCode);
МассивКлючей = Ключи.НайтиСтроки(МойОтбор);
Если МассивКлючей.Количество() > 0 Тогда
    НайденныйКлюч = МассивКлючей[0]; // Ключ найден
    Если НайденныйКлюч.Доступ Тогда
        // Проверка факта оплаты
        Если КлиентОплатилСчет(НайденныйКлюч.Сотрудник) Тогда
            Access = Истина; // Доступ разрешен
        КонецЕсли;
    КонецЕсли;
КонецЕсли;
```

Рис. 1. Пример пользовательского сценария



Используя продукт "СКУД и УРВ для 1С:Предприятие", можно решать следующие задачи и комбинировать их между собой:
1. Контроль доступа.
2. Учет рабочего времени.
3. Автоматизация платных парковок, услуг с депозитным начислением, гостиничных услуг и т.д., где проход разрешен только после факта оплаты или выполнения другого условия.

Гибкость и интегрируемость

Используя продукт "СКУД и УРВ для 1С:Предприятие", можно решать следующие задачи и комбинировать их между собой:

1. Контроль доступа.
2. Учет рабочего времени.
3. Автоматизация платных парковок, услуг с депозитным начислением, гостиничных услуг и т.д., где проход разрешен только после факта оплаты или выполнения другого условия.

В случае централизованного доступа решение рекомендуется для объектов с невысокой интенсивностью проходов, где к одной точке доступа за 5–10 с не накопится очередь.

Имеется возможность интеграции с пожарными системами. В применяемом контроллере доступа "С2000-2" доступен вход, при замыкании которого замки, турникеты, ворота и шлагбаумы отпираются автоматически без участия АРМ.

Аналогичный пользовательский интерфейс создан и для ERP "Парус". Возможны разработки и под другие системы, включая облачные решения. ■

Подробно о решении:
https://bolid.ru/production/urv1c/urv1c8.html

Что принесет нам новый СКУД?

Использование мобильных устройств становится стандартом для новых установок в области контроля доступа. Решения по управлению мобильным доступом наряду с биометрией, облачными платформами и машинным обучением станут основным драйвером рынка СКУД в ближайшие годы. Поговорим о современных тенденциях в сфере управления доступом в новом, 2020 году

Сергей Гордеев
Региональный менеджер по продажам в России и СНГ компании HID Global

Все больше организаций стремятся предоставить своим пользователям новые возможности в безопасной среде с помощью так называемой цифровой взаимосвязи – открывать двери, проходить аутентификацию на корпоративных ресурсах или получать доступ к приложениям и сервисам здания через приложения для смартфонов. Все это требует подхода к защите от угроз, основанного на оценке рисков, поскольку компаниям требуется повысить производительность и обеспечить бесперебойный, более удобный доступ к своим физическим и цифровым активам. Сегодня все чаще можно видеть, как в вестибюлях, у турникетов, в лифтах люди пользуются новыми решениями для мобильного доступа, упрощающими перемещения по объектам и взаимодействие со службами интеллектуального здания.

Выпуск карт перемещается в облако

Процесс выпуска карты ранее требовал подключения компьютера к принтеру и использования его для дизайна идентификационной карты, доступа к базе данных идентификаторов для кодирования данных и последующей отправки карты на принтер. Современные облачные платформы позволяют выполнять весь процесс удаленно, а операции по безопасной выдаче – от проектирования и кодирования до печати – централизованно объединяются в интегрированную систему, к которой администратор может получить доступ в главном офисе, филиале или на другом удаленном объекте, используя планшет, ноутбук или любое устройство с веб-интерфейсом.

Пользователям при этом не нужно посещать главный офис и стоять в длинных очередях для получения идентификатора, а конфиденциальность обеспечивается благодаря сквозному шифрованию всех данных, как при проведении банковских операций.

Облачные модели разработки ускорят внедрение инноваций

Перенос решений по управлению доступом на облачные платформы дает возможность заменить разрозненные решения в области безопасности и оптимизации рабочих мест загружаемыми мобильными приложениями, поддержка которых осуществляется благодаря новым, более гибким моделям подписки. Например, при утере или замене смартфона выпуск мобильного идентификатора по подписной модели производится бесплатно. Облачная модель также сокращает путь от проектирования до развертывания решения, одновременно привлекая новых игроков в сообщество разработчиков. С облачными платформами больше не нужно разрабатывать целое решение и подключать только одного клиента или сайт одновременно, вместо этого такие системы позволяют разработчикам создавать новые приложения и интегрированные решения, которые работают с полной установленной базой миллионов устройств и систем контроля доступа.

Преобразование рабочих мест

Облачные решения для контроля доступа продолжат преобразовывать рабочие места. Имея только свои смартфоны, сотрудники здания и гости смогут открывать двери, просто поднося устройства к считывателю с помощью Near-Field Communications (NFC) или Bluetooth Low Energy (BLE). Для еще большего удобства функция Twist & Go благодаря повороту телефона дает возможность получать доступ на расстоянии, при приближении к считывателю. Пользовательский опыт дополнительно улучшается за счет интеграции в смартфон всех приложений – от парковки и виртуальной регистрации до широкого спектра других функций IoT.

Таким образом, используя возможности мобильных учетных данных и облака, организации могут создавать более интуитивно понятный интерфейс для своих пользователей, одновременно повышая безопасность.

Более широкое применение биометрии

Биометрическая аутентификация является одним из самых быстрорастущих сегментов на рынке управления доступом. Сегодняшние сканеры отпечатков пальцев получили возможность в режиме реального времени проверять подлинность отпечатков, в том числе их принадлежность живому человеку, и обнаруживать поддельные отпечатки. Новейшая технология мультиспектральной визуализации гарантирует высокую точность считывания вне зависимости от условий окружающей среды. Новые считыватели обеспечивают эффективность захвата изображений и сопоставление отпечатков пальцев в течение секунды, тем самым значительно сокращая задержки, которые раньше были постоянной проблемой биометрических решений.

Машинное обучение повышает уровень безопасности

Механизмы машинного обучения приобретают все более важное значение при получении ценной аналитики от современных решений контроля доступа, используемой в дальнейшем для повышения уровня безопасности. Продвинутая аналитика и интеллектуальный анализ на основе рисков будут применяться к важным данным, получаемым из устройств и приложений IoT, систем контроля доступа, цифровых сертификатов и решений для определения местоположения, подключенных к облаку. Включив этот тип аналитики в свои системы контроля доступа, организации повысят безопасность, персонализируют пользовательский опыт и будут принимать более эффективные бизнес-решения.

Идентификация людей и вещей

Одной из самых больших проблем сегодня является управление как физическими, так и цифровыми учетными данными, а также быстро растущим числом подключенных конечных точек в IoT. В то же время системы защиты от угроз физической и кибербезопасности продолжают совершенствоваться и становиться более комплексными. Поэтому одним из крайне важных трендов становится подтверждение личности людей и "вещей" в среде, где правила обеспечения безопасности и конфиденциальности данных продолжают становиться все более строгими.

Поддержка отраслевых стандартов

Прогресс отрасли будет затруднен, если организации станут разворачивать технологии контроля физического доступа (PACS), не поддерживающие отраслевые стандарты. Если инфраструктура организации продолжает развиваться, эти стандарты имеют решающее значение для устранения возникающих угроз, выявления уязвимостей и обновления протоколов безопасности, а также для обеспечения интеграции продуктов контроля доступа и решений для кибербезопасности. Поэтому поддержка индустриальных стандартов становится одной из важнейших тенденций современности в сфере контроля доступа. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Мастер-ключ от всех дверей

Согласитесь, не очень удобно иметь связку ключей, которая занимает место, много весит, может повредить сумку или карман. С этой проблемой сталкивается каждый как на работе, так и в быту. Ее позволяет решить так называемая мастер-система, или система "мастер-ключ". Это весьма удобное и экономичное решение для организации контроля доступа на базе цилиндровых механизмов

Реверсивный профиль ключа penta и английский профиль ключа pextra plus. Защищены патентом до 2032 г.

Мастер-систему рекомендуется использовать в жилых и складских помещениях, загородных домах, всевозможных офисных зданиях, государственных учреждениях, банках и др. А если такие системы собраны на надежных и секретных цилиндрах, например европейского производства dormakaba, то они не только обеспечат безопасность, но и помогут быстрому доступу в помещение при возникновении любой непредвиденной или чрезвычайной ситуации.

Внедрение системы "мастер-ключ" дома или на объекте позволяет:

- серьезно уменьшить количество носимых ключей на связке;
- сгруппировать двери или дверные замки по необходимости;
- снизить затраты на дальнейшую эксплуатацию двери или замка;
- обеспечить требуемую безопасность и сохранность имущества.

Неоспоримые преимущества

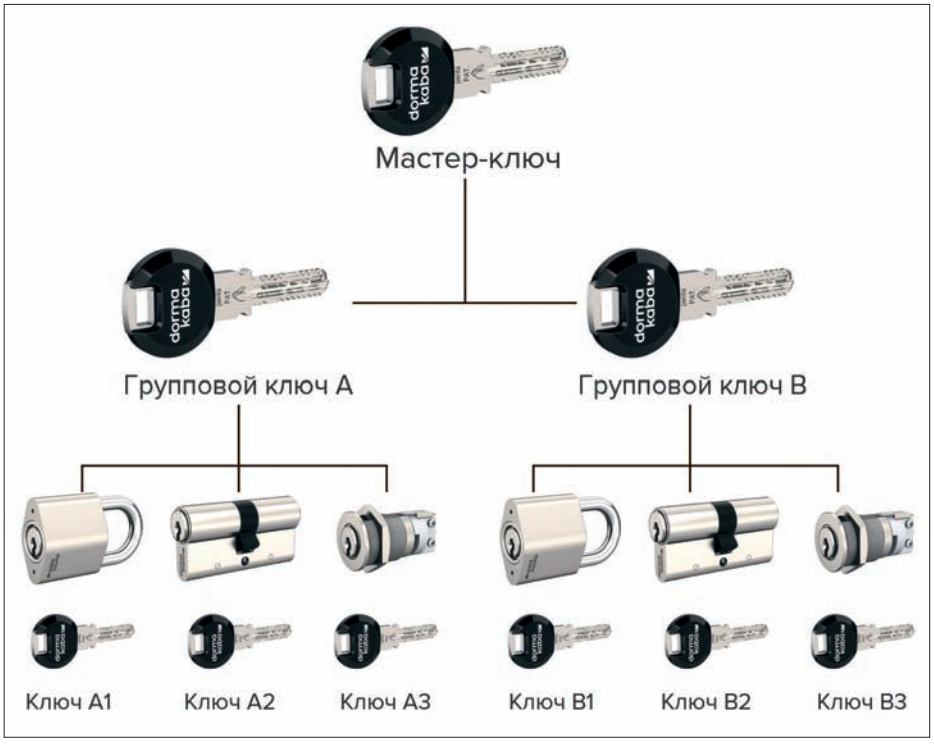
К основным плюсам системы "мастер-ключ" относятся:

1. Простота. Установка или замена цилиндрового механизма, как правило, не вызывает сложности у пользователя и не требует особых знаний и дорогого оборудования.
2. Удобство. Пользователь избавлен от больших и тяжелых связок ключей и получает возможность разграничить контроль доступа.
3. Экономичность. Нет переплаты за ключи, которыми не пользуются. При потере ключей есть возможность переборки мастер-системы специалистом, без необходимости ее замены. При расширении системы достаточно дозаказать необходимое количество цилиндров или ключей.
4. Надежность и безопасность. В случае чрезвычайной ситуации мастер-ключ может открыть все двери системы. Если в мастер-системе используются высокосекретные цилиндровые механизмы или ключи с индивидуальным профилем, то вскрытие таких замков или нелегальное изготовление дубликатов будет максимально затруднено.

Опции на любой вкус

Заказчикам предлагаются разные виды мастер-систем, в зависимости от необходимого функционала:

1. "Под один ключ". Все двери в помещении или на объекте могут быть открыты одним ключом. Например, им можно открыть все технические двери в здании или калитку + дверь в дом + гараж + почтовый ящик.
2. "С главным ключом". В этой системе к каждой двери идет свой индивидуальный ключ, а так называемый мастер-ключ, или главный ключ, может открыть все двери. Такая система позволяет владельцу компании иметь доступ во все помещения, а сотрудникам – только в те, где они работают.
3. "С центральным замком". Индивидуальный ключ может открыть только соответствующую дверь и центральную (например, входную). Такая система удобна для мини-гостиниц или при наличии тамбурной двери на этаже.
4. "Двухуровневая". Система, которая объединяет несколько групп дверей, имеющих индивидуальные ключи. В каждой группе имеется групповой мастер-ключ, открывающий входящие в нее двери, а также генеральный мастер-ключ, открывающий все двери системы. Это наиболее популярный вариант для крупных организаций, когда генеральный директор или начальник службы охраны имеет доступ во все помещения, руководители отделов – только в помещения своих отделов, а сотрудники – только к своим рабочим кабинетам.
5. "Многоуровневая". Любая сложная мастер-система с большим количеством групп и уровней контроля доступа.



Пример двухуровневой мастер-системы

Запатентованные технологии

Компания dormakaba создает мастер-системы любого уровня сложности на базе цилиндровых механизмов с запатентованным английским профилем ключа модели Pextra Plus и на запатентованным перфорированном профиле моделей Expert Plus и Penta. Секретность модели Penta достигает 867 трлн комбинаций, а количество цилиндров в мастер-системе, например с индивидуальными ключами и мастер-ключом, может составлять более 50 млн! Именно так полезное решение от dormakaba объединяет в себе удобство, экономичность, надежность и безопасность. ■

КОЛОНКА РЕДАКТОРА

Удобно государству, бизнесу, гражданину

Одним из самых ярких примеров внедрения биометрии для оказания финансовой помощи можно считать индийскую систему Aadhaar. Она предназначена для организации предоставления целенаправленных финансовых субсидий, а также других льгот и услуг. Aadhaar – это 12-значный уникальный идентификационный номер, который может быть получен добровольно жителями Индии на основе их биометрических и демографических данных.

Номер Aadhaar генерируется после сбора демографической информации и биометрии (отпечатки пальцев и сканирование радужной оболочки). Кроме аутентификации по отпечаткам пальцев, Aadhaar использует пять других методов аутентификации:

1. Соответствие числа Aadhaar и демографических атрибутов.
2. Одноразовый пароль, отправленный на мобильный номер или адрес электронной почты резидента, совместно используемый в центральной базе данных удостоверений.
3. Одну из биометрических модальностей – отпечатки пальцев или сканирование радужной оболочки глаза.
4. Двухфакторную аутентификацию с использованием биометрических данных (радужная оболочка глаза, отпечатки пальцев) и одноразовый пароль.
5. Одноразовый пароль, отпечатки пальцев и радужная оболочка глаза для аутентификации.

По состоянию на октябрь 2017 г. в Индии было зарегистрировано 1,18 млрд биометрических удостоверений личности.

Вероятностный характер биометрии не является препятствием для выдачи адресной помощи. Управляющий орган Aadhaar заявляет, что те люди, чья аутентификация не удалась, не будут лишены своих субсидий, поскольку вместо биометрической аутентификации определены альтернативные варианты выделения адресной помощи.

Другим примером новых вариантов использования биометрии является ее внедрение в услуги в аэропортах.

По данным компании Sita Air Transport IT Insights, в ближайшие три года (2019–2021 гг.) 77% аэропортов и 71% авиалиния начнут тестировать или внедрять биометрические системы досмотра. Распознавание лиц позволит проходить контроль всего за несколько секунд и избавит аэропорты от очередей. Системы распознавания лиц дадут возможность свободно перемещаться между зоной вылета и другими отделами аэропорта, а главное полностью искоренят очереди. Досмотр будет быстрым и для большинства пассажиров автоматическим.

Кроме аэропортов, проводятся попытки внедрить биометрию на другие объекты транспорта [1]. В Китае уже разработана и тестируется биометрическая технология оплаты за проезд на железнодорожном транспорте. С помощью новой технологии планируется просканировать лица сотен тысяч туристов, что позволит в случае необходимости обнаружить злоумышленника с вероятностью 99%. В некоторых китайских городах биометрические системы внедрены в жилые комплексы: для входа в свой подъезд достаточно "предъявить" свое лицо.

Активно развивается использование биометрии в торговле и ритейле. В 2018 г. Amazon открыла магазины с автоматизированной процедурой оплаты без присутствия кассира [2]. А компания Goode Intelligence подготовила отчет, в котором отмечается, что к 2023 г. 2,6 млрд человек будут пользоваться биометрическими платежами.

Технологию оплаты с помощью биометрических данных уже опробовали в "Азбуке вкуса", "Магните" и "Папе Джонсе", а Сбербанк приступил к разработке собственных терминалов с функцией распознавания лиц и отпечатков пальцев [3]. Пока это экспериментальные проекты; по мнению участников рынка, чтобы биометрия стала действительно массовым видом оплаты, нужно предложить пользователям расширенный функционал, а ритейлерам – возможность составлять детальный портрет покупателей.

Самыми активными в плане внедрения биометрических технологий остаются мобильные приложения. Например, для перевода денег в одной из самых популярных китайских платежных систем Alipay (более 120 млн пользователей) данные подтверждаются только сканированием лица покупателя.

Понимая значимость биометрии, Правительство России, крупные игроки рынка обращают самое пристальное внимание на внедрение биометрических технологий, ведь развитие их применения в различных областях может принести желаемый результат, а именно удобство предоставления услуг гражданам.

Список литературы

1. Биометрия на транспорте: для оплаты проезда "предъявите" лицо. https://infostart.ru/journal/news/tekhnologii/biometriya-na-transporte-dlya-oplaty-proezda-predyavite-litso_913107/
2. Биометрия в магазинах: вас приглашают платить лицом. https://www.e-xecutive.ru/management/sales/1991131-budet-li-vostrebovana-biometriya-v-magazinah
3. Предъявите ваше лицо. Крупнейшие ретейлеры тестируют оплату с помощью биометрии. https://www.dp.ru/a/2019/09/02/Predjavite_vashe_lico

Василий Мамаев
Редактор рубрики "Биометрические системы", заместитель директора некоммерческого партнерства "Русское биометрическое общество"

Александр Горшков
Директор по развитию компании Iris Devices – резидента Инновационного центра Сколково

По данным Our World in Data[1], в 2018 г. в мире было зафиксировано 282 сообщения о стихийных бедствиях, которые принесли ущерб в 107,77 млрд долларов. Государство и добровольцы собирают необходимые средства для оказания помощи пострадавшим от наводнений, лесных пожаров, ураганов и других стихийных бедствий. В то же время стремление некоторых граждан незаконно завладеть предоставляемой гуманитарной помощью приводит к совершению преступлений и обману с подменой личности. С 2005 г. в американский Национальный центр по борьбе с мошенничеством поступило более 95 тыс. обращений[2], связанных с правонарушениями в зоне стихийных бедствий. Разработанные на данный момент и широко внедряемые биометрические технологии идентификации личности могут помочь в борьбе с этим явлением.

Аутентификация личности для адресной помощи пострадавшим

Преступники направляют свою деятельность на людей в состоянии стресса и волнения. В таком состоянии находятся не только лица, пострадавшие от стихийных бедствий, но и сочувствующие им люди. Мошенники маскируются под жертвы стихийного бедствия или под физических или юридических лиц, ответственных за распределение помощи пострадавшим, чтобы получить материальную помощь, предназначенную для действительно нуждающихся людей. Было немало случаев, когда получившие гуманитарную помощь выбрасывали ее, поскольку она не представляла для них финансового интереса. У нас в стране это можно было наблюдать в Рязанской области[3], Приамурье[4], на Урале и в Сибири[5]. Развитие технологий способствует тому, что многие организации, занимающиеся оказанием помощи, в значительной степени начинают полагаться на использование цифровых и мобильных решений, которые, к сожалению, могут непреднамеренно создать

[1] *https://ourworldindata.org/natural-disasters*
[2] *https://www.justice.gov/disaster-fraud*
[3] *https://www.kp.ru/daily/24551.4/727697*
[4] *https://www.ntv.ru/novosti/2214821*
[5] *https://www.vesti.ru/doc.html?id=849245*

Биометрия – гарант адресной гуманитарной помощи пострадавшим от стихийных бедствий

Мошенничество и мародерство в районах, пострадавших от стихийных бедствий, является международной проблемой. Как можно решить ее с помощью биометрических технологий, рассмотрим в этой статье

Использование биометрии затрудняет проникновение мошенников в процесс разделения помощи

лазейки для правонарушений. При таком высоком уровне риска обмана необходимо обеспечить поддержание доверия между пострадавшими и организациями или частными лицами, оказывающими помощь.

Решением этой задачи может стать построение многоуровневого подхода для проверки и аутентификации личности пострадавших от стихийных бедствий и реально нуждающихся в помощи. Добавление нескольких уровней аутентификации затрудняет проникновение мошенников в процесс распределения помощи и укрепляет доверие между всеми субъектами, вовлеченными в этот процесс.

Установление доверия

Доверие является основой межличностных отношений, но сегодня оно стало редким явлением, поскольку современные цифровые технологии открыли новые возможности для мошенничества. В условиях хаоса и перемещения людей после стихийного бедствия создаются предпосылки для совершения различного рода преступлений, в том числе и связанных с кражей гуманитарной помощи. Наличие знания о том, кому предоставляется помощь, крайне важно, чтобы не прекратилось ее поступление из-за подозрений в нецелевом распределении.

Подтверждение личности жертвы стихийного бедствия – это первый уровень доверия между пострадавшими и вовлеченными в процесс оказания помощи организациями. При онлайн-взаимодействии анонимность пострадавших является большой угрозой и может стать настоящим препятствием, когда люди, желающие сделать пожертвования на борьбу с последствиями стихийных бедствий, не верят, что помощь будет оказана именно пострадавшим. В этом случае они могут отказаться от ее предоставления. Аналогичным образом, когда у организации нет возможности вовремя осуществить надлежащую проверку жертв стихийных бедствий, предоставление им финансовых и иных средств может задерживаться, а в некоторых случаях действительно нуждающиеся в поддержке могут так и не получить необходимую помощь.

Международная практика

Организация Объединенных Наций (ООН) в 2018 г. расширила использование биометрических данных при раздаче продуктов питания еще на восемь стран, в которых зарегистрировала биометрические признаки[6] у 2,4 млн беженцев. Использование биометрии предназначено для повышения уровня целостности данных о распределении гуманитарной помощи и контроля доступа к ней законных бенефициаров. В 2020 г. в рамках усилий по сокращению дублирования и расходов на управление биометрическая регистрация беженцев должна быть расширена и использоваться в 75 странах. Для надежной идентификации все возрастающего числа нуждающихся в получении гуманитарной помощи сотрудники ООН стали использовать биометрическую идентификацию по радужной оболочке глаз.

По данным ООН, в 2018 г. в Ираке насчитывалось более 120 тыс. семей и около 30 тыс. беженцев, которые получают денежную помощь через УВКБ (Управление Верховного комиссара Организации Объединенных Наций по делам беженцев). Управление выплатило нуждающимся через своих партнеров более 60 млн долларов. Процесс выплаты значительно упростился после начала использования технологии идентификации по радужной оболочке глаз, что сократило ожидание в процессе регистрации и предоставления средств. Биометрическая идентификация по радужной оболочке глаз позволяет легко и быстро осуществлять регистрацию человека в базе данных, а в дальнейшем идентифицировать его личность в течение трех секунд при любом количестве зарегистрированных в базе данных. Биометрическая идентификация по радужной оболочке глаз, в отличие от идентификации по лицу, не имеет предвзятости и одинаково точно идентифицирует людей различной национальности, мужчин, женщин, детей, лиц пожилого возраста.

Усилия ООН поддерживают многие страны. Так, правительство Эфиопии намерено пересмотреть свой механизм реагирования на гуманитарные инциденты, перейдя от бумажного к цифровому и биометрическому способу идентификации, и объединить свой подход к гуманитарным программам[7].

Особое внимание организации хранения и использования биометрических данных уделяют в ООН, как при оказании гуманитарной помощи, так и для борьбы с терроризмом. В организации подготовлен Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом[8]. В нем говорится о требованиях, касающихся управления, и нормативных требованиях к биометрической технологии с точки зрения международного права, стандартов в области прав человека, оценки соблюдения этических норм, требований к защите данных и права на неприкосновенность частной жизни. В документе представлен обзор потенциальных факторов уязвимости биометрических систем и некоторых мер контроля, которые можно применять для снижения этих рисков. Рассматриваются международные технические и технологические стандарты, касающиеся сертификации и аккредитации биометрических приложений, а также систем управления качеством, используемых при проведении экспертно-криминалистических процедур.

[6] *https://www.unhcr.org/excom/standcom/5d81f962d/76th-meeting-standing-committee-crp-23-grand-bargain-english.html*
[7] *https://insight.wfp.org/why-the-ethiopian-government-is-fingerprinting-the-residents-of-baladka-ef56f6c7b584*
[8] *https://www.un.org/sc/ctc/wp-content/uploads/2019/04/V1808431-Biometrics-Manual-RUSSIAN.pdf*

Многоуровневый подход

Разрушение инфраструктуры и депрессивное состояние пострадавших после стихийных бедствий создают условия для кражи как финансовых, так и идентификационных данных. В этих условиях многоуровневый подход является надежным решением для установления личности действительно нуждающихся в помощи. Многоуровневая проверка идентификаторов людей, пострадавших от стихийных бедствий, в сочетании с передовыми технологиями биометрической идентификации позволят обеспечить надежное подтверждение личности.

Опытный пользователь может без особых усилий вести бизнес в цифровой форме со своего телефона и при отсутствии многоуровневого подхода к идентификации. Но если мошенник украдет его телефон, то отсутствие многоуровневого подхода к идентификации сильно ограничит пострадавшего в возможности подтверждения его личности, в том числе для получения помощи. Используя украденный телефон, мошенник может получить помощь, выдавая себя за пострадавшего, при этом законный пользователь ничего не сможет с этим поделать. Напротив, при многоуровневом подходе граждане могут настроить свои учетные записи таким образом, что в случае отсутствия телефона они смогут подтвердить свои учетные данные другим способом, отличным от СМС, например с помощью распознавания лица, голоса или радужки. Такие биометрические идентификаторы мошенникам воспроизвести непросто, и в то же время они позволяют надежно различить двух людей, представляющих одни и те же внешне законные идентификационные данные. Что касается организаций, то использование многоуровневого подхода дает им возможность использовать биометрические идентификаторы своих сотрудников и комбинировать их с алгоритмами для проверки личности с помощью других методов.

Правительство Эфиопии намерено перейти от бумажного к цифровому и биометрическому способу идентификации в подходе к гуманитарным программам

Если биометрический идентификатор используется как единственный источник данных для распознавания, то вопрос их достоверности для обеспечения гарантированной адресной помощи вызывает опасения. Однако когда биометрическая характеристика накладывается на множество других данных для идентификации, то она становится не единственным фактором, влияющим на принятие решения об оказании помощи, а одной из частей системы безопасности. Помощь во время стихийного бедствия должна предоставляться как можно быстрее, и эти несколько уровней идентификации должны не только позволять быстро устанавливать личность, но и служить контрольными точками для надежного исключения возможного мошенничества и зависимости результата идентификации от человеческого фактора. Такое решение гарантирует, что предоставленные средства окажутся в руках тех, кто действительно в них нуждается.

Заключение

Современные технические решения изменяют методы оказания помощи в случае стихийных бедствий. Мобильные технологии упростили финансовые транзакции, но они также предоставили больше возможностей для несанкционированного доступа к ресурсам. К сожалению, там, где происходит катастрофа, есть и люди, которые хотят нажиться на этом. Внедрение многоуровневого подхода для создания надежной системы безопасности с многочисленными точками контроля и идентификации личности позволит обеспечить бесперебойное распределение помощи среди нуждающихся в ней. Главное, что этот метод обеспечивает гарантированную помощь пострадавшим, когда коммерческие и гуманитарные организации сталкиваются с повышенным риском хищения выделенной помощи из-за неверной идентификации личности. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

КОЛОНКА РЕДАКТОРА

Перспективы "пожарной" страховки

На прошедшем в феврале международном форуме "Технологии безопасности" наше внимание привлекла конференция "Пожарная безопасность объектов с массовым пребыванием людей". В ее рамках обсуждались занимающие многих заинтересованных экспертов вопросы реализации механизма "регуляторной гильотины" в области пожарной безопасности и новой концепции страхования ответственности объектов с массовым пребыванием людей.

Вопрос введения обязательного в том или ином виде страхования пожарной ответственности собственника объекта стоит на повестке дня уже давно.

Приводятся два очевидных аргумента "за". Первый – необходимость создания реально работающих механизмов компенсации пострадавшим в результате пожаров на объекте. По мнению представителей страховщиков, сегодня бизнес не чувствует материальную ответственность за последствия пожара перед находящимися на его территории посетителями. Вопросы о возмещении вреда решаются в рамках Гражданского кодекса, только через судебную стадию, с необходимостью сбора и предоставления подтверждающих затраты документов. Таким образом, по оценке экспертов, только около 10% наиболее "упертых", юридически грамотных или имеющих средства на юридическую поддержку людей получают компенсации от собственников объектов. Второй аргумент – необходимость повышения эффективности пожарного надзора за счет привлечения к нему материально заинтересованных в повышении уровня безопасности объектов представителей страховых компаний. Это соответствует провозглашенному принципу "регуляторной гильотины" в части снижения административного давления на бизнес со стороны государственных структур. По этому пути пошли все страны развитого капитализма, и там он доказал свою эффективность.

Но ввести обязательное страхование ответственности, оказывается, не так просто. Согласно концепции развития страхового рынка, утвержденной правительством, в России не планируется введение новых обязательных видов страхования. Кроме того, обязательное страхование становится неудобным для самих страховщиков из-за сильной зарегулированности, в том числе в вопросах тарифов. Поэтому рассматривается вариант принятия изменений Технического регламента о требованиях пожарной безопасности, которыми устанавливается обязанность собственника объекта по возмещению вреда потерпевшим независимо от его вины. В результате пострадавшим не надо будет ждать установления виновника пожара, возмещение вреда будет происходить быстрее и в полном объеме. Для обеспечения этого процесса предлагается использовать механизм добровольного страхования ответственности. При этом для собственника предусмотрены "кнут и пряник": право пожарному надзору проводить внеплановые проверки объектов, не имеющих полисов, и возможность отнесения собственником объекта расходов на страхование на себестоимость. Отсутствие полиса не предполагает автоматический запрет на осуществление деятельности объекта.

Для осуществления представителями страховых компаний проверки объектов Всероссийский союз страховщиков (ВСС) совместно с МЧС разработает максимально простые чек-листы (методики проверки защищенности). Считается, что человек без специального образования вполне способен измерить ширину путей эвакуации, оценить работоспособность пожарной сигнализации и автоматики (сработала или нет при тестовом воздействии).

Концепция страхования ответственности в отношении объектов с массовым пребыванием людей была одобрена президиумом ВСС в конце ноября 2019 г. Следующим этапом должно стать согласование концепции с Экспертным советом по законодательству о страховании при Комитете Государственной Думы по финансовому рынку

В перспективе ВСС считает целесообразным создание собственного техцентра для оценки качества оборудования и материалов, применяемых для противопожарной защиты. Такие центры действуют в Германии и других странах. Собственник, использующий продукцию, прошедшую подобную добровольную сертификацию, получает определенную выгоду при оформлении полисов. Однако на этом этапе возможные затраты на создание данного института пугают представителей страховых компаний: непонятно, за чей счет он должен создаваться. Примечательно, что запрос на создание такого центра уже давно наблюдается со стороны производителей качественной техники.

Концепция страхования ответственности в отношении объектов с массовым пребыванием людей была одобрена президиумом ВСС в конце ноября 2019 г. Следующим этапом должно стать согласование концепции с Экспертным советом по законодательству о страховании при Комитете Государственной Думы по финансовому рынку.

Все описанные начинания можно только приветствовать. Но есть сомнения, не повторит ли эта система страхования судьбу ОСАГО и связанного с ним либерализованного техосмотра автотранспорта. Остается надеяться, что продажа "пожарных" полисов не будет определяться только рыночными механизмами и конкуренцией между страховыми компаниями. ■

Максим Горяченков
Редактор раздела
"ОПС, пожарная безопасность",
руководитель отдела технической
поддержки ЗАО НВП "Болид"

Оповестить – значит предотвратить панику

С 14 по 17 февраля 2020 г. на санно-бобслейной трассе в Сочи запланировано проведение чемпионата мира – 2020 по санному спорту. Это событие привлекает не только огромное количество спортсменов со всего мира, но и их болельщиков. В соответствии с проектной документацией санно-бобслейная трасса в Сочи может вмещать до 11 тыс. зрителей, а значит встает резонный вопрос о готовности владельцев трассы и организаторов соревнований в случае чрезвычайных обстоятельств к оповещению зрителей и спортсменов, говорящих на разных языках, и их безопасной и оперативной эвакуации. При этом нужно помнить о людях с ограниченными физическими возможностями, в первую очередь с нарушением органов слуха, к оповещению которых необходимо подходить индивидуально, и маломобильных группах населения, эвакуация которых без посторонней помощи невозможна

Вячеслав Палащенко
Начальник отдела охраны труда, промышленной безопасности, ГО и ЧС филиала ФГБУ "Центр спортивной подготовки сборных команд России" в г. Сочи (центр санного спорта "Санки")

Павел Казаков
Начальник отдела обслуживания слаботочного оборудования, КИПиА и систем пожарной безопасности филиала ФГБУ "Центр спортивной подготовки сборных команд России" в г. Сочи (центр санного спорта "Санки")

Если русский или английский язык не является для спортсменов родным, оповестить их о чрезвычайной ситуации и порядке действий особенно нелегко

Как было упомянуто в статье "Оповещение и управление эвакуацией в торговых центрах. Взгляд профессионального посетителя" (журнал "Системы безопасности" № 6/2019, стр. 60–61), одна из самых больших проблем при организации оповещения и эвакуации – это паника. Она возникает в тех случаях, когда человек не знает элементарных правил поведения в возникшей ситуации по причине слабой подготовки в школах, на рабочих местах и т.д. Психофизиологический механизм паники заключается в торможении больших участков коры головного мозга, что предопределяет понижение сознательной активности.

Довести до нескольких тысяч гостей и спортсменов, для части которых русский и английский языки не являются родными, информацию о чрезвычайной ситуации и порядке действий особенно нелегко.

Для организации полноценного оповещения всех посетителей, находящихся на спортивном объекте, предлагается разбить задачу оповещения на несколько подзадач:

1. Оповещение русско- и англоговорящих посетителей и спортсменов.
2. Оповещение посетителей и спортсменов, для которых русский и английский языки не являются родными.
3. Оповещение посетителей с нарушением функций слуха.

Оповещение русско- и англоговорящих посетителей и спортсменов

Санно-бобслейная трасса в Сочи была построена к зимней Олимпиаде 2014 г. Системы безопасности, а именно система оповещения и управления эвакуацией и локальная система оповещения, были созданы на базе современных технических средств, позволяющих в полной мере осуществлять оповещение и управление эвакуацией на русском и английском языках в соответствии с требованиями нормативно-правовых актов как в автоматическом, так и в дистанционном и ручном режимах. Дополнительно для оповещения могут использоваться ручные громкоговорители, которые на время проведения соревнований находятся у старших специалистов по безопасности на каждом участке нахождения гостей.

Оповещение посетителей и спортсменов, для которых русский и английский языки не являются родными

На чемпионате мира по санному спорту в феврале 2020 г. ожидается участие 20 команд со всего мира, а значит и приезд болельщиков из 20 стран мира. Перечень стран-участников заранее известен, поэтому подготовиться по вопросам безопасности также не составит большого труда. Экспериментально разработан буклет для спортсменов и участников из каждой страны, в котором вкратце описаны требования безопасности и обозначение сценариев оповещения. К примеру, если болельщик китайской команды услышит повторяющееся сообщение на русском

языке "Внимание! Граждане! Произошла авария с выбросом опасного химического вещества. Распространяется облако зараженного воздуха", в буклете есть перевод этого сообщения на китайский язык, а также порядок действий для каждого конкретного случая.

Оповещение посетителей с нарушением функций слуха

Одна из важнейших задач государства – реализация прав людей с ограниченными возможностями наравне со всеми. Данный тезис прописан в Конвенции ООН "О правах инвалидов", которая была ратифицирована Россией в 2012 г. Поэтому на различные мероприятия, в том числе и спортивные, в последнее время приглашают большое количество гостей с ограниченными возможностями. Одновременно с этим возникает вопрос обеспечения безопасности указанной категории граждан. Оповещение посетителей с нарушением функций слуха является наиболее сложной задачей, так как четких решений в открытом доступе найдено не было, а технические средства коммуникаций людей с нарушением функций слуха в основном являются стационарными, применяемыми для обучения.

На наш взгляд, для решения этой задачи возможно комплексное организационно-техническое решение. В первую очередь для посетителей с нарушениями органов слуха наиболее приемлемым и удобным является получение видеоинформации. Во всех местах размещения зрителей во время проведения соревнований на санно-бобслейной трассе в Сочи расположены экраны, позволяющие организовать доведение экстренной информации с рабочего места

Для посетителей с нарушением органов слуха информацию об оповещении донесут волонтеры с помощью языка жестов

оператора аудиовизуальных систем. Для оперативного доведения информации подготовлены слайдовые сообщения с описанием оповещения и отдельные слайдовые сообщения с описанием порядка действий. При необходимости оператор аудиовизуальных систем, получив от комиссии филиала по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности или от диспетчера информацию о произошедшей чрезвычайной ситуации и порядке действий, сможет подкорректировать подготовленный визуальный материал и оперативно вывести его на все экраны.

Но этого тоже может быть недостаточно. Поэтому для оповещения посетителей с нарушениями органов слуха на каждом участке нахождения гостей планируется размещение волонтеров, владеющих языком жестов. При получении информации по любой из имеющихся систем оповещения или радиосети волонтеры будут транслировать ее на языке жестов посетителям с нарушением органов слуха и далее сопровождать их при эвакуации.

Подготовка на всех уровнях

Организация оповещения гостей и спортсменов в случае возникновения чрезвычайной ситуации во время проведения соревнований требует очень чуткого, планового и досконального подхода. Важно взаимодействие со Всероссийским обществом инвалидов и, в частности, со Всероссийским обществом глухих, чтобы все проводимые мероприятия были апробированы до возможной чрезвычайной ситуации.

Тщательная подготовка к проводимому чемпионату мира позволит не только устроить зрелищное соперничество на высоких скоростях, но и обеспечить сохранность жизни и здоровья людей в случае возникновения чрезвычайных ситуаций. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Противокриминальная защита современных остекленных конструкций: комплексный подход

Остекленные строительные конструкции – окна, двери, крыши, перегородки, витрины, витражи – являются наиболее уязвимыми для проникновения нарушителей в охраняемые здания и помещения. Это не остается незамеченным преступниками, и наибольшее число проникновений происходит именно через оконные конструкции и балконные двери. В статье приведен обзор современных специализированных технических средств для обнаружения попытки взлома остекленных конструкций, проанализирована их эффективность и предложены идеи разработки решений для повышения надежности защиты

Дмитрий Прошутинский
Старший научный сотрудник ФКУ
НИЦ "Охрана" Росгвардии

Михаил Пермяков
Научный сотрудник ФКУ
НИЦ "Охрана" Росгвардии

Сергей Сухих
Инженер ФКУ
НИЦ "Охрана" Росгвардии

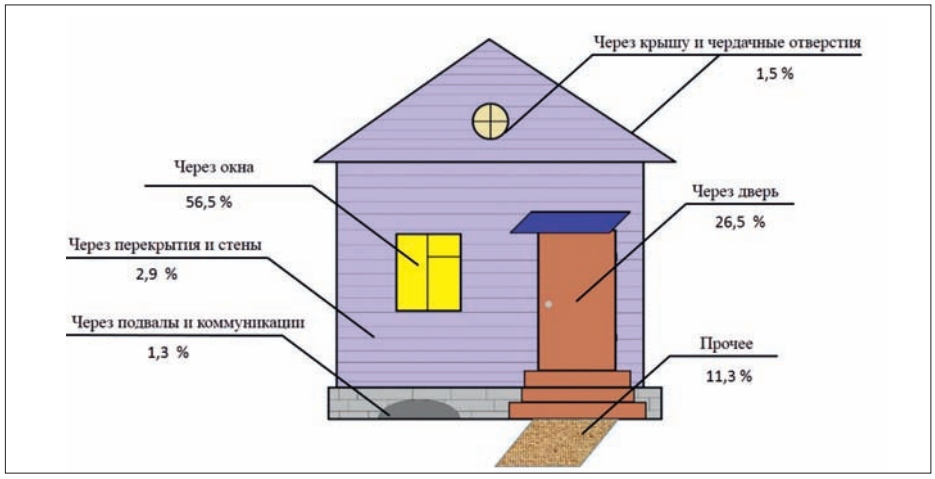


Рис. 1. Способы проникновения в помещение

Наиболее распространенный и простой способ взлома, в том числе алюминиевого или пластикового окна, – это разбитие стекла. Его легко осуществить с помощью подручных предметов или свободно продаваемых компактных стеклорезов.

Часто преступниками используются кирпич, булыжник, тротуарная плитка, кусок трубы или любой другой твердый предмет массой от 0,1 кг. Разрушение стекла производится путем метания твердого предмета в оконный проем. Однако, несмотря на быстрое разбитие окна, после такого взлома нарушителю может понадобиться еще время (от нескольких секунд до нескольких минут) для удаления осколков стекол, оставшихся в створке.

Традиционные способы защиты при разбитии стекла

До недавнего времени обнаружение попытки взлома окон осуществлялось в основном с помощью контактных датчиков, приклеиваемых на стекло и обнаруживающих его разбитие, – электроконтактных и ударноконтактных извещателей. Использование таких датчиков ("Фольга", ДИМК "Окно", "Орбита" и т.д.) было сопряжено с определенными неудобствами, в том числе связанными с нарушением внешнего вида окна, регулярными повреждениями при мытье стекол и т.д.

Датчик "ДРС-2", созданный для решения части этих проблем, к сожалению, в серию не пошел. На рис. 2 представлен извещатель "Окно-6" с датчиком разбития стекла "ДРС-1".

В конце 1990-х гг. начали активно развиваться и применяться на охраняемых объектах бесконтактные акустические извещатели, реагирующие на звук разбиваемого стекла. Но они позволяют гарантированно обнаружить нарушителя только при механическом разбитии стекла ударным воздействием. Детально их особенности рассмотрены в статье "Противокриминальная защита остекленных конструкций"[1]. Внешний вид звукового извещателя "Стекло-4" представлен на рис. 3.

Со временем звуковые извещатели, отличающиеся рядом преимуществ по надежности, поме-

Рис. 2. Точечный ударноконтактный охранный извещатель "Окно-6" с датчиком разбития стекла "ДРС-1"

Рис. 3. Звуковой поверхностный охранной извещатель "Стекло-4"

1 Климов А.В., Рябцев Н.А., Козлов В.А. Противокриминальная защита остекленных конструкций // Алгоритм безопасности. 2015. № 4. С. 6–9.

хоустойчивости, дизайну, простоте монтажа и обслуживания, практически полностью вытеснили устройства других типов и сегодня повсеместно используются для защиты объектов.

Взлом оконных конструкций без разбития стекла

Методы совершения преступлений развиваются, и в последние годы злоумышленники, зная о том, что в охраняемых помещениях, как правило, устанавливаются звуковые извещатели, все чаще начинают применять иные способы проникновения через оконные конструкции. Так, на шесть краж, осуществленных путем разбития стекла, приходится одна совершенная без его разбития.

Взлом пластикового (алюминиевого) окна производится с помощью монтировки/лома методом отжимания открывающейся створки окна или выламывания оконной рамы из оконного проема. Данный способ требует больше времени, но позволяет сохранить в целости стеклопакет, что маскирует процесс проникновения в помещение. Современные оконные конструкции особенно уязвимы к подобному виду взлома, если створка окна находится в положении проветривания.

Установка на створку магнитоконтактного извещателя не обеспечивает контроль состояния самого запорного механизма оконной конструкции и не позволяет своевременно, до проникновения нарушителя внутрь объекта, обнаружить попытку высверливания запорного механизма или предварительное открытие конструкции изнутри преступником или его сообщником.

Взлом окна с применением режущих и пилящих инструментов (например, болгарки) заключается в выпиливании стекла из створки окна по периметру. Это наиболее продолжительный по времени, сложный в исполнении и, соответственно, редкий способ взлома оконных конструкций.

Для всех способов их взлома актуальна проблема, состоящая в том, что преступники зачастую нацеливаются на совершение кражи "на рывок", успевая покинуть охраняемый объект до прибытия сил реагирования.

Средства инженерно-технической укрепленности

Для защиты остекленных конструкций применяют средства инженерно-технической укрепленности, которые затрудняют проникновение в дом путем силового воздействия: решетки, ставни, роллеты. К сожалению, подобные решения редко оснащаются техническими средствами охраны и по большей части нарушитель их преодолевает, а извещение о тревоге не формируется. Поэтому такие средства инженерно-технической укрепленности способны лишь задержать нарушителя вне охраняемого помещения, что, конечно, немаловажно, но не являются достаточной защитой от мотивированного подготовленного злоумышленника.

В ряде случаев применение средств инженерной-технической укрепленности оконной конструкции ограничено либо из эстетических соображений, либо нормами противопожарной безопасности.

Таким образом, к защите современных остекленных конструкций необходимо подходить комплексно, как внедряя средства обнаружения, так и повышая инженерно-техническую укрепленность установленного стеклопакета, что позволяет обеспечить раннее обнаружение проникновения.

Выход – раннее обнаружение

Проведя анализ и руководствуясь подходом, определенным ГОСТ Р 50776–95[2] и описанным в статье "Методика оценки эффективности системы безопасности объектов дистанционного банковского обслуживания"[3], получаем критерий эффективности системы охраны: разницу между временем взлома оконной конструкции и проникновения нарушителя в охраняемое помещение и сумму времени, необходимого для обнаружения системой централизованного наблюдения (СЦН) попытки проникновения, передачи извещения на пульт централизованного наблюдения (ПЦН) и прибытия сил реагирования.

Следует отметить, что время взлома оконной конструкции и скорость проникновения нарушителя в охраняемое помещение может быть неодинаковой для разных способов взлома, выбранных нарушителем.

Для СЦН, применяемых в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации и занимающих значительную долю рынка технических средств охраны, время, необходимое для передачи тревожного извещения на ПЦН, жестко задается Едиными требованиями 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[4], и составляет 15 с. Это на порядок меньше среднего времени прибытия сил реагирования после поступления тревожного извещения на ПЦН.

Из вышесказанного видно, что эффективность системы охраны при невозможности изменения скорости прибытия сил реагирования в первую очередь зависит от возможности раннего обнаружения криминального воздействия, которое определяется разницей между временем наиболее быстрого способа взлома и проникновения нарушителя на объект и временем обнаружения взлома техническими средствами охраны.

Важнейшим фактором становится время сохранения устойчивости оконной конструкции после формирования техническими средствами обнаружения извещения о проникновении нарушителя.

Недостатки обычных методов защиты

Рассмотрим наиболее распространенные способы охраны оконной конструкции.

1. Обеспечение защиты оконной конструкции при помощи пассивного оптико-электронного извещателя с поверхностной зоной обнаружения (рис. 4), установленного над оконным проемом с внутренней стороны объекта охраны.

В этом случае нарушитель попадает в зону обнаружения извещателя уже после проникновения в охраняемое помещение, и тревожная ситуация характеризуется максимально возможным временем на совершение правонарушения и попытку скрыться с места преступления. По этой причине применение данного способа охраны объекта в качестве основного не рекомендуется.

2. Наиболее распространенный способ – обеспечение защиты оконной конструкции с помощью пассивного звукового извещателя. Извещение о тревоге гарантированно формируется звуковым охранным извещателем при разрушении внутреннего стекла стеклопакета. В этом случае обнаружение проникновения не соответствует вышеописанному критерию и не является ранним в связи с тем, что на передачу извещения о тревоге и прибытие сил реагирования, как правило, требуется значительно большее время, чем необходимо нарушителю для проникновения на объект уже после взлома всех средств инженерно-технической укрепленности.

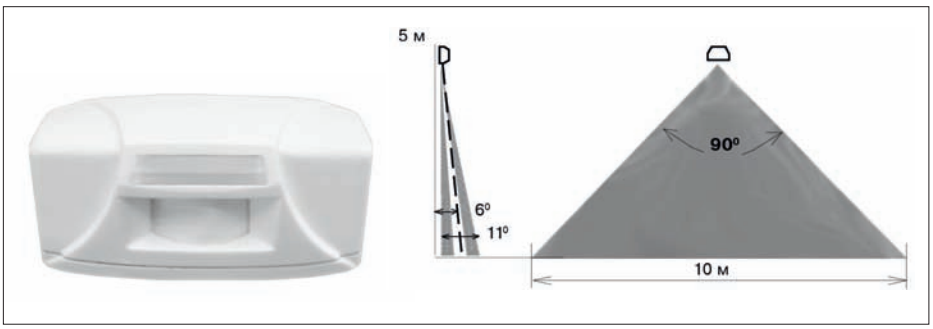


Рис. 4. Поверхностный оптико-электронный охранный извещатель "Фотон-Ш2"

[2] ГОСТ Р 50776–95. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

[3] Членов А.Н., Климов А.В. Методика оценки эффективности системы безопасности объектов дистанционного банковского обслуживания // Технологии техносферной безопасности. 2015. Вып. 2 (60). С. 205–211. https://academygps.ru/ttb

[4] Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации (утв. ГУВО Росгвардии 13.12.2019).

По результатам анализа применения технических средств охраны остекленных конструкций можно сделать следующие выводы:

1. Ни один из представленных на рынке типов технических средств охраны не способен обеспечить раннее обнаружение попытки воздействия (взлом, разрушение оконной рамы и/или стеклопакета, открывание).

2. Установка на стеклопакет ряда технических средств охраны, обеспечивающих максимальную эффективность, связана с серьезным нарушением конструкции стеклопакета и большим объемом монтажных работ.

Какой же комплекс технических средств защиты оконных конструкций будет наиболее эффективным?

Перспективное комплексное решение

Кроме внешних средств инженерно-технической укрепленности, конструкция стеклопакетов и их фурнитуры может включать в себя специальные стекла (противоударные, противовзломные, пуленепробиваемые), оконные замки повышенной устойчивости к физическим воздействиям, противовзломную фурнитуру, защитные пленки и специальные штапики, предотвращающие выдавливание стекла. Применение подобных технических решений позволяет максимально увеличить время сохранения устойчивости оконной конструкции после формирования техническими средствами обнаружения извещения о проникновении.

Функциональный состав комплекса, способного обеспечить обнаружение попытки взлома остекленных конструкций, используя структуру, приведенную в ГОСТ 56102.1–2014[5], и результаты поиска вариантов построения каналов обнаружения, обеспечивающих защиту от вышеприведенных способов взлома оконных конструкций, можно представить следующим образом:

- средства обнаружения, обеспечивающие обнаружение попытки взлома оконной конструкции при помощи блока обработки сигнала (БОС) информации, получаемой с чувствительного элемента (ЧЭ);
- средство сбора и обработки информации (ССОИ);
- вспомогательные средства защиты от саботажа (СЗС);
- модуль электропитания.

СЗС обеспечивают защиту комплекса от несанкционированных воздействий, которые могут привести к потере работоспособности, и представляют собой отдельные датчики, контролирующие закрытое состояние ниш оконной конструкции, в которых установлены элементы комплекса обнаружения взлома.

ССОИ осуществляют контроль работоспособности и диагностику модулей комплекса, сбор информации о тревожных событиях, формирование извещений о тревоге по стандартным проводным и/или беспроводным интерфейсам. Структура комплекса изображена на рис. 5.

Основные функции комплекса

На основании анализа информации о способах криминальных воздействий на остекленные конструкции комплекс должен обеспечить обнаружение следующих криминальных воздействий:

- разбитие стекла при помощи механического воздействия или нагрева;
- вскрытие окна путем разрушения запорного механизма при помощи сверлильного инструмента;
- отжим створки окна при помощи рычажного или гидравлического инструмента;
- разрушение створки при помощи электрорежущего инструмента (сабельной пилы, болгарки);
- извлечение рамы из проема при помощи рычажного или гидравлического инструмента.

Исходя из анализа информации о возможностях ЧЭ, использующих различные физические принципы и результаты экспериментальных исследований, можно выбрать варианты состава комплекса специализированных технических средств, обеспечивающих обнаружение попытки взлома остекленных конструкций.

ЧЭ, предназначенные для формирования модуля средств обнаружения проникновения, могут быть следующими:

1. Ударно-контактные, емкостные, электроконтактные, звуковые, вибрационные ЧЭ (на основе пьезоэлемента или акселерометра) для обнаружения попытки взлома полотна стекла способом разбития.

2. ЧЭ на основе пьезоэлемента, обладающего более широким частотным диапазоном, или акселерометра, для обнаружения попытки взлома путем воздействия сверлильного инструмента на запорный механизм или разрушения створки при помощи электрорежущего инструмента (сабельной пилы, болгарки).

3. Точечный магнитоконтактный, магнитоуправляемый извещатель или извещатель на основе акселерометра, определяющего изменение угла наклона охраняемой конструкции, для обнаружения попытки взлома от отжима створки окна при помощи рычажного или гидравлического инструмента.

4. Для обнаружения попытки взлома от извлечения рамы из проема при помощи рычажного или гидравлического инструмента требуется или сложная установка магнитоконтактных извещателей в раму остекленной конструкции и стену здания, или применение акселерометра.

Пути оптимизации

Прежде всего требуется учитывать необходимость минимизировать габариты, энергопотребление и стоимость соответствующего комплекса. Для этого целесообразно ряд элементов конструктивно объединить в единый блок.

Электропитание

ССОИ и модуль электропитания комплекса могут быть выполнены в отдельном корпусе (корпусах), однако в рассматриваемом случае стоит разместить все возможные функциональные элементы в едином корпусе. Такое решение позволит уменьшить количество датчиков вскрытия корпуса в составе СЗС.

Часть функций модуля электропитания может быть возложена на источник вторичного электропитания с резервом (ИЭПВР), установленный на защищаемом объекте, или же модуль электропитания может быть выполнен в виде отдельного конструктивного элемента, вмонтированного в корпус оконной конструкции. Изготовление подобного модуля электропитания негативно повлияет на стоимость остекленной конструкции, оснащенной комплексом. Использование независимого модуля электропитания снизит нагрузку на ИЭПВР объекта, но не повысит устойчивость системы охраны объекта к потере электропитания из-за невозможности передать извещение о тревоге, минуя оконечное объектовое устройство.

Особое внимание следует уделить модулю электропитания беспроводного варианта конструктивного исполнения комплекса, в нем должны обеспечиваться легкость замены элементов питания и срок службы без замены элементов питания в течение не менее 1–2 лет.

Создание комплекса в беспроводном исполнении позволит избежать сложных работ по монтажу линий связи и электропитания, но приведет к необходимости своевременной замены элементов питания, а значит усложнению обслуживания.

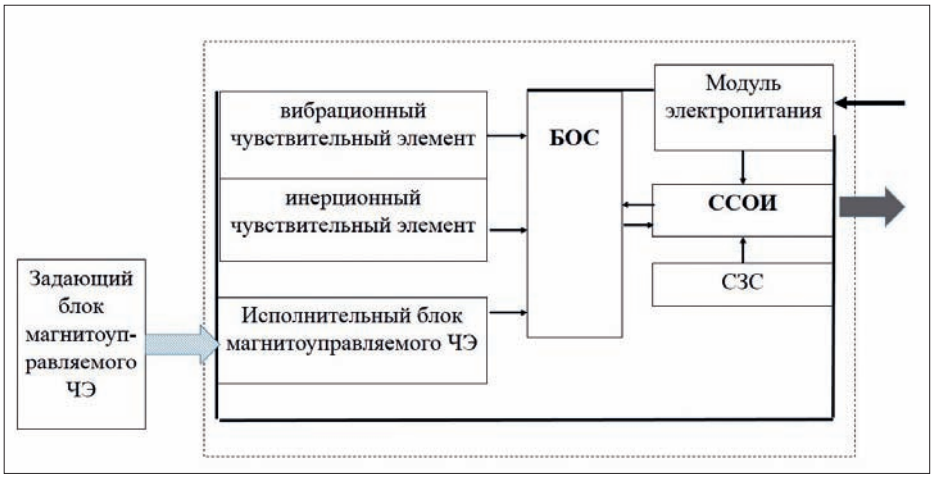


Рис. 5. Структура комплекса

[5] *ГОСТ Р 56102.1–2014. Системы централизованного наблюдения. Часть 1. Общие положения.*

Габариты

Одним из путей оптимизации конструкции и электропотребления комплекса является использование чувствительного элемента на основе акселерометра в качестве чувствительного элемента инерционного и вибрационного канала обнаружения. Несмотря на некоторое снижение показателей параметров обнаружения и, соответственно, помехоустойчивости комплекса, данное решение позволяет добиться кардинального уменьшения его габаритов и возможности установки как в новые оконные конструкции, так и в ранее установленные.

Для повышения чувствительности акселерометра к типовым воздействиям на оконную конструкцию все ЧЭ комплекса целесообразно разместить на торцевой части створки окна рядом с запорным механизмом. При таком размещении определить извне наличие охранного оборудования на окне невозможно, а первоначальный внешний вид окна полностью сохраняется.

Варианты блокировки

Необходимой функцией комплекса должна стать блокировка постановки на охрану при открытых на проветривание створках охраняемой конструкции либо открытом запорном механизме. Для этого нужно использовать магнитоуправляемый ЧЭ на основе датчика Холла. Кроме того, применение этого варианта ЧЭ обеспечит защиту от блокировки чувствительной части комплекса магнитом большой мощности.

Таким образом, приходим к следующим вариантам реализации модуля средств обнаружения попытки взлома:

а) вибрационный извещатель на основе пьезоэлектрического ЧЭ, акселерометр, магнитоконтактный извещатель;

б) малогабаритный вибрационный извещатель на основе акселерометра, точечный извещатель на основе датчика Холла.

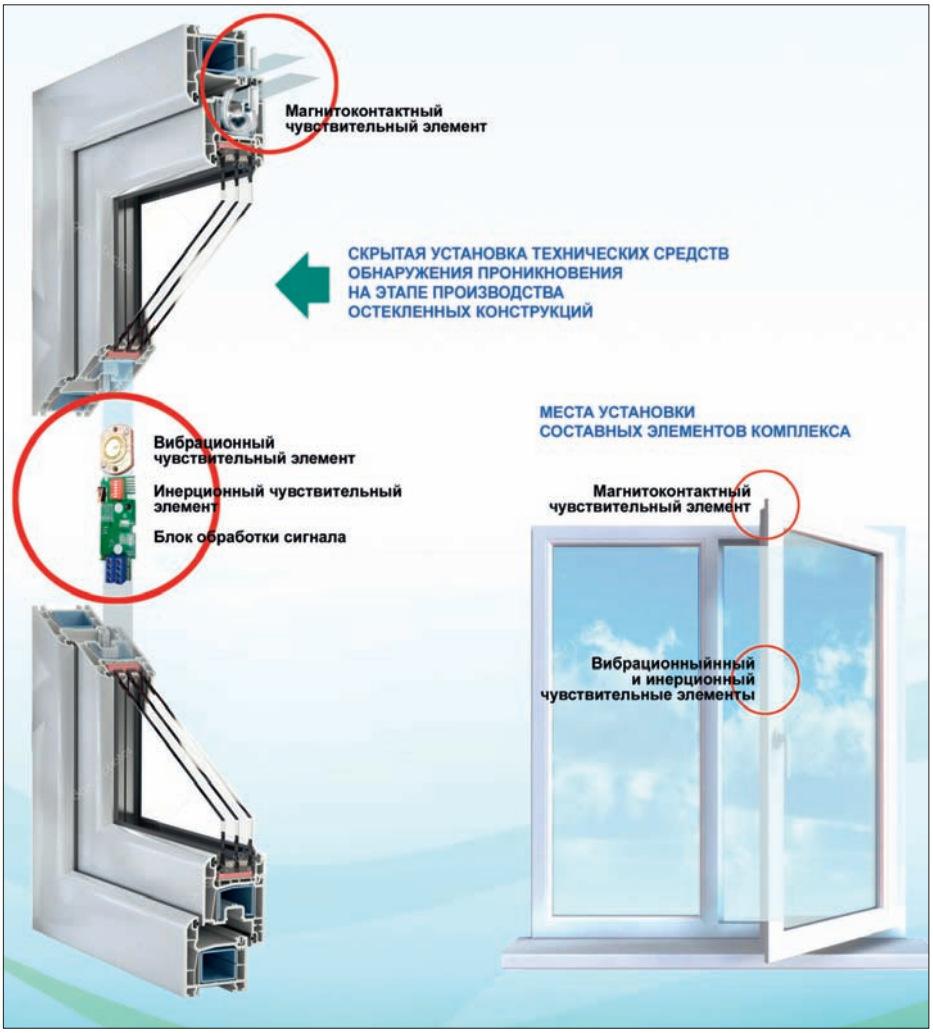


Рис. 6. Комплекс для защиты остекленных конструкций, построенный на основе серийно выпускаемых извещателей

Требования к извещателям

После рассмотрения состава модуля средств обнаружения комплекса, учитывая также требования минимизации стоимости и габаритов, приходим к выводу, что оптимальным вариантом комплекса является его реализация в соответствии с требованиями к совмещенным охранным извещателям по ГОСТ Р 52435–2015[6], в радиоканальном или проводном исполнении. Можно сформулировать следующие технические предложения:

1. Наиболее целесообразным способом комплексной защиты остекленных конструкций является совмещенный охранный извещатель в радиоканальном или проводном исполнении.

2. Электропитание совмещенного охранного извещателя лучше осуществлять от внешнего источника электропитания или автономных элементов электропитания (при использовании беспроводных каналов передачи тревожных извещений).

3. Для повышения чувствительности к типовым воздействиям на оконную конструкцию ЧЭ комплекса целесообразно разместить на торцевой части створки окна рядом с запорным механизмом.

4. Извещатель должен формировать извещение о тревоге при открытии окна (каналы обнаружения переориентации извещателя и точечные магнитоконтактные), разрушении конструкции рамы и створки окна, разбитии полотна стеклопакета (вибрационный канал обнаружения).

Общий вид одного из вариантов комплекса, построенного на основе серийно выпускаемых извещателей, изображен на рис. 6.

Извещатель должен обеспечивать выдачу не менее пяти извещений:

1) нормальное состояние;
2) взлом стеклопакета;
3) неисправность извещателя/электропитания;
4) вскрытие извещателя или отрыв его от монтажной поверхности;
5) открывание створки оконной конструкции.

Приведенные конструктивные решения и выбранные типы ЧЭ позволяют блокировать прием объекта на охрану при:

- открытой створке окна;
- створке, установленной на проветривание;
- визуально закрытой, но не запертой створке (когда запирающая ручка повернута не полностью).

Точное обнаружение в любых ситуациях

Представленные варианты построения комплекса обеспечивают обнаружение разбития внешнего стекла стеклопакета и попытки высверливания запорного механизма или отжимания створки оконной конструкции на ранней стадии.

Таким образом, при защите оконных блоков высокого класса по ГОСТ Р 57788–2017[7] комплекс производит раннее обнаружение следующих видов криминальных воздействий:

1) разбитие внешнего стекла стеклопакета;
2) попытка взлома оконной конструкции путем выведения из строя запорных механизмов (высверливание, выпиливание, выбивание) на начальном этапе сверления (реза);
3) силовой отжим створки или фрамуги с помощью слесарных инструментов;
4) выпиливание стекла дисковой электропилой;
5) выдавливание или вырывание тросом всей оконной конструкции из проема. ■

[6] ГОСТ Р 52435–2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.

[7] ГОСТ Р 57788–2017. Национальный стандарт Российской Федерации. Блоки оконные и дверные защитные для охраняемых помещений. Общие технические условия.

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

Извещатели разбития стекла реагируют первыми

Мнения экспертов

Главная задача извещателей разбития стекла – генерация сигнала тревоги при повреждении стекол на объектах разного типа. Они предупреждают о механическом воздействии на стекла и позволяют предотвратить несанкционированное проникновение в помещение. При выборе таких извещателей следует ориентироваться на принцип их действия и наличие нужных параметров. Эксперты из компаний "Болид" и "Теко-ТД" рассказали, на какие характеристики нужно обращать внимание в первую очередь, где извещатели разбития стекла незаменимы и как будет развиваться их технологическая составляющая

Николай Перепелица
Ведущий инженер
ЗАО НВП "Болид"

Павел Ильин
Старший инженер отдела маркетинга
ООО "Теко-ТД"

В целом эволюция извещателей идет от однофункциональных извещателей к комбинированным мультифункциональным.
К примеру, извещатель может измерять шумы, изменение теплового или температурного фона, состава газа, движение воздушных потоков и на основании первичных данных строить более комплексную и взаимосвязанную картину на объекте в дополнение к системам видеонаблюдения

Какой функционал извещателей разбития стекла можно назвать типовым, а какой расширенным?

Николай Перепелица, "Болид"

К типовому функционалу извещателей можно отнести параметры, удовлетворяющие обязательным минимальным требованиям ГОСТ 34025–2016:

- чувствительность, достаточная для обнаружения (с вероятностью не менее 0,9), разрушающего воздействия на охраняемое стекло (стеклопакет);
- рабочая частота (от 31,5 до 16 000 Гц);
- максимальная дальность действия (не менее 6 м);
- минимальная контролируемая площадь стекла (не более 0,1 кв. м);
- вероятность обнаружения (не менее 0,9);
- помехоустойчивость (не формировать извещение о тревоге при нанесении по охраняемому стеклу (стеклопакету) неразрушающих механических ударов предметами, выполненными из материалов различной твердости);
- угол диаграммы направленности (не менее 90 град. в вертикальной и горизонтальной плоскостях);
- время готовности извещателей к работе (не менее 60 с);
- длительность извещения о тревоге для неадресных извещателей (не менее 2 с);
- время восстановления нормального состояния извещателей после формирования извещения о тревоге (не более 30 с для питаемых по ШС и не более 60 с для адресных и беспроводных извещателей);
- не менее четырех видов извещений (нормальное состояние, тревога, неисправность, несанкционированный доступ);
- устойчивость к воздействию климатических факторов.

К расширенному (дополнительному) функционалу можно отнести:

- функцию антимаскирования;
- дискретную регулировку чувствительности;
- повышенную устойчивость к воздействию помех;
- дистанционное управление режимами работы и индикацией.

Павел Ильин, "Теко-ТД"

На рынке представлены извещатели четырех основных типов по принципу действия:

- ударокontактные;
- вибрационные;
- пьезоэлектрические;
- акустические.

Первые три имеют недостатки в монтаже и эстетичности, заметны и требуют установки на поверхность стекла. Применяются в исключительных случаях.

Наиболее распространенным видом являются акустические извещатели. Большинство из них имеют типовой функционал:

- дальность действия – 6 м;
- угол охвата – 120 град.;
- микропроцессорный анализ сигнала для достоверного (за счет заложенных алгоритмов) определения и отделения признаков именно разбития стекла от ложных событий.

Для привлечения интереса покупателей производители добавляют в извещатели полезные опции, например:

- определение точного адреса (а следовательно, и места на плане помещения) извещателя, зафиксировавшего тревогу;
- передача сигналов без проводов по радиоканалу, что позволяет существенно сократить время и расходы на монтаж и не портить интерьер помещений;
- регулировка чувствительности микрофона;
- подключение дополнительных технологических устройств, имеющих выход типа "сухой контакт" и работающих на размыкание.

На каких объектах извещатели разбития стекла являются незаменимыми с технической точки зрения и по нормам и требованиям?

Николай Перепелица, "Болид"
По назначению и принципу обнаружения данные извещатели незаменимы для комплексной системы безопасности в зданиях, где на первом этаже есть помещения с остекленными конструкциями на доступной высоте. По сути, они обнаруживают нарушителя в самой начальной стадии проникновения, когда он еще находится вне периметра объекта, и формируется определенный запас времени на реагирование службой безопасности. Поэтому использование данного типа извещателей регламентируется как обязательное многими ведомственными нормами, в частности, на объектах, охраняемых национальной гвардией.

Павел Ильин, "Теко-ТД"
Извещатели разбития стекла востребованы на любых типах объектов, где существует возможность проникновения через слабо укрепленные места (окна, стеклянные двери), а также в банках, ювелирных магазинах и музеях для защиты ценностей, размещенных в остекленных конструкциях (витринах).

Основными заказчиками извещателей разбития стекла являются различные охранные структуры и подразделения вневедомственной охраны войск национальной гвардии Российской Федерации. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений описано в Р 78.36.044–2014 и Р 78.36.028–2012.

Извещатели незаменимы для комплексной системы безопасности в зданиях, где на первом этаже есть помещения с остекленными конструкциями на доступной высоте. По сути, они обнаруживают нарушителя в самой начальной стадии проникновения, когда он еще находится вне периметра объекта

Какие методы тестирования извещателей можно считать максимально убедительными для заказчика?

Николай Перепелица, "Болид"
Регулярно встречаются недоверчивые заказчики, которые задают вопрос, можно ли доверять методам тестирования, если реального разрушения не происходит. В настоящее время широко предлагаются два метода – с помощью "стального шара" и звуковых имитаторов.
Безусловно, удобнее тестировать и настраивать с помощью имитатора разбития стекла, так как его преимуществами являются отсутствие риска механического повреждения остекленной поверхности и оперативность проверки. Однако при всей привлекательности данный метод использует усредненные параметры тестового сигнала, зачастую не полностью соответствующие конкретным стеклам.
Лучше все-таки пользоваться "шариковым" методом. Что касается его убедительности, то до заказчиков следует доводить информацию, что данный метод утвержден специалистами Межгосударственного технического комитета по стандартизации ТК 234 "Системы тревожной сигнализации и противокриминальной защиты", действующего на базе ФКУ "НИЦ "Охрана" Росгвардии.

Павел Ильин, "Теко-ТД"
Наиболее удобный и эффективный способ проверки работоспособности – использование электронных акустических имитаторов разрушения стекла. Однако при испытаниях необходимо учитывать, что извещатель настроен для обнаружения разбития стекол в раме или стене.
Кроме того, имеется способ тестирования резиновым шариком.

Насколько эффективны предлагаемые многими производителями совмещенные решения?

Николай Перепелица, "Болид"
Совмещенные в одном корпусе извещатели – хорошее решение для помещений, в которых необходимо одним извещателем перекрыть два рубежа защиты при меньшем ветвлении кабельных трасс. При этом в дневное время, в присутствии людей, ИК-канал совмещенного извещателя (объемный или поверхностный) можно отключать, а окна оставлять под охраной акустического канала.
В качестве защиты витрин можно использовать оба канала совмещенного извещателя по схеме "или" для повышения вероятности обнаружения. Для снижения ложного срабатывания используют каналы совмещенного извещателя по схеме "и".

Павел Ильин, "Теко-ТД"
Эффективность повышается в два раза. Каналы обнаружения работают независимо друг от друга. Фактически это два изделия в одном корпусе. Второй канал подтверждает первоначальное определение тревожного события. Применение совмещенных извещателей снижает стоимость оборудования, монтажа и настройки.

Какие новые технологии уже применяются или будут применяться в извещателях разбития стекла в ближайшее время?

Николай Перепелица, "Болид"
В извещателях применяются современная схемотехника и способы микропроцессорной обработки сигналов, позволяющие повысить вероятность обнаружения, чувствительность, устойчивость к воздействию помех и максимальную дальность действия. Что касается внедрения новых физических принципов, некоторыми производителями проработан вопрос использования ультразвука для обеспечения функции антимаскирования в извещателе разбития стекла.

Павел Ильин, "Теко-ТД"
На сегодняшний день применяется в основном пассивная технология выделения из звукового сигнала спектра частот и вычисление, сравнение их "весовых" характеристик друг с другом и шаблоном. При превышении определенных порогов и соотношений извещатель формирует сигнал тревоги.
Потенциально применимы технологии нейросетей, аналогично распознаванию речи. Такие извещатели позволят надежнее определять разбитие (или даже покушение на разбитие) и более четко отсеивать ложные события. Кроме того, они смогут выполнять смежные функции, например прослушивание помещения и анализ речи.
В целом эволюция извещателей идет от однофункциональных извещателей к комбинированным мультифункциональным. К примеру, извещатель может измерять шумы, изменение теплового или температурного фона, состава газа, движение воздушных потоков и на основании первичных данных строить более комплексную и взаимосвязанную картину на объекте в дополнение к системам видеонаблюдения. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Модель извещателя	"Арфа–2Р"	"Арфа-И"	"Арфа-ПРО"
			
Производитель, сайт производителя	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru
Компания, предоставившая информацию, сайт	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru	ООО "АРГУС-СПЕКТР", www.argus-spectr.ru
Физический принцип обнаружения разрушения стекла	Акустический	Акустический	Акустический
Виды и марки стекол, разрушение которых фиксирует извещатель	Стекла, в том числе стеклопакеты (однокамерные и двухкамерные по ГОСТ 24866-99), выполненные с использованием листовых стекол: обычное марок М4–М8 по ГОСТ 111-90 толщиной 2,5–8 мм; закаленное по ГОСТ 5727-88, 3–6 мм; армированное по ГОСТ 7481-78, 5,5/6 мм; узорчатое по ГОСТ 5533-86, 3,5–7 мм; трехслойное защитное по классу А1–А3 по ГОСТ Р 51136-98, 4–11 мм; покрытое защитной полимерной пленкой, обеспечивающей класс защиты А1–А3 по ГОСТ Р 51136-98	Стекла, в том числе стеклопакеты (однокамерные и двухкамерные по ГОСТ 24866-99), выполненные с использованием листовых стекол: обычное марок М4–М8 по ГОСТ 111-90 толщиной 2,5–8 мм; закаленное по ГОСТ 5727-88, 3–6 мм; армированное по ГОСТ 7481-78, 5,5/6 мм; узорчатое по ГОСТ 5533-86, 3,5–7 мм; трехслойное защитное по классу А1–А3 по ГОСТ Р 51136-98, 4–11 мм; покрытое защитной полимерной пленкой, обеспечивающей класс защиты А1–А3 по ГОСТ Р 51136-98	Стекла, в том числе стеклопакеты (однокамерные и двухкамерные по ГОСТ 24866-99), выполненные с использованием листовых стекол: обычное марок М4–М8 по ГОСТ 111-90 толщиной 2,5–8 мм; закаленное по ГОСТ 5727-88, 3–6 мм; армированное по ГОСТ 7481-78, 5,5/6 мм; узорчатое по ГОСТ 5533-86, 3,5–7 мм; трехслойное защитное по классу А1–А3 по ГОСТ Р 51136-98, 4–11 мм; покрытое защитной полимерной пленкой, обеспечивающей класс защиты А1–А3 по ГОСТ Р 51136-98
Дальность действия, м	6	6	6
Угол обзора, град.	120	120	120
Минимальная охраняемая площадь, кв. м	0,05	0,05	0,05
Количество анализируемых акустических частотных диапазонов	2	2	2
Контроль вскрытия корпуса	Да	Да	Да
Регулировка чувствительности	Да, 3 уровня	Да, 2 уровня	Да, 3 уровня
Контроль маскирования, его принцип	Алгоритм "Антисаботаж-2"	Алгоритм "Антисаботаж-2"	Алгоритм "Антисаботаж-2"
Второй канал обнаружения проникновения	Да, вход ШС	Да, вход ШС	Да, вход ШС
Адресность	Адресный радиоканальный	Адресный проводной	Адресный радиоканальный
Схема питания	Литиевые батареи	По сигнальной линии	Литиевые батареи
Напряжение питания, В	3	22–27	3
Ток потребления в дежурном режиме, мА	0,003	0,3	0,003
Ток потребления в режиме "тревога", мА	0,003	6	0,003
Степень защиты оболочки IP	IP30	IP30	IP30
ЭМС, степень жесткости	3	3	3
Диапазон рабочих температур, °С	-20…+55	-20…+55	-20…+55
Габаритные размеры, мм	80x36	80x36	80x36
Цвет корпуса	Белый	Белый	Белый
Масса, кг	0,2	0,1	0,2
Розничная цена, руб.	3360,34	2564,64	3360

Модель извещателя	"ИО329-17 Сонар-2"	"С2000-СТ исп. 04"	"С2000-СТИК"
			
Производитель, сайт производителя	"Сибирский Арсенал", www.arsenal-sib.ru	ЗАО НВП "Болид", www.bolid.ru	ЗАО НВП "Болид", www.bolid.ru
Компания, предоставившая информацию, сайт	ООО "ТД Актив-СБ", www.aktivsb.ru	ЗАО НВП "Болид", www.bolid.ru	ЗАО НВП "Болид", www.bolid.ru
Физический принцип обнаружения разрушения стекла	Извещатель должен зарегистрировать низкочастотный и высокочастотный сигналы и оценить характер их изменения в определенном интервале времени. Низкочастотный звуковой сигнал возникает в момент удара по стеклу, высокочастотный – в момент разрушения стекла	Акустический	Акустический
Виды и марки стекол, разрушение которых фиксирует извещатель	Обычные толщиной 4–10 мм; узорчатые 3,5 мм; закаленные 4–10 мм; армированные 5,5 мм; защищенные полимерной пленкой толщиной 4 мм, классы А1, А2, А3	Обычное, закаленное, армированное, триплекс	Обычные стекла толщиной 2,5–8 мм марок М4-М8 по ГОСТ 111-90; покрытые защитной полимерной пленкой, обеспечивающей класс защиты А1–А3 по РД 78.148-94 МВД России
Дальность действия, м	До 6	Не менее 6	6
Угол обзора, град.	120	Не менее 90	120
Минимальная охраняемая площадь, кв. м	Не менее 0,1	0,1	0,1
Количество анализируемых акустических частотных диапазонов	2	2	2
Контроль вскрытия корпуса	Да	Да	Да
Регулировка чувствительности	Да	Да	Да
Контроль маскирования, его принцип	Нет	Да, акустический ультразвуковой	Да, активный акустический
Второй канал обнаружения проникновения	Нет	Нет	Да, пассивный инфракрасный
Адресность	Неадресный	Адресный проводной	Адресный
Схема питания	По ШС	По ШС (ДПЛС)	По ШС
Напряжение питания, В	8–30	8–12	12
Ток потребления в дежурном режиме, мА	Не более 0,5	0,7	1
Ток потребления в режиме "тревога", мА	8–12	1,5	1
Степень защиты оболочки IP	IP40	IP30	IP41
ЭМС, степень жесткости	Нет данных	3	3
Диапазон рабочих температур, ˚С	-20…+50	-10…+45	-10…+45
Габаритные размеры, мм	90x57x34	95x65x30	130x68x44
Цвет корпуса	Белый	Белый	Серый
Масса, кг	Не более 0,06	Не более 0,1	0,1
Розничная цена, руб.	690	По запросу	1592

Модель извещателя	"Астра-С"	"Астра-Z-6145"	"Астра-6131"
			
Производитель, сайт производителя	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz
Компания, предоставившая информацию, сайт	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz
Физический принцип обнаружения разрушения стекла	Акустический	Акустический	Акустический
Виды и марки стекол, разрушение которых фиксирует извещатель	Обычные и защищенные полимерной пленкой толщиной 2,5–8 мм; армированные до 6 мм; узорчатые 4–8 мм; многослойные строительные 6–8 мм; закаленные 4–6 мм	Обычные и защищенные полимерной пленкой толщиной 2,5–8 мм; армированные до 6 мм; узорчатые 4–8 мм; многослойные строительные 6–8 мм; закаленные 4–6 мм	Обычные и защищенные полимерной пленкой толщиной 2,5–8 мм; армированные до 6 мм; узорчатые 4–8 мм; многослойные строительные 6–8 мм; закаленные 4–6 мм
Дальность действия, м	6	6	6
Угол обзора, град.	120	120	120
Минимальная охраняемая площадь, кв. м	Не менее 0,1 (при длине одной из сторон не менее 0,3 м)	Не менее 0,1 (при длине одной из сторон не менее 0,3 м)	Не менее 0,1 (при длине одной из сторон не менее 0,3 м)
Количество анализируемых акустических частотных диапазонов	2	2	2
Контроль вскрытия корпуса	Да	Да	Да
Регулировка чувствительности	Да	Да	Да
Контроль маскирования, его принцип	Нет	Да, вход для СМК	Нет
Второй канал обнаружения проникновения	Нет	Нет	Да, вход для СМК
Адресность	Неадресный	Адресный радиоканальный	Адресный радиоканальный
Схема питания	Внешнее	АКБ	АКБ
Напряжение питания, В	8–15	3,6	3
Ток потребления в дежурном режиме, мА	Не более 12	Не более 0,06	Не более 0,06
Ток потребления в режиме "тревога", мА	Не более 12	Не более 105	Не более 25
Степень защиты оболочки IP	IP30	IP30	IP30
ЭМС, степень жесткости	ГОСТ Р5009-200; УК1, УК2 – 2-я степень жесткости; УЭ1, УИ1 – 3-я степень жесткости	ГОСТ Р5009-200; УК1, УК2 – 2-я степень жесткости; УЭ1, УИ1 – 3-я степень жесткости	ГОСТ Р5009-200; УК1, УК2 – 2-я степень жесткости; УЭ1, УИ1 – 3-я степень жесткости
Диапазон рабочих температур, ˚С	-20…+50	-20…+50	-20…+50
Габаритные размеры, мм	87x55x28	101,5x63x32	87x54x28
Цвет корпуса	Белый	Белый	Белый
Масса, кг	0,05	0,07 кг	0,04
Розничная цена, руб.	620	2466	1987

Модель извещателя	"Астра-621"	"Астра-8 исп. РК"	LC-105DGB
			
Производитель, сайт производителя	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz	DSC, www.dsc.com
Компания, предоставившая информацию, сайт	ООО "Теко-ТД", www.teko.biz	ООО "Теко-ТД", www.teko.biz	"ЗС Групп", www.new-satro.ru
Физический принцип обнаружения разрушения стекла	Акустический	Акустический	Конденсаторный микрофон с двухканальной обработкой сигнала (выдача сигнала тревоги после последовательного срабатывания низкочастотного и высокочастотного каналов)
Виды и марки стекол, разрушение которых фиксирует извещатель	Обычные и защищенные полимерной пленкой толщиной 2,5–8 мм; армированные до 6 мм; узорчатые 4–8 мм; многослойные строительные 6–8 мм; закаленные 4–6 мм	Обычные и защищенные полимерной пленкой толщиной 2,5–8 мм; армированные до 6 мм; узорчатые 4–8 мм; многослойные строительные 6–8 мм; закаленные 4–6 мм	Все виды оконных стекол, функция определения резки алмазом
Дальность действия, м	6	6	10
Угол обзора, град.	120	120	Нет данных
Минимальная охраняемая площадь, кв. м	Не менее 0,1 (при длине одной из сторон не менее 0,3 м)	Не менее 0,1 (при длине одной из сторон не менее 0,3 м)	Нет данных
Количество анализируемых акустических частотных диапазонов	2	2	2
Контроль вскрытия корпуса	Да	Да	Да
Регулировка чувствительности	Да	Да	Да
Контроль маскирования, его принцип	Нет	Нет	Нет данных
Второй канал обнаружения проникновения	ИК	ИК	Нет
Адресность	Неадресный	Адресный радиоканальный	Неадресный
Схема питания	Внешнее	АКБ	По ШС
Напряжение питания, В	8–15	3	9–16
Ток потребления в дежурном режиме, мА	Не более 15	Не более 0,13	22 (±5%)
Ток потребления в режиме "тревога", мА	Не более 15	Не более 25	25 (±5%)
Степень защиты оболочки IP	IP30	IP30	Нет данных
ЭМС, степень жесткости	ГОСТ Р5009-200; УК1, УК2 – 2-я степень жесткости; УЭ1, УИ1 – 3-я степень жесткости	ГОСТ Р5009-200; УК1, УК2 – 2-я степень жесткости; УЭ1, УИ1 – 3-я степень жесткости	Нет данных
Диапазон рабочих температур, ˚С	-20…+50	-20…+50	-20…+50
Габаритные размеры, мм	110x60x45	Ø108	78x51x21
Цвет корпуса	Белый	Белый	Светло-серый
Масса, кг	0,09	0,09	0,07
Розничная цена, руб.	998	2258	1214

КОЛОНКА РЕДАКТОРА

Живучесть противопожарных систем как новое нормативное требование

На протяжении нескольких лет в нашей стране разрабатываются новые нормативные требования к пожарной безопасности, которые призваны устранить недостатки действующих. У профессионального сообщества проекты новых стандартов и правил вызывают массу обсуждений и вопросов, так как их соблюдение потребует принципиально нового подхода к работе и со стороны производителей, и со стороны проектно-монтажных организаций.

Один из важнейших аспектов, который затрагивают новые требования и правила, – это вопрос устойчивости приборов и системы в целом к внешним и внутренним воздействиям. Другими словами, обеспечение максимальной устойчивости и надежности системы, чтобы при возникновении неисправности отдельной ее части – выходе из строя прибора или линии связи – она сохраняла работоспособность. О том, что единичная неисправность не должна влиять на работоспособность системы в целом, уже сказано во вступившем в силу с 1 января текущего года техническом регламенте ЕАЭС "О требованиях к средствам обеспечения пожарной безопасности и пожаротушения". В последних редакциях межгосударственного стандарта и свода правил данное требование также зафиксировано, и довольно однозначно.

Таким образом, перед производителями стоит задача обеспечивать максимальную живучесть системы и высокий уровень устойчивости к внутренним и внешним воздействиям. Одно из наиболее эффективных решений данной задачи – применение технологии глобального роуминга, то есть многосвязной маршрутизации, которая поддерживает живучесть системы охранно-пожарной сигнализации за счет множества резервных путей доставки сигнала между извещателями и радиорасширителями. Безусловно, речь идет именно о радиоканальных системах, что лишний раз подчеркивает: будущее именно за системами без проводов. В предлагаемой в данном номере статье подробно описывается технология глобального роуминга, ее особенности и преимущества при построении системы охранно-пожарной сигнализации.

Михаил Левчук
Редактор рубрики "Беспроводные технологии", исполнительный директор ООО "Аргус-Спектр"

Глобальный роуминг
в беспроводных системах безопасности

Широкая популярность беспроводных систем безопасности объясняется их улучшенными техническими характеристиками, которые позволяют решать задачи более высокого уровня и оборудовать объекты любой сложности и размеров. Технологию глобального роуминга можно уверенно назвать одной из главных отличительных особенностей современных радиоканальных решений. В этой статье речь пойдет об основных характеристиках этой технологии и ее преимуществах для рынка беспроводных систем безопасности

Олег Тимонин
Генеральный директор
ООО "КОМПАНИЯ "ФОРМА ГРУПП"

Основой глобального роуминга является технология Mesh–сетей, которые в последнее время приобрели большую популярность и используются в самых различных областях: в мобильных и информационных технологиях, в военной и транспортной сферах, безопасности жилых, культурных и промышленных объектов. В зависимости от поставленной задачи сеть можно настроить наиболее подходящим образом.

Глобальный роуминг базируется на принципе ячеистой топологии, где части сети соединяются друг с другом и могут принимать на себя роль коммутатора для остальных участников. При глобальном роуминге данные передаются от одного устройства к другому до тех пор, пока они не достигнут назначенного получателя (рис. 1).

Уникальный уровень живучести

Радиоканальные системы безопасности, как правило, строятся на базе ретрансляторов (или радиорасширителей), которые устанавливаются в разных точках здания и контролируют определенное количество извещателей и других устройств. При этом один из этих ретрансляторов будет центральным, и именно он является конечной точкой всех маршрутов передачи данных в системе. Поэтому в случае с беспроводной системой безопасности технология глобального роуминга формируется из двух составляющих:

- автоматический выбор ретранслятора каждым устройством;

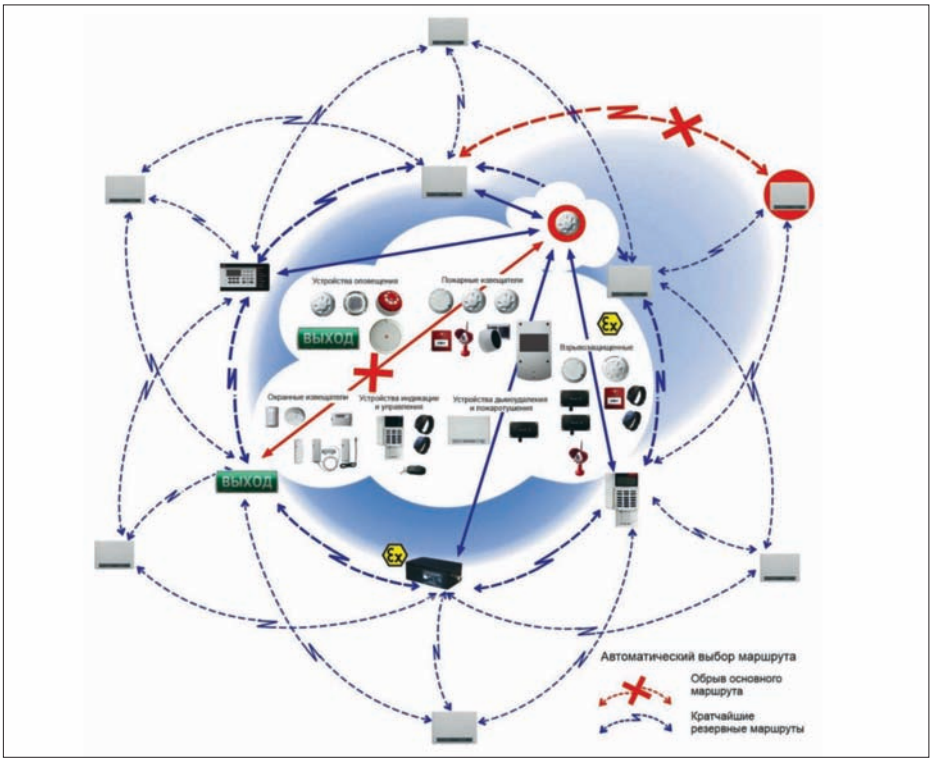


Рис. 1. Схема глобального роуминга на примере беспроводной системы пожарной сигнализации, оповещения и локализации

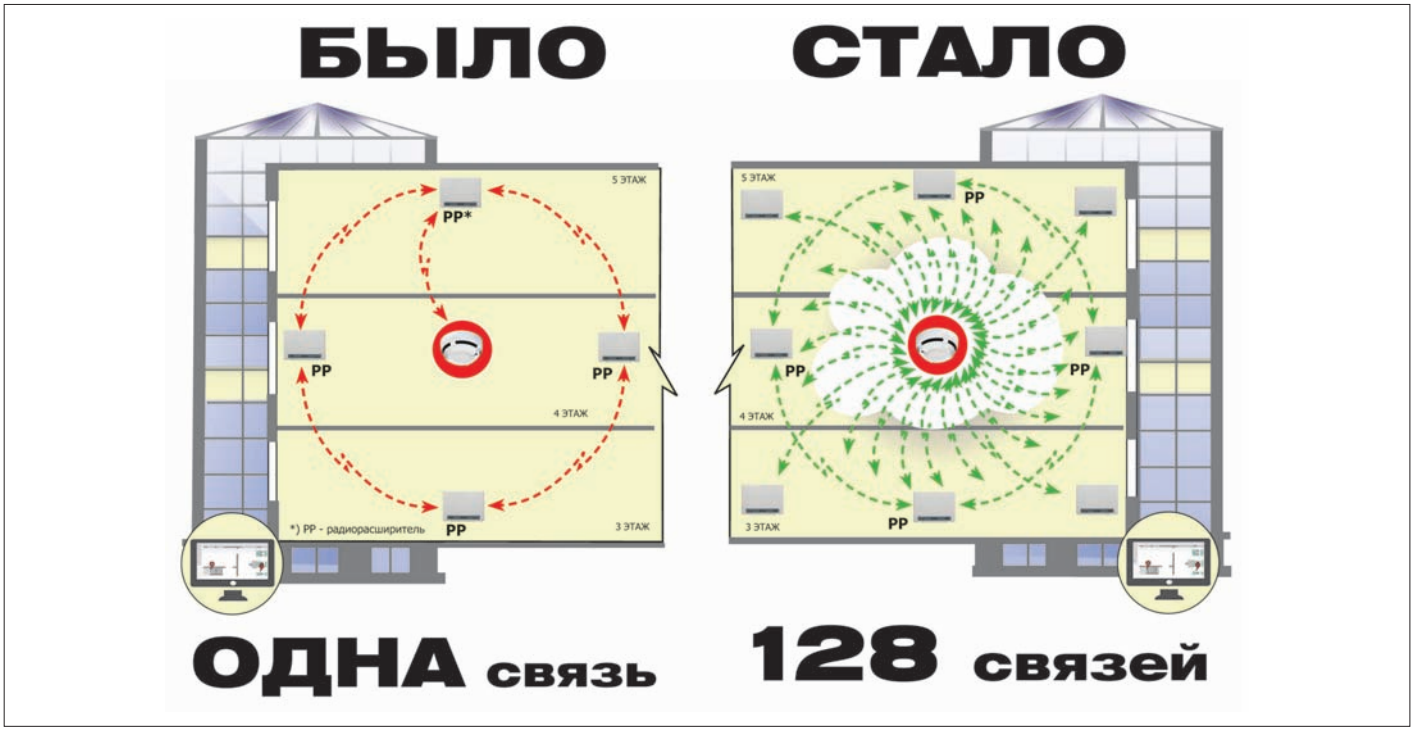


Рис. 2. Старые и новые радиоканальные системы

- автоматический выбор пути связи ретрансляторов с пультом (динамическая маршрутизация).

Технология Mesh-сетей, заложенная в глобальном роуминге, определяет принцип построения сети, при котором появляется самоорганизующаяся архитектура, позволяющая выйти на новый уникальный уровень живучести: сеть становится устойчива к потере отдельных элементов.

Высокий уровень живучести крайне важен при разработке беспроводных систем пожарной сигнализации: современные российские и международные стандарты и нормативные документы диктуют производителям требования, при которых системы должны быть устойчивы к внешним воздействующим факторам. Например, единичная неисправность линии связи системы в одной части здания или сооружения не должна приводить к выходу всей системы из строя. Именно глобальный роуминг помогает обеспечивать высокий уровень надежности системы, благодаря которому ее практически невозможно вывести из строя.

Многосвязность системы

В качестве примера представим радиоканальную систему пожарной сигнализации, состоящую из большого количества устройств – пожарных извещателей, устройств оповещения, контроллеров и радиорасширителей (ретрансляторов). Предположим, что при пожаре или неисправности вышел из строя ретранслятор. В проводных системах при выходе из строя прибора или линии связи теряется контроль над несколькими помещениями или этажами здания. В системе с глобальным роумингом другой подход: ранее привязанные к ретранслятору устройства переподключаются к другим приборам и изменяют маршрут связи с пультом, используя резервные пути доставки сигналов. В итоге работоспособность системы сохраняется.

А теперь представим, что количество ретрансляторов в сети – 128 шт. При таком числе узлов каждый прибор может иметь множество резервных путей доставки сигнала (рис. 2). Надежность связи в подобной сетевой топологии становится исключительно высокой, так как для связи дочерних устройств с пультом используются все возможные пути.

Многосвязность системы, которая образуется при использовании глобального роуминга, обеспечивает беспрерывность работы: каждый из ретрансляторов всегда сможет найти резервный маршрут в случае потери основной линии связи. Каждый ретранслятор хранит в памяти запасные маршруты для соединения с нужным ему сегментом, что повышает надежность и живучесть системы.

Почему так важен уровень живучести в радиоканальных системах безопасности? Живучесть можно интерпретировать как параметр, обеспечивающий функционирование системы пожарной сигнализации в процессе развития пожара в течение всего периода времени, который необходим для эвакуации людей и дальнейшей ликвидации пожара. Даже если часть пожарных извещателей в ходе пожара выйдет из строя, то остальное оборудование продолжит функционировать в полном объеме, что позволит отслеживать динамику развития пожара и оперативно управлять эвакуацией людей в соответствии со складывающейся обстановкой.

Выгоды для проектно-монтажных организаций

Благодаря технологии глобального роуминга процессы проектирования, монтажа и пусконаладки максимально упрощаются, поскольку сама система выполняет большую часть рутинной работы:

- распределяет извещатели между расширителями;
- автоматически создает сеть из расширителей;
- адаптируется под изменяющиеся условия эксплуатации.

В итоге нужно всего лишь оценить качество связи и расставить достаточное количество радиорасширителей. Система автоматически определит, к какому прибору привяжется дочернее устройство и как будут связаны между собой ретрансляторы в сети.

Благодаря глобальному роумингу проектирование системы займет меньше времени и сил. Процесс монтажа будет выглядеть следующим образом:

1. Расстановка на поэтажных планах в проекте дочерних устройств (извещатели, оповещатели и исполнительные устройства). Тип, место установки и количество определяются в соответствии с требованиями нормативных документов по пожарной безопасности.
2. Расстановка на поэтажных планах в проекте радиорасширителей, исходя из радиуса их действия в данном здании.
3. При глобальном роуминге каждое дочернее устройство после программирования автоматически подключается к ближайшему радиорасширителю.

3 убедительных преимущества

Технология глобального роуминга выводит беспроводные системы безопасности на новый уровень и предоставляет существенные преимущества:

1. Автоматическая адаптация под изменяющиеся условия эксплуатации. Дочернее устройство выбирает прибор с лучшим уровнем связи.
2. Повышение уровня живучести системы, который помогает ей продолжать свою работу при воздействии внешних факторов. Система способна сохранять работоспособность на все время, необходимое для эвакуации людей из зданий и помещений.
3. Удобство проектирования и проведения пусконаладочных работ. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

АРГУССПЕКТР

Умные пожарные извещатели нового поколения

"Аргус-Спектр" представляет новую линейку радиоканальных точечных пожарных извещателей серии "Аврора-ПРО" из состава "СТРЕЛЬЦА-ПРО"

Компания "Аргус-Спектр" продолжает переход на новую беспроводную систему охранно-пожарной сигнализации, оповещения и локализации "СТРЕЛЕЦ-ПРО" и с 1 марта снимает с производства пожарные извещатели серии "Аврора-Р", предлагая на замену новую линейку радиоканальных извещателей "Аврора-ПРО". При той же цене новые устройства имеют ряд существенных преимуществ по сравнению с предыдущим поколением датчиков.

Извещатели для комплексных решений

"Аврора-ПРО" – это серия извещателей с функциями как обнаружения признаков пожара, так и оповещения о пожаре в здании. В табл. 1 приведены состав и основные функциональные характеристики продукции.

Уникальность "Авроры-ДО-ПРО" в том, что устройство не только обнаруживает дым, но и реализует функцию речевого, звукового ("белый шум") и светового оповещения. Извещатели "Аврора-ДО-ПРО" позволяют построить в здании систему динамического управления эвакуацией "Нить Ариадны": устройства последовательно воспроизводят шумовые сигналы и вспышки, создавая звуковую и световую дорожку, указывающую направление к безопасному выходу. При этом возможности системы позволяют при необходимости изменить направление звуковой волны и световой дорожки к другому эвакуационному выходу.

Точечный дымовой извещатель "Аврора-ДС-ПРО", помимо прямого назначения, реализует функцию звукового оповещения для систем оповещения о пожаре 1-го и 2-го типов.

В извещателе "Аврора-ДТ-ПРО" для повышения вероятности обнаружения пожара используется двухфакторное выявление события по двум основным признакам – появлению дыма и быстрому повышению температуры.

Улучшенные технические характеристики

Радиоканальная система нового поколения "СТРЕЛЕЦ-ПРО" разработана с учетом многолетнего опыта эксплуатации системы "СТРЕЛЕЦ", поэтому извещатели серии "Аврора-ПРО" обладают не только полным набором функций своих предшественников, но и рядом существенных преимуществ. При этом извещатели новой линейки выпускаются в той же ценовой категории, что и датчики из состава предыдущей версии системы.

Глобальный роуминг

Благодаря реализованной в системе "СТРЕЛЕЦ-ПРО" технологии глобального роуминга устройства "Аврора-ПРО" автоматически по уровню связи переключаются на тот радиорасширитель, с которым устанавливается наиболее стабильный обмен данными. Радиорасширители системы, в свою очередь, определяют кратчайший маршрут передачи сигналов через другие ретрансляторы на пульт дежурного.

Таблица 1. Характеристики извещателей "Аврора-ПРО"

Наименование	Факторы обнаружения пожара		Встроенная функция оповещения		
	Дым	Тепло	Звуковое	Речевое	Световое
Аврора-Д-ПРО	●	○	○	○	○
Аврора-Т-ПРО	○	●	○	○	○
Аврора-ДТ-ПРО	●	●	○	○	○
Аврора-ДС-ПРО	●	○	●	○	○
Аврора-ДО-ПРО	●	○	○	●	●

Таблица 2. Сравнение извещателей "Аврора-Р" и "Аврора-ПРО"

Параметр	Серия "Аврора-Р"	Серия "Аврора-ПРО"
Автоматический выбор радиорасширителя, резервирование путей доставки сигнала	Нет	Да
Время работы от батарей	5 лет	10 лет
Время запуска оповещения*, с	12–120	3
Дальность связи, м	600	1200
Количество в одной радиосистеме	512	1 920
Удаленный мониторинг аналоговых значений (включая заряд батарей)	Нет	Да
Изменение любых настроек по радиоканалу без перепрограммирования	Нет	Да
Передача локационных сигналов (контроль местонахождения носимых браслетов внутри здания)	Нет	Да
Цена	Одинаковая	
* Для извещателей со встроенным оповещателем		

Локализация и пейджинг

Извещатели серии "Аврора-ПРО" принимают локационные сигналы от "Браслетов-ПРО" – электронных носимых устройств, входящих в состав системы "СТРЕЛЕЦ-ПРО".

"Браслет-ПРО" предназначен для контроля местонахождения, состояния и оповещения персонала и посетителей объекта. Устройство также используется для приема текстовых сообщений с контрольного пункта (в том числе о ЧС и необходимости эвакуации) и персональной навигации. Состояние персонала контролируется при помощи встроенного датчика неподвижности, отправляющего сигнал тревоги на контрольный пункт при нажатии кнопки или автоматически при отсутствии движения браслета дольше 45 с.

Локализация по "Браслетам-ПРО" происходит внутри здания (по сигналам пожарных датчиков) и снаружи (по сигналам спутников GPS/ГЛОНАСС).

10 лет работы от батарей

Энергопотребление радиоканальных извещателей в системе "СТРЕЛЕЦ-ПРО" обеспечивает 10 лет работы устройств от батарей против прежних 3–5 лет. Каждое дочернее устройство системы контролирует состояние основной и резервной батареи. В случае разряда на устройстве загорается светодиоидный индикатор и информация о состоянии батареи поступает на приемно-контрольное устройство.

Дальность связи с радиорасширителем 1200 м

В открытом пространстве дальность связи между "Авророй-ПРО" и радиорасширителем достигает 1200 м, а между двумя радиорасширителями – 2000 м.

Компания "Аргус-Спектр" продолжает переход на новую беспроводную систему охранно-пожарной сигнализации, оповещения и локализации "СТРЕЛЕЦ-ПРО". Эти устройства имеют ряд существенных преимуществ по сравнению с предыдущим поколением датчиков.

Запуск оповещения о пожарной тревоге за 3 с

В новой системе с момента срабатывания извещателя "Аврора-ПРО" до синхронного запуска оповещения проходит 3 с.

1920 извещателей в системе

"СТРЕЛЕЦ-ПРО" является масштабируемой системой с емкостью:

- 1920 извещателей;
- 127 радиорасширителей.

Удаленный мониторинг состояния системы

АРМ обслуживания позволяет удаленно отслеживать текущее состояние всех показателей

устройств (дым, температура, запыленность, уровень батарей). Таким образом, по состоянию системы можно спланировать график обслуживания, не выезжая на объект.

Программирование по радиосети

После первичной инициализации устройств в системе "СТРЕЛЕЦ-ПРО" в дальнейшем все изменения их настройки программируются по радиоканалу. Повторная инициализация устройств не требуется.

Самодиагностика извещателей

Испытания извещателей серии "Аврора-ПРО", проведенные ФГБУ ВНИИПО МЧС России, подтверждают, что все датчики линейки обладают встроенными функциями самодиагностики и способны формировать сигналы о своей исправности (неисправности) или необходимости технического обслуживания. Эти сигналы формируются средствами индикации извещателей и передаются на приемно-контрольный прибор. В защищенном помещении или выделенных зонах контроля допускается устанавливать один автоматический пожарный извещатель серии "Аврора-ПРО" при условии соблюдения прочих требований СП5.13130.

Уникальная конструкция

Корпус новых извещателей серии "Аврора-ПРО" спроектирован таким образом, чтобы обеспечить наиболее надежную работу, простоту эксплуатации и обслуживания, свести к минимуму вероятность ложных срабатываний и снизить количество выездов обслуживающей бригады на объект.

Двойная защита от пыли

Одной из основных причин ложных срабатываний в оптико-электронных датчиках дыма является пыль, которая со временем оседает и копится в дымовой камере. Поэтому в корпусе извещателей "Аврора-ПРО" предусмотрено два пылесборника, в которых оседает большая часть пыли.

Извещатель также автоматически измеряет уровень запыленности камеры и передает сообщение о неисправности, когда запыленность достигает критического значения.

Устойчивость к "засветке"

Нередко причиной ложного срабатывания оптико-электронных дымовых датчиков является так называемая засветка. Лучи света из внешних источников попадают на фотоприемник оптопары, создавая световые шумы, которые могут вызвать ложное срабатывание. Для предотвращения "засветки" в корпусе дымовых извещателей линейки "Аврора-ПРО" имеется система отражателей, исключающая возможность попадания внешнего освещения на светочувствительные элементы.

Преграда от насекомых

Зачастую причиной ложной тревоги или неисправности пожарных извещателей становятся насекомые или мелкие предметы, попавшие внутрь корпуса. Защитная сетка в конструкции корпуса извещателей линейки "Авроры-ПРО" предотвращает попадание любых мелких предметов внутрь.

Чувствительность к дыму по всем направлениям

Симметричность воздухозаборника извещателей "Аврора-ПРО" гарантирует одинаковую чувствительность детекторов дыма по всем направлениям.

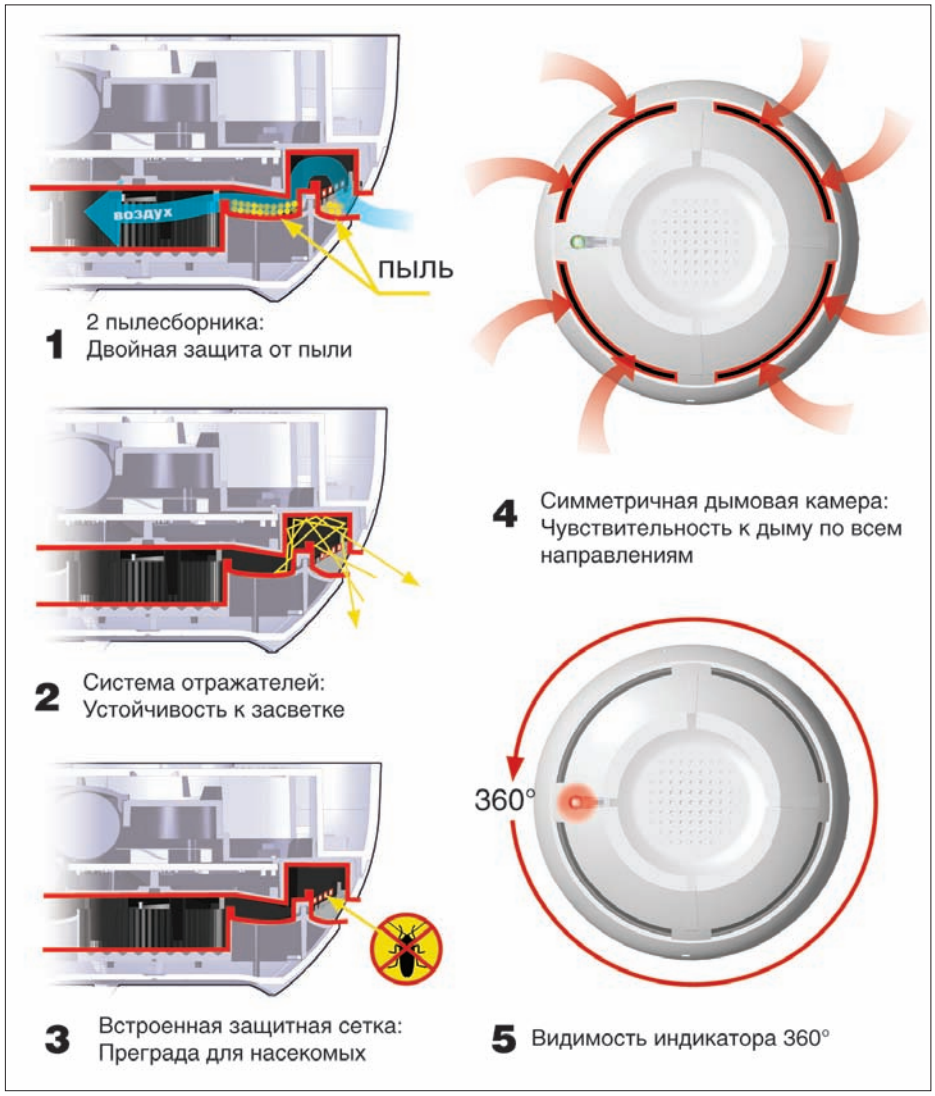


Рис. 1. Уникальная конструкция извещателей "Аврора-ПРО"

Простой монтаж

Простота и быстрота монтажа системы достигается благодаря особой конструкции корпуса "Аврора-ПРО". Весь процесс монтажа заключается в креплении "базы" извещателя к несущей поверхности двумя саморезами и установке извещателя в "базу" одним поворотом руки.

Быстрее, проще, надежнее

Резюмируя, можно разделить усовершенствования в радиоканальной системе безопасности "СТРЕЛЕЦ-ПРО" на три основных направления:

1. Сохранение работоспособности даже в случае выхода из строя ряда устройств. Используя технологию многосвязной маршрутизации (глобального роуминга), извещатели "Аврора-ПРО" автоматически выбирают маршрут передачи сигнала на пульт дежурного и при необходимости переключаются на резервные пути доставки сигнала. Таким образом, при выходе из строя одного или нескольких приборов система сохраняет работоспособность.

2. Упрощенные проектирование и пусконаладка, удобство технического обслуживания. После программирования связи между извещателями и радиорасширителями формируются автоматически, и в дальнейшем система адаптирует сеть приборов под изменяющиеся условия эксплуатации. В итоге нужно лишь оценить качество связи и расставить достаточное количество радиорасширителей. Работы по обслуживанию системы значительно упрощаются благодаря удаленному мониторингу показателей устройств. Специалисты могут заранее и без выезда на объект планировать техническое обслуживание.

3. Максимально быстрое оповещение о пожаре и динамическое управление эвакуацией. Извещатели "Аврора-ПРО" гарантируют своевременное формирование сигнала пожарной тревоги в системе для запуска оповещения на объекте и передачи на пульт наблюдения. В новых извещателях оповещение о пожаре запускается за 3 с. Устройства линейки "Аврора-ДО-ПРО" позволяют построить на объекте беспроводную систему динамического управления эвакуацией "Нить Ариадны" – звуковую и световую дорожку к ближайшему безопасному выходу.

Все перечисленные улучшения делают систему "СТРЕЛЕЦ-ПРО" уникальным решением в области радиоканальных систем безопасности. ■

КОЛОНКА РЕДАКТОРА

Доверяй, но проверяй

Из дорожных записок

Посещение реальных объектов дает пищу для размышлений. Вот и на этот раз, приехав к одному из заказчиков, я невольно обратил внимание на установленный при въезде на объект поворотный шлагбаум. На нем шильдик: название поставщика, его адрес, телефоны и адреса электронной почты отдела продаж, здесь же указана модификация шлагбаума – противотаранный барьер (ПТБ) такой-то. Далее следуют контакты производителя, год выпуска, ширина проезда, высота стрелы над поверхностью. И, как положено, надпись "Изготовлено в России".

Вроде бы все указано, даже некоторые технические характеристики, кроме одной, а именно – какой таранный удар сможет выдержать конструкция? Спросил об этом представителя заказчика, тот не без гордости заявил, что это довольно мощное устройство и рассчитано на удар 7-тонного грузовика, движущегося со скоростью 50 км/час. Можете представить себе загруженный доверху ЗиЛ-130? Действительно, заявленные показатели внушительные. Спросил, есть ли акты натурных испытаний. Увы, их у заказчика не оказалось, объяснили, что основные характеристики ПТБ были представлены поставщиком на конкурс, исходя из математических расчетов.

Многолетняя практика показывает, что расчетные показатели конструкций подобного назначения могут расходится с результатами натурных испытаний на 50%, как правило, в худшую сторону, то есть по расчетам балка должна выдержать нагрузку, а она разрывается.

Заказчик предлагает ознакомиться с информационным листком, где подробно указаны габариты и технические характеристики ПТБ. Здесь, и ширина проезда (4 м), и угол поворота стрелы (90 град.), и температурный диапазон (-45...+50 °С), и габариты замковой стойки со стрелой и без оной.

Но опять же нет ключевой характеристики: на какой таранный удар рассчитана конструкция шлагбаума.

Обращаюсь к веб-сайту поставщика. Первое, что бросается в глаза, – баннер со слоганом "Быстрый расчет нестандартных изделий". И далее помельче: "Наш проектный отдел рассчитает любое нестандартное изделие за один час".

Захожу в раздел "Противотаранные барьеры", кликаю на нужную модификацию поворотного шлагбаума и опять не нахожу ни результатов натурных испытаний, ни физических характеристик устойчивости к таранному удару. Зато под заголовком "Плюсы и минусы эксплуатации разных типов ПТБ" читаю в общем описании линейки изделий: "Стрела у ПТБ шлагбаумного типа находится на высоте 90 см от поверхности проезжей части, благодаря этому при возникновении таранного удара автомобиль наезжает на стрелу ПТБ непосредственно кузовом. Это позволяет мгновенно остановить транспортное средство, все части автомобиля остаются за пределами огражденной территории. Вероятность попадания элементов автомобиля в пешеходов и материальные объекты крайне мала. При таранящем ударе нарушится форма стрелы, но ее целостность будет сохранена".

О том, что конструкция выдержит таранный удар, утверждает последняя фраза. Однако где приложенный для убедительности расчет?

Беру линейку, замеряю сечение стрелы шлагбаума, сваренной из двух швеллеров 16П. При этом внутри барьера нет ни тросов, ни каких-то иных усиливающих конструкцию элементов. Вношу замеры в компьютерную программу. Заметьте, что погрешность таких расчетов может составлять до 50%.

В итоге определяю, что максимальное усилие деформации балки, приложенной посередине, пролетом 4 м для стали с пределом прочности 500 МПа составляет 100 000 Н, или 10 тонн, в упругой зоне работы материала. Далее происходит пластическая деформация балки без уменьшения указанного усилия. Максимальное смещение балки определяется величиной перекрытия балки с опорой и составляет по результатам замеров 300 мм. Данному перемещению равна деформация середины пролета балки, и, соответственно, максимальное расстояние для остановки прорывающегося автомобиля – 0,7 метра.

На основе силовых расчетов и геометрических построений прихожу к выводу: действительно, конструкция ПТБ шлагбаумного типа данной модификации выдержит таранный удар транспортным средством массой 7 тонн, движущимся со скоростью... 15 (а не заявленные 50) км/час. Понятно, что расчеты имеют приблизительный характер. Предлагаю специалистам проверить и, быть может, даже опровергнуть полученные мной результаты.

Хочу напомнить и разработчикам, и потенциальным заказчикам, что натурные испытания противотаранной техники методом краш-теста (которые считаются обязательными за рубежом), может быть, и затратный, но самый убедительный способ подтвердить расчетные характеристики конструкций.

На сайте того же поставщика есть пояснение: "Противотаранный барьер – сложный инженерный объект, специально созданный для защиты периметра стратегически важных государственных особо охраняемых объектов. Данные устройства препятствуют проникновению посторонних небронированных колесных транспортных средств (автомобилей) на защищаемую территорию..."

В заключение советую владельцам объектов обращать внимание на документы или расчеты, подтверждающие технические характеристики предлагаемого оборудования.

Рис. 1. Поворотный шлагбаум с пустотелой стрелой, сваренной из двух швеллеров

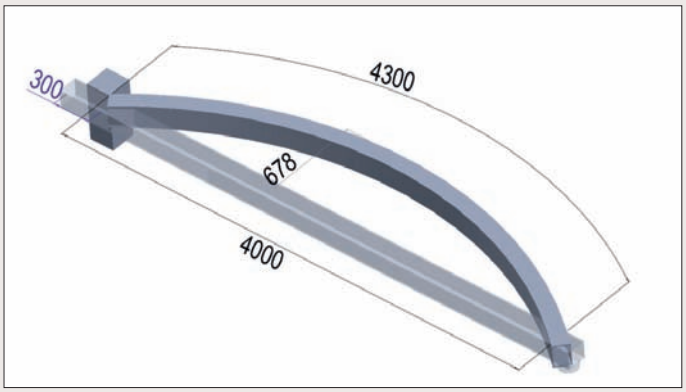


Рис. 2. Максимальная деформация балки длиной 4,3 м до выхода из зацепления с опорой

Игорь Васильев

Редактор раздела "Комплексная безопасность, периметровые системы", главный конструктор ЦеСИС

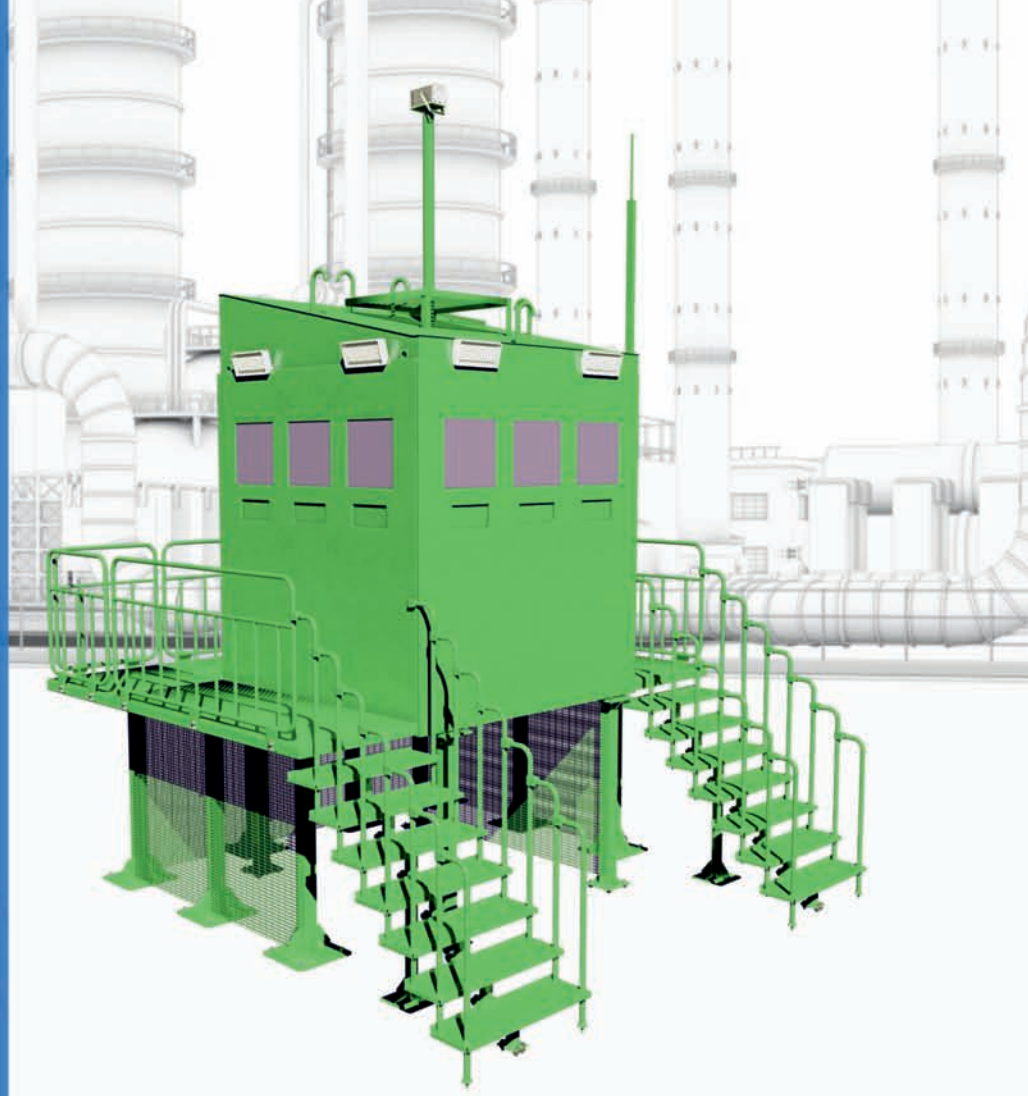
ЦеСИС®

ЦЕНТР СПЕЦИАЛЬНЫХ
ИНЖЕНЕРНЫХ СООРУЖЕНИЙ

440067, г. Пенза,
ул. Чаадаева, 62
т/ф: (8412) 37-40-48, 37-40-50
8 (800) 444-22-51

info@cesis.ru,
snabsbit@cesis.ru

www.cesis.ru,
www.cesis-proekt.ru



ЭСТАКАДА ДОСМОТРОВАЯ, МОДУЛЬНАЯ

Сферы применения:

- досмотровые автомобильные площадки и шлюзы;
- лестничные входы в здания и сооружения;
- переходные мостики через технологические магистрали (трубопроводы) и другие возвышенные протяженные препятствия на пути прохода людей;
- в качестве грузовых рамп и площадок, расположенных над уровнем земли.

Универсальность:

- компактная упаковка, простая и прочная конструкция;
- универсальные составные модули:
  - ступени;
  - опора;
  - площадка;
- высота и ширина эстакады варьируется в размерах универсальных модулей.

Соответствие нормативам:

- конструкция модульной эстакады соответствует требованиям ГОСТ 23120-2016.
- модули эстакады устойчивы при нормативной временной нагрузке 300 кгс/м^2.

Основные преимущества:

- серийный выпуск;
- простота установки;
- жесткость конструкции;
- сборка без применения сварки;
- возможность установки эстакады на уклонах местности;
- компактная упаковка.

Борис Казеннов
Андрей Киселев
Александр Павлов
Эксперты управления Центра ФСБ России

Обязательная сертификация технических систем и средств досмотра и интеллектуального видеонаблюдения

Ведомственный сегмент системы обязательной сертификации технических средств обеспечения транспортной безопасности приступил к работе в августе 2017 г. С тех пор произошли значительные изменения в области обязательной сертификации технических систем и средств досмотра, а также интеллектуального видеонаблюдения

В качестве аппарата федерального органа по сертификации выступает ФГКУ "В/ч 68240", которое в соответствии с функциональными обязанностями, определенными Правилами обязательной сертификации, организует рассмотрение обращений и жалоб на действие органа по сертификации и размещение справочной информации в информационно-телекоммуникационной сети Интернет на официальном сайте ФСБ России в разделе "Научно-техническое сотрудничество".

Органом по сертификации является ФГУП "НТЦ "Орион", которое оперативно информирует о выданных сертификатах соответствия на собственном сайте.

Аккредитованы две ведомственные испытательные лаборатории и одна коммерческая:

- для проведения сертификационных испытаний технических систем и средств досмотра – ФГКУ "В/ч 35533" и ФГУП НИИР (в отношении металлодетекторов, газоанализаторов и ренгенотелевизионных установок);
- для проведения сертификационных испытаний технических систем и средств интеллектуального видеонаблюдения – ФГКУ "В/ч 44236".

Результаты 2019 года

Итоги работы ведомственного сегмента в прошедшем году следующие:

- за истекший период выдано 77 сертификатов соответствия (из них 66 – на технические средства досмотра и 11 – интеллектуального видеонаблюдения), отказано в выдаче сертификата соответствия по 10 заявкам семи организациям;
- начались работы по обязательной сертификации по схеме сертификации № 4;
- организован и проведен инспекционный контроль пяти наименований сертифицированных ТС ОТБ;
- ведется работа по рассмотрению жалоб на действия органа по сертификации.

На данный момент лабораторий достаточно – загрузка в 2019 г. не превысила одной трети мощности. Кроме того, еще три организации проходят процедуру аккредитации в качестве испытательных лабораторий.

За прошедший год наметились положительные тенденции в работе с заявителями. В результате постоянного информирования участников обязательной сертификации в 2,5 раза сократилось количество обращений за разъяснениями о порядке действий.

Сертификация зарубежных продуктов

Рекомендации по вопросу сертификации ТС ОТБ иностранного производства были учтены поставщиками оборудования. Прекратились попытки организовать проведение сертификации такого оборудования по схеме № 3. Совместными усилиями налажена работа по сертификации партий ТС ОТБ (схема № 2), зачастую достаточно крупных. Мы всегда идем навстречу заявителям, по возможности сертификационные испытания проводятся на их объектах, что позволяет сократить удельные расходы на проведение обязательной сертификации. Стараемся, не в ущерб качеству выпускаемой продукции, уменьшить финансовую нагрузку на производителей серийных ТС ОТБ: инспекционный контроль пока проводился только по заявкам держателей сертификатов в связи с внесением изменений в технические условия или после обращений потребителей.

Проверенные методики испытаний

Опыт работы за истекший период подтвердил эффективность и универсальность разработанных методик проведения сертификационных испытаний. Это дает возможность проводить испытания даже в нестандартных условиях, например с использованием движущегося на скорости до 70 км/ч железнодорожного состава в качестве тест-объекта. Так, совместно с Росжелдором, ОАО "РЖД" и ООО "Скантроник Системс" организована и проведена в кратчайшие сроки (за 38 календарных дней при норме 90 рабочих дней) уникальная работа по сертификации стационарного инспекционно-досмотрового комплекса для досмотра железнодорожных составов (СТ-2630Т-2), установленного на подходе к Крымскому мосту со стороны Краснодарского края.

Схема сертификации № 4 на практике

Остается ряд проблемных вопросов, они в основном связаны со схемой сертификации № 4. По ней выдано всего 10 сертификатов соответствия. Это при том, что только в 2019 г. поступило порядка 240 заявок (в 2018 г. – более 500). По результатам их рассмотрения направлены 342 отказа в проведении обязательной сертификации в связи с неправильным оформлением. Еще одно распространенное явление – прекращение переписки заявителями с органом по сертификации после получения замечаний. Это может быть обусловлено незаинтересованностью субъектов транспортной инфраструктуры в проведении сертификации ТС ОТБ, уже установленных на ОТИ. Основная цель таких заявителей – вступить в переписку и отчитаться перед надзорными органами. Это приводит к задержкам в рассмотрении заявок добросовестных заявителей, с чем связаны жалобы на действия органа по сертификации.

Расставим все точки над i

Субъекты транспортной инфраструктуры отказываются от проведения сертификации ТС ОТБ, установленных на ОТИ, ссылаясь на то, что их закупка проводилась в соответствии с требованиями Центра ФСБ России в рамках Комплексной программы обеспечения безопасности населения на транспорте. Внесем предельную ясность в этот вопрос.

Актуальность требований Центра ФСБ

Рекомендации по оснащению наиболее уязвимых ОТИ были разработаны Центром ФСБ России по просьбе Минтранса России до создания системы обязательной сертификации ТС ОТБ в качестве помощи в исполнении Указа Президента Российской Федерации от 30 марта 2010 г.

№ 403 "О создании комплексной системы обеспечения безопасности населения на транспорте". За основу требований были взяты лучшие на тот момент технические характеристики ТС ОТБ, производимых отечественной промышленностью.

В целях оценки эффективности использования указанных рекомендаций для оснащения зон досмотра были организованы пилотные зоны на объектах железнодорожного транспорта и метрополитенов. По результатам опытной эксплуатации пилотных зон Минтрансом России принято решение об оснащении ОТИ техническими средствами в соответствии с указанными рекомендациями.

Таким образом, формулировка "требования Центра ФСБ России" является не вполне корректной по смыслу. Правильнее было бы говорить о "требованиях Минтранса России, разработанных при участии Центра ФСБ России", так как Центр ФСБ России не наделен полномочиями по установлению правил и порядка оснащения ОТИ ТС ОТБ, а также корректировке или отмене указанных требований. В связи с этим нами направлено обращение председателю Межведомственной рабочей группы по сертификации ТС ОТБ, организованной Минтрансом России, с предложением на очередном заседании рассмотреть вопрос об актуальности требований с учетом действия системы обязательной сертификации.

Принципы обязательной сертификации

Данная позиция субъектов транспортной инфраструктуры основывается на неправильном понимании принципов обязательной сертификации ТС ОТБ. Ее основной принцип – непрерывный контроль за соответствием поставляемых ТС ОТБ требованиям к их функциональным свойствам.

Контроль осуществляется путем проведения испытаний:

- для единичных образцов (проверка каждого образца);
- для партий (выборочные проверки образцов из партии);
- для серийного производства (проверки в рамках процедуры сертификации и последующего регулярного инспекционного контроля в течение трех лет).

До вступления в силу правил обязательной сертификации при закупках такой контроль не был предусмотрен: требования к функциональным свойствам ТС ОТБ утверждены Правительством Российской Федерации только в 2016 г. после принятия соответствующих поправок в закон "О транспортной безопасности".

Таким образом, несмотря на то, что большинство моделей ТС ОТБ, закупленных субъектами транспортной инфраструктуры в рамках Комплексной программы, в настоящее время имеют сертификаты соответствия, конкретное оборудование, установленное до вступления в силу сертификатов соответствия, не может быть признано сертифицированным, так как не прошли соответствующие процедуры в соответствии с Правилами обязательной сертификации. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Модернизация системы физической защиты промышленного объекта

Модернизация системы физической защиты (СФЗ) промышленного объекта (ПО) – это обусловленный вызовами и запросами современной жизни процесс приведения СФЗ в соответствие с новыми требованиями и нормами. В этой статье рассмотрим его прикладные аспекты

Вадим Скворцов
Генеральный директор
ООО "Московский электроламповый завод"

Витольд Василец
Руководитель бюро
ООО "Московский электроламповый завод", доктор безопасности

Система физической защиты ПО определяется как организационно-техническая система, предназначенная для обеспечения физической безопасности ПО в условиях неопределенности в части потенциальных угроз и модели нарушителя.

Физическая безопасность – меры, предпринимаемые для обеспечения физической защиты материальных ценностей (ресурсов) от преднамеренных и случайных угроз.

Промышленный объект отождествляется, независимо от его организационно-правовой формы и формы собственности, с производственным комплексом, используемым субъектом производственной деятельности для ее осуществления. Подразумевается, что доступ на ПО разрешается или запрещается в соответствии с режимом предоставления полномочий, а требования, предъявляемые к физической защите ПО, увязаны с существующим производственным процессом ПО и привычными для персонала путями передвижения в различных зонах.

Операционная схема (алгоритм), определяющая структуру процесса модернизации системы физической защиты ПО, приведена на рис. 1.

Анализ факторов, предопределяющих качество СФЗ

Качество СФЗ – это совокупность свойств СФЗ, обусловливающих пригодность системы выполнять возложенные на нее функции по предотвращению (нейтрализации) воздействия базовых проектных угроз (БПУ). К числу факторов, предопределяющих качество СФЗ, в статье отнесены результаты выполнения следующих процедур:

- анализ типов потенциальных нарушителей и их проектных моделей;
- прогнозная оценка негативных последствий (ущерба ПО) от реализации угроз;
- анализ уязвимости ПО и оценка эффективности существующей СФЗ.

Обследование состояния физической защиты ПО проводится аккредитованной испытательной лабораторией разработчика СФЗ на договорной основе с ПО (заказчик).

Источники угроз

Основными источниками угроз для ПО могут быть:

- акции потенциальных нарушителей и сценарии их осуществления, предпринимаемые извне охраняемой территории ПО;
- чрезвычайные ситуации (ЧС) природного и техногенного характера, относящиеся к категории локальных и местных ЧС (по определению Федерального закона от 21.12.1994 г. № 68-ФЗ "О защите населения и территорий от ЧС природного и техногенного характера" (с изм. от 28.12.2013 г.);
- повышенная зависимость безопасности эксплуатации технологического оборудования ПО от влияния человеческого фактора вслед-

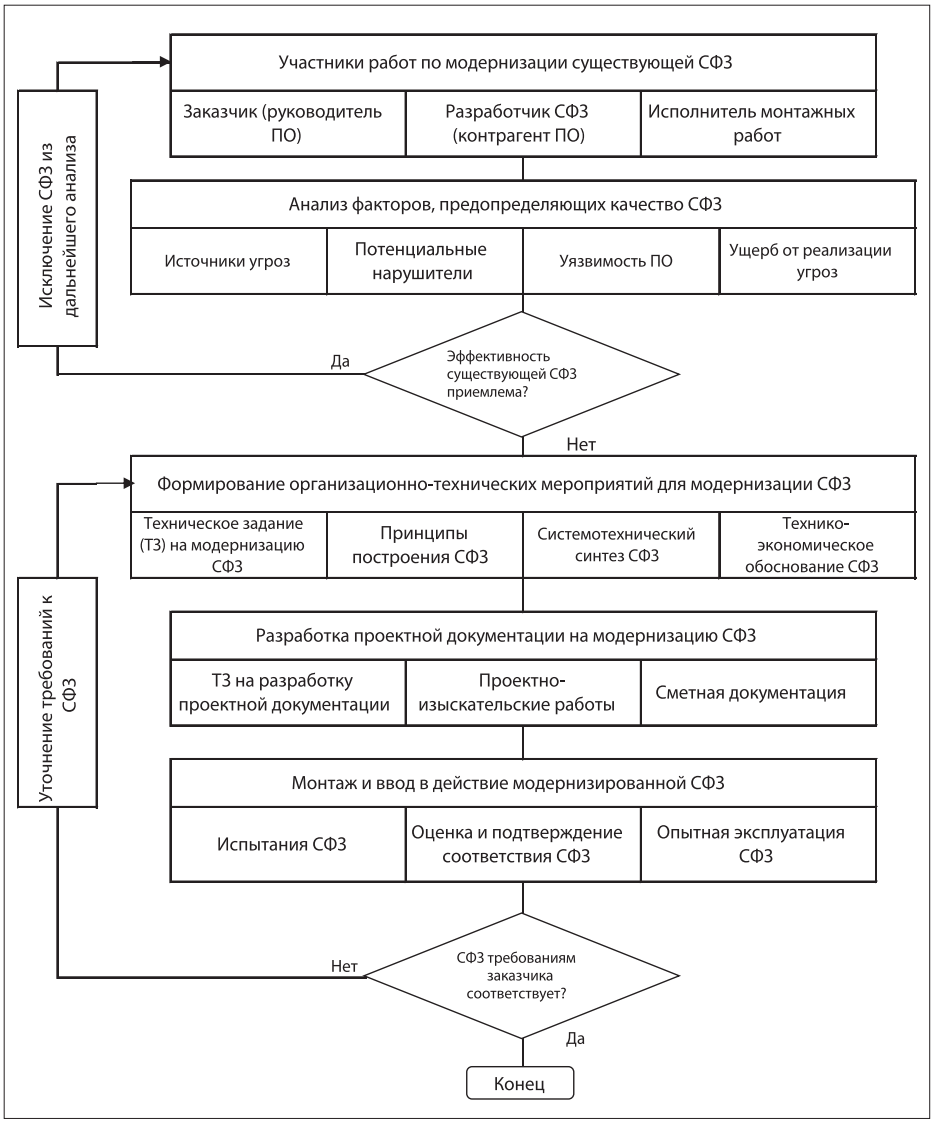


Рис. 1. Схема алгоритма модернизации СФЗ ПО

ствие ослабления трудовой мотивации персонала ПО.

Потенциальные нарушители

К потенциальным нарушителям могут быть отнесены[1]:

- криминальные (террористические) элементы, целью которых является хищение материальных ценностей или рейдерский захват ПО (за плату – проведение диверсий);
- представители протестных организаций (реализуемые ими угрозы – блокирование ПО, в крайних случаях – нарушение технологических процессов (нанесение вреда) объекта);
- лица с психическими отклонениями (сценарии осуществляемых ими актов незаконного вмешательства в деятельность ПО часто непредсказуемы).

Уязвимость ПО

Характеризует степень несоответствия фактических мер физической защиты ПО прогнозируемым угрозам или требованиям безопасности, заданным заказчиком СФЗ. Оценка уязвимости ПО выполняется для определения слабых (уязвимых) мест воздействия угроз ("поиск того, что нужно защищать, – предметов физической защиты и определение моделей нарушителя для каждого предмета"[2]).

Ущерб от реализации угроз

Общий профиль ущерба от реализации угроз физической безопасности ПО определяется условиями, которые могут возникнуть или способствовать проявлению рисковых событий, порождающих опасность причинения ущерба (нанесения вреда) ПО. Существует методический подход к количественной оценке размеров ущерба от реализации нарушителями АНВ[3]. Результаты оценки ущерба являются основанием для планирования мероприятий по выбору методов и технических средств физической защиты от актуальных ПО угроз.

Эффективность существующей СФЗ

Количественно эффективность СФЗ может быть оценена путем математического моделирования на ПЭВМ действий нарушителя и подразделения охраны ПО при наличии соответствующей компьютерной программы, которая должна обеспечивать возможность определения основного показателя эффективности СФЗ – вероятности перехвата нарушителя в конкретных ситуациях.

Результаты оценки эффективности существующей СФЗ позволяют дать ответ, насколько указанная система способна противостоять указанным выше угрозам. В качестве показателя эффективности СФЗ может быть избрана вероятность того, что силы охраны, действующие по сигналам тревоги от ТСФЗ, сумеют пресечь акцию нарушителя, то есть будет обеспечено обнаружение нарушителя, своевременное выдвижение сил охраны и нейтрализация злоумышленника.

Формирование организационно-технических мероприятий

Модернизация СФЗ проводится в обеспечение требований ПО (заказчик), изложенных им в техническом задании (ТЗ) на оборудование ПО комплексом технических средств физической защиты (ТСФЗ), соответствующих новым требованиям и нормам физической безопасности ПО. Техническое задание и исходные данные для выполнения проектных работ, подготовленные заказчиком, являются основанием для заключения договора с аккредитованным контрагентом ПО.

Принципы построения СФЗ

Основой построения СФЗ, схема которой приведена на рис. 2, является ее диверсификация, то есть применение техники там, где это возможно, а персонала там, где это необходимо. Функциональные подсистемы СФЗ содержат технические средства предотвращения (нейтрализации) базовых проектных угроз (БПУ), а персонал ПО осуществляет охрану, мониторинг, оперативное реагирование на тревожные извещения и техническое обслуживание СФЗ.

"Конечная задача СФЗ, состоящей из разнородных подсистем (технические комплексы, физические барьеры, подразделение охраны), состоит в защите находящихся на объекте предметов физической защиты. СФЗ рассматривается как единое целое, а ее составные части (подсистемы) должны вносить свой вклад в решение указанной задачи"[2]. В общем случае к предметам физической защиты могут быть отнесены:

- материальные ценности и иное имущество ПО;
- материальные носители информации ограниченного доступа;
- объекты интеллектуальной собственности ПО, в том числе не обеспеченные юридической защитой технологии, применяемые ПО.

Пригодность СФЗ выполнять возложенные на нее функции предопределяется полнотой соблюдения принципов построения СФЗ (см. табл. 2) и эффективностью управления процессами обеспечения качества СФЗ (см. табл. 3).

[1] Ничиков А.В. Понятие "модель нарушителя" и его связь с задачами обеспечения транспортной безопасности// Мир и безопасность, 2014. № 3 (113), С. 18.

[2] Измайлов А.В. Методы системного анализа в задачах обеспечения физической защиты критически важных объектов// Сборник научных трудов (выпуск № 3). М.: ФГУП "СНПО "Элерон", 2012. С. 83–86.

[3] Василец В.И. Априорная оценка уровня обеспечения безопасности ПО по величине предотвращенного ущерба от реализации угроз безопасности // Сборник трудов XXI Всероссийской научной конференции. М.: Академия управления МВД России, 2012. С. 290–292.

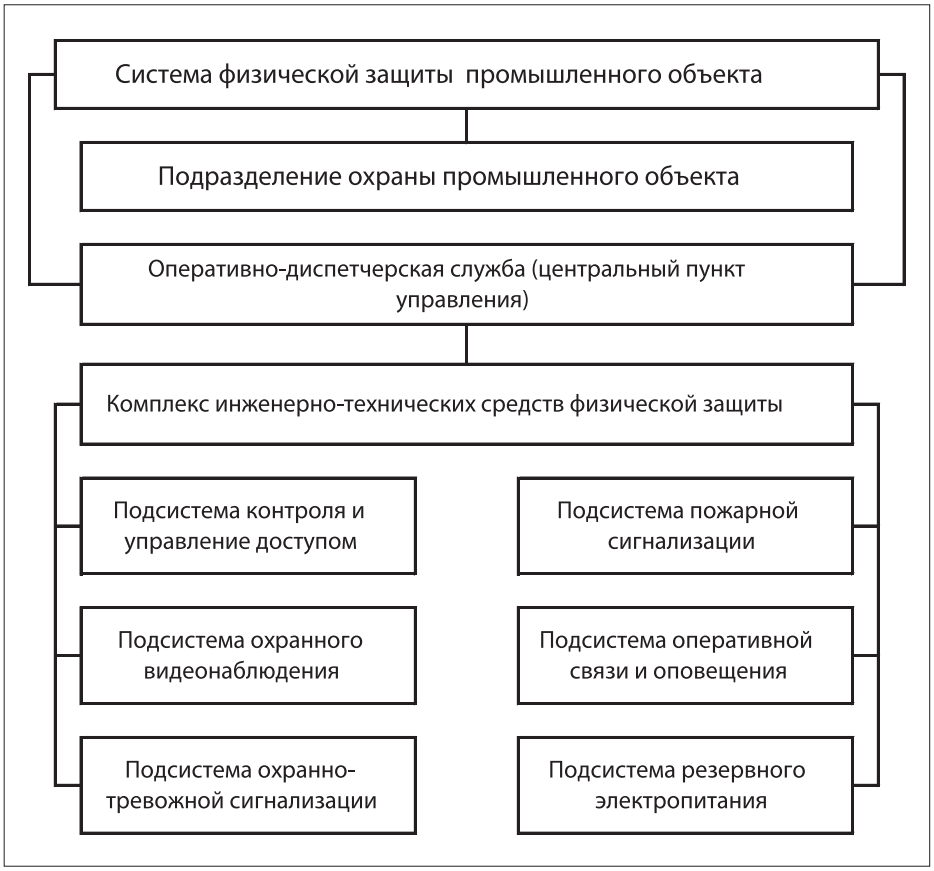


Рис. 2. Вариант структуры построения СФЗ ПО

Системотехнический синтез модернизируемой СФЗ

Это процесс обоснования и выбора облика оптимальной структуры СФЗ, а также предназначенных для нее ТСФЗ по соотношению "эффективность/стоимость". Сегодня экспертами предлагается вариант векторной оптимизации структуры СФЗ и оптимизации состава функциональных подсистем по безусловному критерию предпочтения (В. Парето)[4].

Технико-экономическое обоснование СФЗ

Технико-экономическое обоснование СФЗ разрабатывается для подготовки исходных данных, необходимых для оборудования ПО комплексом инженерно-технических средств физической защиты. Основополагающий принцип обоснования: от экономических возможностей ПО – к составу и уровню решения задач по предотвращению (нейтрализации) воздействия БПУ в условиях ограниченных ассигнований (ресурсов). Математическая форма записи указанного принципа имеет вид:

$W \to \max$ при $C \leqslant C_{выд.}$,

где W – достигаемый уровень эффективности предотвращения (нейтрализации) воздействия БПУ; $C_{выд.}$ – заданный (выделенный) размер ассигнований С, под который создается СФЗ.

В практических приложениях сформулированный экономический принцип дополняют:

- принцип иерархичности, согласно которому стоимость СФЗ представляется в виде совокупности затрат на отдельные этапы работ;
- принцип многовариантности (обеспечивает возможность получения оценок стоимости СФЗ при различном объеме исходных данных);
- принцип системности (процесс ценообразования рассматривается в неразрывной связи с общей экономической ситуацией в стране).

Критерий экономической эффективности

Это признак, позволяющий установить экономическую целесообразность (или нецелесообразность) формирования СФЗ.

Под указанным критерием правомерно понимать сравнение суммы C_{max} всех видов затрат на СФЗ с величиной предотвращенного ущерба (в денежном выражении) UПУ, отражающего результаты целенаправленных действий по ограждению ПО от негативных последствий реализации БПУ. В контексте изложенного критерий F экономической эффективности СФЗ можно представить в виде:

$F = U_{ПУ}/C_{max}$.

Допускается, что создание и внедрение СФЗ в условиях ПО экономически оправдано (целесообразно) при превышении критерием F единицы. Иными словами, затраты на компенсацию возможного ущерба ПО от акций нарушителя должны быть меньше величины указанного ущерба.

Виды затрат

Стоимостная оценка затрат на СФЗ представляет собой выраженные в денежной форме затраты ПО на разработку, внедрение и эксплуатацию системы. Основными видами указанных затрат являются:

- стоимость проектно-изыскательских работ по уточнению требований заказчика, изложенных в ТЗ на создание СФЗ;
- стоимость разработки конструкторской и сметной документации на СФЗ;
- стоимость реализации проектных решений СФЗ в условиях ПО;

Таблица 1. Обобщенная характеристика нарушителя

Тип нарушителя (вид нарушителя)	Используемые оружие и технические средства	Сценарий действий нарушителя
Криминальные и террористические элементы (внешний)	Автоматическое стрелковое оружие, взрывчатые вещества, средства преодоления физической защиты	Хищение материальных ценностей или рейдерский захват ПО (за плату – проведение диверсий)
Представители протестных организаций (внешний, внутренний)	Приспособления для нарушения целостности ограждения периметра ПО	Блокирование ПО, в крайнем случае – нарушение технологических процессов (причинение вреда ПО)
Лица с психическими отклонениями (внешний, внутренний)	Подручный инструмент	Сценарии осуществления актов незаконного вмешательства в деятельность ПО непредсказуемы

Таблица 2. Принципы, которым должна удовлетворять СФЗ ПО

Перечень принципов	Содержание принципов
Адекватность требованиям защиты	Принятые на ПО организационные меры и технические способы осуществления физической защиты должны соответствовать проектным угрозам и моделям нарушителей
Зональное построение	СФЗ должна предусматривать создание охраняемых зон и размещение в них зон ограниченного доступа
Равнопрочность	СФЗ должна обеспечивать заданный уровень эффективности для всех типов нарушителей и способов совершения ими АНВ в деятельность ПО
Адаптируемость	СФЗ должна обладать способностью к целенаправленному приспособлению при изменении технологических схем или условий функционирования ПО

[4] Пышкин Н.Б., Скворцов В. Э., Василец В.И. Концептуальное проектирование объектовой системы физической защиты// Мир и безопасность, 2014. № 3 (113), С. 20–23.

Таблица 3. Совокупность свойств СФЗ, определяющих ее качество

Свойства СЗИ	Определение свойств
Функциональная безопасность	Свойство (состояние) СФЗ, при котором она способна эффективно осуществлять возложенные на нее функции по исключению или снижению до допустимых значений воздействий на пользователей системы негативных факторов, которые могут возникнуть при ее эксплуатации
Надежность (безотказность, долговечность, ремонтопригодность)	Свойство СФЗ сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять базовые функции в заданных условиях и режимах применения, технического обслуживания и ремонта (ТО и Р)
Стойкость к внешним воздействующим факторам (ВВФ)	Свойство (способность) СФЗ сохранять работоспособное состояние в условиях и после воздействия ВВФ
Техническая эффективность	Свойство СФЗ, характеризующее степень приспособленности системы для применения по назначению в заданных условиях
Эксплуатационная технологичность	Совокупность конструктивно-технологических свойств СФЗ, определяющих пригодность системы к выполнению всех видов ТО и Р в принятых условиях эксплуатации с использованием наиболее эффективных технологических процессов

● стоимость применения (эксплуатации) СФЗ.

Сумма затрат по статьям калькуляции на разработку и реализацию проектных решений СФЗ определяет производственную себестоимость системы.

Методический подход к разработке технико-экономического обоснования СФЗ базируется на утверждении: "Затраты на создание и содержание СФЗ можно признать экономически целесообразными в том случае, если они не превышают сумм, необходимых для компенсации возможного ущерба от акций нарушителя"[5].

Динамика изменения затрат на СФЗ

Характеризует связь между производственной себестоимостью СФЗ и уровнем угроз, подлежащих нейтрализации, или между указанной себестоимостью и надежностью СФЗ.

Наглядной иллюстрацией динамики изменения затрат на СФЗ является график (см. рис. 3), устанавливающий связь между затратами (ордината С) и вероятностью безотказной работы СФЗ (абсцисса R). Указанный график представляет собой сумму ординат двух зависимостей, одна из которых определяет изменение затрат на разработку $C_Р$ и реализацию СП проектных решений СФЗ, а другая – изменение затрат $C_Э$ на эксплуатацию СФЗ. Проведя касательную к результирующей кривой, параллельную оси абсцисс в точке $R_{опт}$, можно найти минимальную величину затрат на СФЗ (точка $R_{опт}$ находится путем проведения касательной к результирующей кривой через начало координат 0).

Как и следовало ожидать, производственная себестоимость СФЗ возрастает при попытке обеспечить вероятность R, равную единице. В то же время эксплуатационные затраты на СФЗ, обусловленные мерами по совершенствованию системы и оптимизации ее технического обслуживания и ремонта, имеют тенденцию к уменьшению. Оценкой общих затрат на СФЗ является сумма ординат, описывающих затраты $C_Р + C_П$ и $C_Э$.

Динамика изменения затрат на СФЗ, приведенная на рис. 3, сохраняется также при анализе зависимости затрат от уровня БПУ, присущих данному ПО. Условия снижения указанных затрат до минимума формулируются так[6]: "Издержки предотвращения угроз и ущербов или расходы на содержание системы должны сравняться с ущербами и потерями от состоявшихся угроз". И далее (там же): "Чтобы минимизировать общие затраты, предприятия должны определить и принять некоторый оптимальный (ненулевой) уровень финансовых потерь. Отклонения от этого оптимального уровня в любую сторону являются нежелательными".

Показатель затрат на применение (эксплуатацию) СФЗ

Для СФЗ, производственная себестоимость которой известна, показатель затрат на применение (эксплуатацию) СФ имеет вид:

$$C_Э = C_{ПЗ} + (к_{АО} \times C_{КСБ}),$$

где $C_{ПЗ}$ – плановые затраты на эксплуатацию СФЗ (руб/год); $K_{АО}$ – коэффициент, определяющий уровень ежегодных амортизационных отчислений (без учета влияния инфляции) на приобретение исправных технических средств для замены изношенных экземпляров.

Влияние инфляции на эксплуатационные затраты СФЗ характеризуется следующими особенностями:

● инфляция обусловливает необходимость учета такого понятия, как "стоимость денег во времени";

● размер затрат на СФЗ, достигаемый в рамках годовой инфляции, принимается в новом году в качестве базового значения, от которого начинается новый отсчет;

● измерение разновременных (текущих и будущих) затрат на эксплуатацию СФЗ в одном масштабе осуществляется с помощью метода дисконтирования.

Пути оптимизации затрат на СФЗ

Можно выделить в качестве приоритетных следующие пути оптимизации затрат на СФЗ:

● на предпроектной стадии создания СФЗ – полнота сбора исходных данных, необходимых для разработки и согласования проектных документов (позволяет минимизировать число ошибок, которые придется устранять при монтаже технических средств СФЗ и на этапе ввода ее в действие);

● на этапе разработки технического задания на создание СФЗ – дифференцированный подход к предъявлению технических требований к качеству СФЗ (обеспечивает объективный подход к выбору приемлемых по стоимости технических средств для нейтрализации БПУ);

● на стадии опытной эксплуатации СФЗ – своевременное выявление причин, снижающих качество технической эксплуатации СФЗ (позволяет своевременно разработать обоснованные рекомендации по улучшению организации эксплуатации системы).

Вариант многокритериальной оптимизации затрат на эксплуатацию СФЗ

Многокритериальная оптимизация производится из условия соблюдения неравенства: размер предотвращенного ущерба от воздействия БПУ превышает затраты на эксплуатацию СФЗ (предотвращенный ущерб рассматривается здесь в качестве показателя экономической эффективности функционирования СФЗ).

Требуется, с одной стороны, максимально увеличить указанный ущерб, а с другой – максимально снизить затраты на эксплуатацию СФЗ. Указанная задача может быть представлена в следующем виде:

$$U_{ПУ} - [C_{ПЗ} + (K_{АО} \times C_{КСБ})] \to \max$$

при системе ограничений

$$U_{ПУ} \geqslant C_{ПЗ} + K_{АО} \times C_{КСБ};$$
$$K_{АО} \times C_{КСБ} \leqslant K_{АО} \times C_{max};$$
$$C_{ПЗ} \leqslant C_{КСБ};$$
$$U_{ПУ}, C_{ПЗ}, K_{АО}, C_{КСБ} \geqslant 0.$$

Сформулированная задача решается путем приведения ее к однокритериальной задаче, что может быть достигнуто при $U_{ПУ}$ = const и $C_Э$ = var.

Разработка проектной документации

Разработка проектной документации проводится на основании задания на проектирование, с учетом ТЗ на модернизацию СФЗ и исходных данных на проектирование, представляемых заказчиком. К указанным данным в общем случае относятся[7]:

● генплан территории ПО с инженерными коммуникациями;

[5] Ревин С.М., Грачев Д.Д. Современные методы и инструменты оценки уязвимости, эффективности инженерно-технической и физической защиты особо важных объектов // Сборник трудов XIX Международной научной конференции. М.: Академия управления МВД России, 2010. С. 194.

[6] Гапоненко В.Ф., Гитинов А.Г. Некоторые проблемы обеспечения экономической и информационной безопасности предприятий региона // Сборник трудов XVIII Международной научной конференции. М.: Академия управления МВД России, 2009. С. 6.

[7] Кузьмин В.Ю. Проектирование СФЗ критически важных объектов// Сборник научных трудов (выпуск №4). М.: ТЦСБ СНПО "Элерон", 2013. С. 105–113.

- архитектурно-строительные чертежи зданий и сооружений, подлежащих оснащению комплексом ТСФЗ, в том числе поэтажные планировки, фасады, разрезы;
- категорирование зданий и помещений по требованиям физической безопасности;
- перечень объектов блокирования;
- места расположения контрольно-пропускных пунктов (внешних и внутренних), интенсивность перемещения персонала;
- места расположения пунктов управления (центрального и локальных);
- указание на планировках зданий мест расположения рабочих, аварийных и технологических выходов из категорированных зон;
- процедуры постановки/снятия под охрану объектов блокирования;
- процедуры проходов в охраняемые зоны, помещения;
- перечень абонентов прямой телефонной связи и места установки периферийных устройств системы громкоговорящей связи.

Разработке технического задания предшествует проведение проектно-изыскательских работ в местах размещения ТСФЗ.

Проектно-изыскательские работы

Указанные работы предусматривают:

- уточнение исходных данных, выданных заказчиком, и условий работы функциональных подсистем СФЗ в местах их размещения, включая оценку техногенной и природной помеховой обстановки (оказывает существенное влияние на выбор того или иного технического средства защиты);
- осуществление "привязки" мест установки ТСФЗ;
- определение основных трасс и способов прокладки кабельных соединительных линий комплекса ТСФЗ;
- сбор исходных данных для разработки сметной документации.

Сметная документация

Разрабатывается для определения стоимости работ по реализации проектных решений, составляющими которой являются:

- стоимость ТСФЗ, подлежащих приобретению для комплектования функциональных подсистем, и программного обеспечения средств защиты информации;
- стоимость работ по установке, монтажу и настройке технических средств;
- стоимость сопутствующих инженерных решений СФЗ.

Оценка стоимости проектных работ

Стоимость указанных работ определяется как сумма затрат на выполнение следующих видов работ:

- выявление уязвимости ПО;
- проведение проектно-изыскательских работ;
- разработка проектно-сметной документации и рабочей документации на СФЗ.

Монтаж и ввод в действие модернизированной СФЗ

Ввод в действие СФЗ предусматривает поэтапное выполнение мероприятий:

- испытания;
- оценка и подтверждение соответствия СФЗ;
- опытная эксплуатация СФЗ.

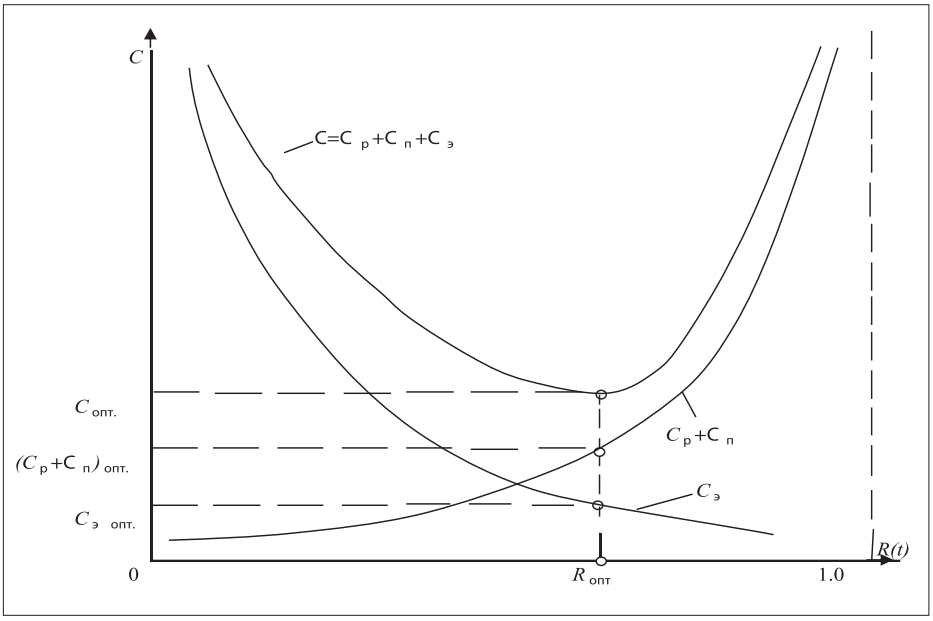


Рис. 3. Графический прием построения зависимости затрат на СФЗ от вероятности ее безотказной работы

Испытания СФЗ

Проводятся для проверки работоспособности и правильности функционирования СФЗ в заданных условиях эксплуатации. Содержание и порядок проведения испытаний устанавливают в программе испытаний, составляемой контрагентами ПО (разработчиком и изготовителем СФЗ) по согласованию с заказчиком СФЗ.

Оценка и подтверждение соответствия СФЗ

Оценка соответствия СФЗ требованиям ТЗ заключается в прямом или косвенном определении соблюдения указанных требований, а подтверждение соответствия – в документальном удостоверении соответствия СФЗ условиям договора ПО (заказчик) с контрагентами и распространяющимся на нее НТД.

В практическом плане подтверждение соответствия СФЗ может быть только компромиссным, основанным на обобщении результатов:

- инспекционного контроля органом по сертификации полноты и правильности (качества) проектных решений СФЗ на месте ее эксплуатации;
- проведения аккредитованной испытательной лабораторией, привлекаемой для оценки соответствия СФЗ, полного набора операций в рамках принятых ею договорных обязательств.

Документальным удостоверением соответствия СФЗ (входящих в ее состав функциональных подсистем) могут быть:

- для СФЗ в целом – декларация о соответствии, принимаемая изготовителем СФЗ (см. ст. 23 Федерального закона от 27.12.2002 г. № 184-ФЗ "О техническом регулировании", с изм. от 1 мая 2007 г. № 65-ФЗ);
- для функциональных подсистем СФЗ – сертификаты соответствия, выдаваемые органом по сертификации.

Опытная эксплуатация СФЗ

Основными задачами опытной эксплуатации СФЗ являются:

- учет суммарной наработки СФЗ и функциональных подсистем в отдельности, а также календарной продолжительности эксплуатации с целью уточнения декларированной разработчиком безотказности СФЗ;
- учет данных о выявленных неисправностях и обусловленных ими отказах функциональных подсистем, установление видов и причин указанных неисправностей, разработка мероприятий по оперативному воздействию на показатели качества СФЗ.

Опытная эксплуатация СФЗ осуществляется специалистами ПО, владеющими необходимым опытом работы с системой, в течение календарного срока, установленного в ТЗ на модернизацию СФЗ.

В течение опытной эксплуатации СФЗ, абстрагируясь от контроля за соблюдением персоналом ПО правил эксплуатации СФЗ, контрагенты ПО выполняют следующие виды работ, подпадающие под гарантийный надзор:

- оперативное и безвозмездное устранение дефектов, выявленных в процессе эксплуатации;
- оказание помощи специалистам ПО в выполнении сложных операций технического обслуживания и ремонта СФЗ в период их освоения;
- изучение опыта эксплуатации СФЗ в интересах накопления сведений о надежности СФЗ, удобстве ее технического обслуживания, экономическом или ином эффекте от применения.

Продвинутый подход

Рассмотренный алгоритм обеспечения физической безопасности ПО содержит предметное описание совокупности процедур, необходимых для выполнения основной задачи СФЗ – пресечения актов незаконного вмешательства нарушителя в деятельность ПО.

Приведенный в статье системный подход к модернизации СФЗ созвучен современной парадигме физической безопасности ПО, характеризующей состояние его защищенности от АНВ. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Только без жертв!

Как минимизировать последствия ЧС на производстве

Сергей Полухин
Руководитель направления видеоаналитики для безопасности предприятий и городов компании TRASSIR

Специалисты по безопасности постоянно говорят, что угрозу лучше предотвратить, чтобы потом не столкнуться с последствиями ее реализации. Поскольку это утверждение – не более чем аналог известного принципа "Лучше быть богатым и здоровым, чем бедным и больным", оспаривать его бессмысленно. Данная истина абсолютна, поэтому на практике зачастую бывает бесполезна. А что полезно?

Снизить риск возникновения чрезвычайных ситуации можно с помощью интеллектуальных технических средств безопасности

Аварии были, есть и будут. Любые профилактические меры могут только снизить вероятность возникновения чрезвычайной ситуации, но 100%-ной гарантии не дают, в том числе и потому, что не могут устранить их главную причину – человеческий фактор.

Реальность, как она есть

Август, 2018 год. В Нижегородской области в результате аварии на производстве боеприпасов погибли три человека. Еще два погибли из-за взрыва в самарском филиале завода "Кузнецов"[1].

Февраль, 2019 год. Сразу в трех городах Кузбасса выпал черный снег. В ходе расследования выяснилось, что два предприятия превысили допустимую норму выбросов пыли и сажи в атмосферу. По результатам возбуждено два уголовных дела[2].

Май, 2019 год. На химкомбинате в Березниках произошел взрыв, в результате которого погибло три человека. Виновными в происшествии были признаны несколько руководителей среднего звена, которым в качестве наказания назначены различные сроки заключения[3].

Полный список чрезвычайных ситуаций на российских предприятиях слишком велик, чтобы приводить его в статье. Конечно, положительная динамика имеет место. Например, в 2018 г. их число сократилось почти на 16%, в первую очередь благодаря профилактическим мерам – количество предупреждений Ростехнадзора тоже выросло на 10%[4]. Но о полной победе над аварийностью говорить рано. Нельзя исключать, что этот идеал не будет достигнут никогда. На всех упомянутых предприятиях проходили проверки. Их руководство наверняка принимало какие-то меры, направленные на повышение безопасности производства.

Но никто не может гарантировать, что у ответственного сотрудника в какой-то день не заболит голова и он недостаточно тщательно проверит надежность закрытия вентилей. Ничто не спасет от порыва ветра, который унесет непогашенный окурок по направлению к складу. Все работает так, как должно, только в идеальных системах, а не в реальной жизни.

"Неизбежная в море случайность"

Почему морское ведомство дореволюционной России придало официальный статус этому ничего не объясняющему термину? Не исключено, что прежде всего для того, чтобы не тратить время на поиски виноватого, когда нужно решать конкретные насущные задачи.

Есть распространенная и ошибочная точка зрения, согласно которой обеспечение безопасности сводится к предотвращению угроз. В действительности речь идет о минимизации ущерба от них.

Вот пример: на складе готовой продукции случился пожар – загорелись несколько пустых упаковок, рядом с которыми находились коробки с дорогим товаром. Если рабочий вовремя это заметил и успел отнести ценные предметы в недосягаемое для огня место, то реализация угрозы есть, а ущерба от этого никакого.

Безусловно, данный пример не отрицает необходимости профилактических мер. Он говорит только об их недостаточности для реализации на предприятии эффективной политики безопасности. В общем случае она должна включать в себя несколько равноценных составляющих:

- меры, направленные на минимизацию количества типов угроз;
- меры, направленные на минимизацию реализации существующих угроз;
- меры, направленные на минимизацию ущерба от реализации существующих угроз.

[1] *https://www.1tv.ru/news/2018-08-31/351513-avarii_v_rezultate_kotoryh_pogibli_lyudi_proizoshli_srazu_na_dvuh_rossiyskih_predpriyatiyah*
[2] *https://dprom.online/chindustry/ugolovnoe-delo-za-chernyj-sneg/*
[3] *http://rcc.ru/category/6*
[4] *https://srgroup.ru/news/eco/industry_news/glava-rostekhnadzora-aleksey-aleshin-ob-avariyakh-proverkakh-i-predosterezheniyakh/*

Главная причина аварий – человеческий фактор

Последний пункт особенно важен на объектах с высоким уровнем непредсказуемости рисков, например на крупных производственных площадках, где причиной чрезвычайной ситуации может стать множество факторов, учесть которые заранее практически невозможно. Именно поэтому руководству таких предприятий следует уделять особое внимание устранению последствий реализации угроз – быстро локализовать место происшествия и организовать эвакуацию людей.

Все поддается оценке

Только человеческая жизнь бесценна. Грамотные меры по ликвидации последствий ЧС позволяют либо избежать человеческих жертв, либо существенно сократить их количество.

Если на предприятии происходит утечка вредных веществ, первостепенная задача при ликвидации ее последствий – обнаружение потерявших сознание людей и их эвакуация из опасной зоны. Важно сделать это как можно быстрее, пока их еще можно спасти.

Но усложняет решение этой задачи то, что некоторые сотрудники могут находиться в труднодоступных местах. Осматривать все в данной ситуации – бесполезная трата времени. Желательно точно знать, где именно находятся люди, которым необходима незамедлительная помощь.

Вторая задача, возникающая при ликвидации последствий ЧС, – спасение дорогостоящего имущества, например вычислительной техники или специального технологического оборудования.

Если в административном здании прорвало трубу и вода начинает заливать оргтехнику, что-то наверняка пострадает. Но все-таки лучше потерять один компьютер, а не десять. На первый взгляд, ситуация банальная: обслуживающий персонал закрывает вентиль и каждый сотрудник спасает то, что ближе лежит. А если это случилось ночью или в выходной, когда в здании находится только дежурная смена службы безопасности? Им надо не только быстро узнать про аварию, но и выяснить, какие помещения залиты водой, чтобы приступить к выносу имущества. Только в этом случае ущерб будет относительно невелик.

Допустим, последствия ЧС уже устранены. Означает ли это, что можно переворачивать страницу? Вовсе нет.

Руководству компании важно получить максимально объективную информацию о происшествии и действиях должностных лиц во время ликвидации последствий. Не исключено, что в качестве некой компенсации за причиненный ущерб оно именно так сможет заметить сотрудника, способного принимать быстрые и правильные решения в сложных ситуациях.

Наконец, есть еще одно обстоятельство, про которое не следует забывать: если результатом ЧС стали человеческие жертвы, то у него будут юридические последствия. И весьма вероятно, что признанный виновным руководитель получит срок по приговору суда.

За всем не уследишь

Без специальных технических средств – действительно никак. Причем совершенно не обязательно, что для этого потребуются дорогие и технически сложные инструменты.

Материальные потери в случае с прорывом трубы были бы минимальны при использовании обычных датчиков протечки, сигнал из которых выводится на центральный пульт. В этом случае дежурная смена не только будет сразу же оповещена о начале ЧС, но и получит информацию о помещениях, которым угрожает опасность.

В примере с возгоранием на складе дела обстоят несколько сложнее. Обычные дымовые извещатели срабатывают слишком поздно, в лучшем случае через 15–20 секунд после начала возгорания. Конечно, их наличие поможет предотвратить большой пожар, но часть товара при этом пострадает.

Гораздо эффективнее в данных ситуациях будут более сложные технические решения. Например, системы видеонаблюдения с аналитическим модулем. Они не только быстрее регистрируют появление очага возгорания, но и могут выполнять ряд диспетчерских функций. В частности, система управления видеоданными (камера, сервер, ПО) позволяют найти сотрудника, который в данный момент времени находится ближе всего к опасной зоне, чтобы направить его на ликвидацию ЧС по ближайшему маршруту.

Наиболее эффективны сложные интегрированные системы, собирающие информацию с множества датчиков и видеокамер, а также имеющие возможность подавать управляющие сигналы на различное электромеханическое оборудование. С их помощью можно решить большинство проблем, связанных с ликвидацией последствий ЧС.

Довериться умной технике

Чрезвычайная ситуация на крупных производствах, как правило, означает реализацию множества различных угроз – возгорания, отключения электропитания, задымления помещений токсичными продуктами сгорания... Зачастую все это усугубляется паникой сотрудников, стремящихся быстрее выбраться из опасной зоны.

Основная сложность в таком случае заключается в быстром изменении обстановки: пригодный минуту назад для эвакуации коридор заполняется дымом, у одного из выходов внезапно образуется давка, упавшая балка закрывает проход и т.д.

Диспетчер не в состоянии быстро оценить ситуацию, найти максимально безопасный маршрут и направить к нему сотрудников, находящихся в опасной зоне. Техника справится с этой задачей значительно лучше, причем управление эвакуацией в данном случае будет происходить автоматически посредством включения световых указателей и ламп аварийного освещения. Ориентируясь по их сигналам, люди быстрее доберутся до выхода из помещения.

Если система обнаружит людей, которые по каким-либо причинам не могут самостоятельно добраться до безопасного места, к ним будут высланы спасательные группы. При этом их маршрут формируется таким образом, чтобы они оказали помощь максимальному количеству пострадавших.

Наконец, когда последствия ЧС будут благополучно устранены, руководство сможет проанализировать записи. Это позволит найти виновных, поощрить отличившихся и принять меры для предотвращения подобных ситуаций в будущем.

Таким образом, сложные технические системы безопасности помогут не только предотвратить реализацию потенциальной угрозы, но и минимизировать ущерб, если беда все-таки произойдет. Так они позволят предприятию быстрее вернуться в нормальный рабочий режим и избежать невосполнимых потерь. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

Интеллектуальные здания: возвращение к истокам

В ноябре 1992 г. две известные компании – Honeywell и AT&T – разработали систему SYSTIMAX®, в которой обеспечивалась взаимосвязь инженерного оборудования и систем управления с использованием сети передачи данных. Применительно к этой системе практически впервые было употреблено понятие "интеллектуальное здание". Термин прижился и понравился настолько, что стал использоваться маркетологами чрезвычайно активно и даже бездумно...

Владимир Максименко
Эксперт сектора обучения и информационной поддержки
ЗАО НВП "Болид"

Завтрашние проблемы могут быть решены только с помощью интеллектуальных сетевых зданий – так называемых интеллектуальных зданий
Light + Building 2020

Чтобы навести какой-то порядок в применении термина "интеллектуальное здание", а также помочь отечественным специалистам освоить современную международную нормативную базу в активно развивающейся области автоматизации инженерных систем зданий, в НП "АВОК" был создан комитет "Интеллектуальные здания и информационно-управляющие системы".

Создание фундамента

В комитет были приглашены ведущие специалисты отечественных и зарубежных компаний, работавших в России с проектами автоматизации инженерного оборудования зданий. В результате активной деятельности комитета появилось рабочее определение интеллектуального здания: "Интеллектуальным можно назвать здание, которое обеспечивает оптимальную среду обитания, адаптивную и эффективную, с точки зрения затрат в течение всего жизненного цикла здания – от проектирования до утилизации".

В данном определении эффективность – это достижение минимальных затрат при заданном качестве. Ввиду острой нехватки современных нормативных документов в области автоматизации зданий комитет, используя широкие международные связи НП "АВОК", начал активно сотрудничать с комитетом ISO/TC 205, рабочей группой 3 (WG3). В результате этого сотрудничества на основе стандарта ISO 16484 вышли в свет две части стандарта НП "АВОК" "Системы автоматизации и управления зданиями" и трехъязычный словарь терминов по автоматизации зданий. Структура комплекса стандартов АВОК соответствует ГОСТ 34.003–90 "Термины и определения" и ГОСТ 34.001–90 "Основные положения". Таким образом, усилиями комитета появились современные нормативные документы в области интеллектуальных зданий, адаптированные к отечественной терминологии и графическим обозначениям.

Новый этап – протоколы автоматизации

Тем временем в России стало активно развиваться высотное строительство, которое потребовало как новых технологий, так и новой нормативной базы, в том числе и в области автоматизации зданий. Большой интерес вызвало применение рекомендованных стандартом ISO 16484 открытых протоколов автоматизации KNX, LON, BACNet и ряда других. Постепенно сошли на нет дебаты по поводу того, какой протокол лучше, уступив место профессиональному владению особенностями их использования. Проекты автоматизации инженерного оборудования стали находить все более широкое применение на самых разных объектах благодаря своей энергоэффективности, надежности и комфорту. Появились межпротокольные шлюзы и IP-преобразователи протоколов, что облегчило работу разных протоколов в одном проекте.

Качественный скачок

Все эти события постепенно готовили почву для качественного скачка. Совершенствование интеллектуальных зданий способствовало их более глубокому взаимодействию с системами безопасности и появлению конвергентных проектов. Использование облачных технологий, Big Data, Интернета вещей и элементов искусственного интеллекта привело к появлению когнитивных зданий.

Активное применение интернет-технологий для обеспечения безопасности и управления создало предпосылки для перехода к новому пониманию интеллектуального здания как подключенного здания. Спиралевидное развитие общества – неотъемлемая часть диалектики Гегеля – в отношении интеллектуального здания выразилось в возвращении к исходному термину на более высокой стадии.

Новое содержание

Любопытно наблюдать на современных отечественных мероприятиях то же бездумное применение термина "интеллектуальное здание", как и 20 лет назад, еще и усиленное напористостью малообразованных "эффективных менеджеров". Однако не это, к счастью, определяет суть вопроса.

ИТ-технологии уже так плотно окружают нас, что и понятие интеллектуального здания впитало в себя новое содержание:

- подключенные здания, все системы которых обмениваются данными с внешним миром и используют его ресурсы;
- искусственный интеллект, поднимающий сервис и надежность зданий на качественно более высокий уровень;
- информационное моделирование зданий (BIM), позволяющее на стадии проектирования обеспечить соответствие кибербезопасности, противопожарной защиты, управления инженерными системами, видеотехнологий, интеллектуального управления доступом, систем охраны и сигнализации, взаимосвязи технологий и предоставления услуг существующей правовой базе.

Миссия выполнена

Уже применение интеллектуальных технологий в управлении и интеграции систем зданий обеспечивает реализацию изначальной задачи создания оптимальной среды обитания, адаптивной и эффективной, с точки зрения затрат в течение всего жизненного цикла здания – от проектирования до утилизации.

Айрис Джеглица-Мошаге, старший вице-президент Messe Frankfurt, отмечает: "Связь может генерировать интеллект и, следовательно, экономическую эффективность, когда все строительные системы взаимодействуют между собой. Потому нужен общий язык. Таким образом, полностью интегрированное цифровое планирование систем безопасности, охраны и строительных услуг является необходимостью для будущего". ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

ОПС. ПОЖАРНАЯ БЕЗОПАСНОСТЬ

Инфракрасный адресный извещатель пламени С2000-ПЛ

Производитель: ЗАО НВП "Болид"
Сертификат: RU C-RU.ЧС13.В.00001/18, выдан ПОЖТЕСТ
Назначение: обнаружение открытого пламени и выдача извещений "Пожар"
Особенности:
- работа под управлением контроллера ДПЛС "С2000-КДЛ" в составе интегрированной системы охраны "Орион"
- первый класс чувствительности к пламени (по ГОСТ 53325–2012)
- высокая помехоустойчивость
- низкая чувствительность к электродуговой сварке
- автоматический контроль работоспособности, при некорректной работе выдача извещения "Неисправность"
- на С2000-ПЛ серия 01 контроль работоспособности ведется ИК-светодиодом 4,3 мкм
- хранение адреса извещателя в энергонезависимой памяти
- световая индикация состояния извещателя

Возможности:
- вывод значения напряжения в ДПЛС в месте установки
- вывод текущей мощности входного сигнала (обстановка в поле наблюдения)
- ручная проверка работоспособности лазерным тестером с получением извещения "Тест"

Характеристики:
- максимум спектральной чувствительности 4,3 мкм
- дальность обнаружения типовых пожаров ТП5, ТП6 не менее 25 м
- время обнаружения пламени не более 30 с
- угол обзора 70 град.
- устойчивость к свету лампы накаливания не менее 250 лк
- устойчивость к свету люминесцентной лампы не менее 2500 лк
- степень защиты оболочки IP65
- диапазон рабочих температур от -25 до +55 °С
- время технической готовности не более 30 с
- напряжение питания от 8 до 11 В
- потребляемый ток не более 0,5 мА

Время появления на российском рынке: I квартал 2020 г.
Подробная информация: https://bolid.ru/production/orion/ops-subsystems/spi2000a/s2_pl.html
Фирма, предоставившая информацию: БОЛИД, НВП, ЗАО

Блоки речевого оповещения "Рупор исп.02", "Рупор исп.03" и блок расширения "Рупор-БР"

Производитель: ЗАО НВП "Болид"
Сертификат: RU C-RU.ЧС13.В00108/19, выдан ПОЖТЕСТ

Назначение: для построения систем оповещения на небольших объектах с использованием низкомных речевых оповещателей серии ОПР-С0, ОПР-П0 или аналогичных с сопротивлением 4 или 8 Ом
Особенности:
- компактный размер ("Рупор исп.02")
- возможность ретрансляции сигналов ГО и ЧС или подключения внешнего микрофона ("Рупор исп.03")
- 4 предварительно записанных речевых сообщения
- регулируемая выходная мощность (5 уровней от 5 до 40 Вт)

Возможности:
- управление и контроль по интерфейсу RS-485
- увеличение площади зоны оповещения с помощью блоков расширения "Рупор-БР"
- возможность самостоятельного изменения речевых сообщений в памяти блоков

Характеристики:
- максимальная выходная мощность 40 Вт
- допустимый диапазон сопротивлений линии оповещения от 4 до 22 Ом
- общая продолжительность речевых сообщений 84 с
- основное питание: 220 В, 50 Гц ("Рупор исп.03" и "Рупор-БР"), 10–28 В ("Рупор исп.02")
- резервное питание – АКБ 12 В, 7 Ач ("Рупор исп.03" и "Рупор-БР"), 10–28 В ("Рупор исп.02")
- интерфейс RS-485, протокол "Орион"
- энергонезависимый буфер событий – 256 событий ("Рупор исп.02", "Рупор исп.03")
- степень защиты оболочки IP30
- диапазон рабочих температур от -10 до +55 °С
- относительная влажность воздуха до 98% при +25 °С
- габаритные размеры блока: 211x165x89 мм ("Рупор исп.03" и "Рупор-БР"), 102x107x39 мм ("Рупор исп.02")
- материал корпуса – пластик
- масса блока: 0,2 кг ("Рупор исп.02"), 2,95 кг ("Рупор исп.03" и "Рупор-БР" с АКБ)

Время появления на российском рынке: I квартал 2020 г.
Подробная информация: https://bolid.ru/production/orion/sound-notice/rupor_02.html, https://bolid.ru/production/orion/sound-notice/rupor_03.html, https://bolid.ru/production/orion/sound-notice/rupor-br.html
Фирма, предоставившая информацию: БОЛИД, НВП, ЗАО

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Дверной доводчик TS Match

Производитель: dormakaba
Сертификат: информация не предоставлена
Назначение: устройство для самозакрывания двери гидравлическое регулируемое
Особенности: бюджетное решение со скользящим каналом
Возможности: для дверей шириной до 1250 мм
Характеристики:
- усилие EN3-4, EN3-5
- максимальная масса двери до 120 кг
- универсальный монтаж
- ветровой тормоз

Ориентировочная цена: 5100 руб. (розничная)
Время появления на российском рынке: январь 2020 г.
Подробная информация: https://www.dormakaba.com/ru-ru/products/products/door-hardware/doorclosers-dormakaba/–ts-match-558866
Фирма, предоставившая информацию: дормакаба Евразия, ООО

Вызывная панель DS06A в исполнении DsxxxP-3L

Производитель: НПП "Бевард"
Сертификат: информация не предоставлена
Назначение: однабонетская вызывная видеопанель с трехканальным контроллером

Особенности:
- полное дуплексное аудио
- интеллектуальное эхоподавление
- открытие двери по распознаванию лица со встроенной базой на 30 лиц
- подключение трех исполнительных устройств

Возможности:
- поддержка SIP-протокола
- открытие двери с сотового телефона без приложений (DTMF)
- управление с ПК, ноутбука или мобильного устройства под Android и iOS
- работа с облачным сервисом CamDrive
- уникальный поворотный антивандальный корпус

Характеристики:
- 1,3 Мпкс сенсор SONY Exmor нового поколения
- эксплуатация при температурах от -40 до +50 °С
- ИК-подсветка до 10 м
- питание PoE или 12 В

Ориентировочная цена: 15 000 руб. (опт 2)
Подробная информация: www.beward.ru
Фирма, предоставившая информацию: БЕВАРД, НПП

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 127–128 "Ньюсмейкеры"

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 127–128 "Ньюсмейкеры"

ВИДЕОНАБЛЮДЕНИЕ

BOLID RGG-1622 Версия 2

Производитель: ЗАО НВП "Болид"
Сертификат: № RU C-RU. ME61.B.01269, выдан ОС "МНИТИ-СЕРТИФИКА"
Назначение: запись и отображение видеоизображения с аналоговых и сетевых видеокамер
Особенности:
- запись звука с камер через коаксиальный кабель
- управление моторизированными приводами камер через коаксиальный кабель
- встроенная видеоаналитика, захват лиц
- RealTime запись 1080p (25 кадр/с на канал)
- до 24 каналов в гибридном режиме

Возможности: отображение, запись, воспроизведение, снимок, PTZ-управление, отправка письма по e-mail, передача видеозаписи по FTP, включение звукового предупреждения и вывод информации на монитор
Характеристики:
- поддержка двух встраиваемых жестких дисков емкостью до 10 Тбайт каждый
- поддержка камер форматов: CVI, TVI, AHD, CVBS, IP
- макс. разрешение записи 4K
- макс. разрешение вывода 4K
- IP-входы:16 + 8 каналов, каждый до 8 Мпкс
- кодек H.265/H.264
- видеоаналитика: вторжение в зону, оставленные/пропавшие предметы, захват (обнаружение) лиц
- напряжение питания 12 В (DC)
- потребляемая мощность не более 20 Вт
- диапазон рабочих температур от -10 до +55 °С
- габариты 375x287x53 мм
- масса 1,7 кг без HDD

Время появления на российском рынке: III квартал 2019 г.
Подробная информация: https://bolid.ru/production/cctv/analog_dvr/1080p/rgg_1622.html
Фирма, предоставившая информацию: БОЛИД, НВП, ЗАО

IP-камера SV2215M

Производитель: НПП "Бевард"
Сертификат: информация не предоставлена
Назначение: сверхчувствительная box-камера для решения сложных задач
Особенности:
- 2 Мпкс сверхчувствительный сенсор 1/1.9" SONY Exmor R до 0,0005 лк (ночь)
- режим высокоскоростной съемки 60 кадр/с
- автоматическая подстройка фокусировки (функция ABF)

Возможности:
- встроенная видеоаналитика на 8 функций (по лицензии)
- аппаратная поддержка расширенного динамического диапазона до 140 дБ
- функция "стабилизация изображения"
- различные уличные исполнения с широким выбором рабочих температур, типов питания, передачи видеосигнала

Характеристики:
- поддержка кодирования H.265/H.264/MJPEG и режима Smart Stream
- питание 12 В или PoE
- поддержка ONVIF profile S и SIP-протокола

Ориентировочная цена: 28 000 руб. (опт 2)
Время появления на российском рынке: I квартал 2020 г.
Подробная информация: https://www.beward.ru
Фирма, предоставившая информацию: БЕВАРД, НПП

IP-камера SV2215RBZ

Производитель: НПП "Бевард"
Сертификат: информация не предоставлена
Назначение: удобная в эксплуатации сверхчувствительная уличная камера
Особенности:
- 2 Мпкс сверхчувствительный сенсор 1/1.9" SONY Exmor R до 0,0005 лк (ночь)
- режим высокоскоростной съемки 60 кадр/с
- встроенная в кронштейн монтажная коробка
- моторизованный объектив 3,6–10 мм с АРД

Возможности:
- встроенная видеоаналитика на 8 функций (по лицензии)
- аппаратная поддержка расширенного динамического диапазона до 120 дБ
- функция "стабилизация изображения"
- ИК-светодиоды III поколения, дальность подсветки до 60 м

Характеристики:
- уличное исполнение, диапазон рабочих температур от -40 до +60 °С, IP67
- поддержка кодирования H.265/H.264/MJPEG и режима Smart Stream
- питание 12 В или PoE
- поддержка ONVIF profile S и SIP-протокола

Ориентировочная цена: 36 100 руб. (опт 2)
Время появления на российском рынке: I квартал 2020 г.
Подробная информация: https://www.beward.ru
Фирма, предоставившая информацию: БЕВАРД, НПП

IP-камера SV5020RBZ

Производитель: НПП "Бевард"
Сертификат: информация не предоставлена
Назначение: удобная в эксплуатации 4K уличная камера
Особенности:
- 8 Мпкс сенсор 1/1.8" SONY Starvis до 0,003 лк (ночь)
- съемка в реальном времени 30 кадр/с при любом разрешении
- встроенная в кронштейн монтажная коробка
- моторизованный объектив 3–11 мм с АРД

Возможности: встроенная видеоаналитика на 8 функций (по лицензии); аппаратная поддержка расширенного динамического диапазона до 120 дБ; функция "стабилизация изображения"; ИК-подсветка до 60 м;
Характеристики: уличное исполнение, от -40 до +60°С, IP67; поддержка кодирования H.265/H.264/MJPEG и режима Smart Stream; питание 12 В или PoE; поддержка ONVIF profile S и SIP-протокола.
Ориентировочная цена: 41 200 руб. (опт 2)
Время появления на российском рынке: I квартал 2020 г.
Подробная информация: https://www.beward.ru
Фирма, предоставившая информацию: БЕВАРД, НПП

TRASSIR NVR 7800R/128-S

Производитель: TRASSIR
Сертификат: информация не предоставлена
Назначение: видеонаблюдение для всех вертикалей бизнеса
Особенности: сетевой видеорегистратор на базе TRASSIR OS (Linux) с записью и воспроизведением до 128 IP-камер. Позволяет организовать АРМ оператора с возможностью подключения до шести мониторов
Возможности:
- удаленный доступ к камерам через приложения TRASSIR
- обнаружение огня и дыма
- управление поворотными PTZ-камерами
- настройка правил и реакций на события
- поиск в видеоархиве по движению в зоне
- мониторинг работоспособности системы через TRASSIR Cloud

Характеристики:
- операционная система TRASSIR OS
- до 128 каналов IP-камер

- до шести подключаемых мониторов (3 x HDMI, 3 x DisplayPort)
- максимальное разрешение вывода до 4K
- разрешение записи: без ограничений
- сетевой интерфейс 2 Ethernet 10/100/1000 Мбит/с
- размер архива 8 HDD размером 3.5"

Ориентировочная цена: по запросу. Проектное оборудование

Время появления на российском рынке: март–апрель 2020 г.

Фирма, предоставившая информацию: DSSL

TRASSIR NeuroStation 8216R/TR

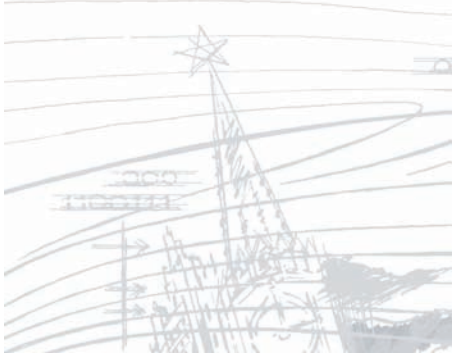
Производитель: TRASSIR

Сертификат: информация не предоставлена

Назначение: видеонаблюдение, интеллектуальное решение для охраны периметра

Особенности:

- нейросетевая видеоаналитика: обнаружение вторжений в охраняемую зону с классификацией типа объекта (человек, транспорт, животное) и специальной логикой фильтрации ложных срабатываний
- обнаружение саботажа видеокамеры при потере сигнала, закрытии объектива, расфокусировки, отворота и засветки
- доставка уведомлений о событиях (в АРМ оператора, мобильные приложения TRASSIR, Telegram, СМС, а также e-mail)
- поддержка интеграции с внешними системами и датчиками



Возможности:

- удаленный доступ к камерам через приложения TRASSIR
- обнаружение огня и дыма
- удаленный контроль отработки тревог
- включение/выключение охранной аналитики с мобильного приложения, а также автоматически по расписанию
- управление поворотными PTZ-камерами
- поиск в видеоархиве по движению в зоне, по событиям видеоаналитики, по сработке внешних датчиков
- прием и обработка видео и отдельных кадров с других серверов TRASSIR (Offload-аналитика)
- мониторинг работоспособности системы через TRASSIR Cloud

Характеристики:

- операционная система TRASSIR OS
- до 16 каналов IP-камер бренда TRASSIR
- видеоаналитика – детектор обнаружения объектов
- разрешение записи: без ограничений
- до двух подключаемых мониторов (1 x D-SUB 1 x HDMI)
- максимальное разрешение вывода до 2K
- сетевой интерфейс 1 Ethernet 10/100/1000 Мбит/с
- размер архива 2 HDD размером 3.5"

Ориентировочная цена: 64 980 руб.

Время появления на российском рынке: март 2020 г.

Фирма, предоставившая информацию: DSSL

IP-камера TRASSIR TR-D2224WDZIR7

Производитель: TRASSIR

Сертификат: информация не предоставлена

Назначение: видеонаблюдение, детекция автономеров

Особенности: камера линейки TRASSIR TREND PRO, оснащенная вариофокальным объективом 5–50 мм с мотор-зумом, создана на базе технологии Sony Starvis. Подходит для работы в паре с системой распознавания автомобильных номеров AutoTRASSIR

Возможности:

- улучшенная цветопередача и детализация изображения
- высокое качество изображения в видимом свете и в области инфракрасной подсветки
- тревожные входы/выходы для интеграции со СКУД

Характеристики:

- матрица 1/2.8" Sony STARVIS CMOS
- разрешение Full HD@25 кадр/с
- чувствительность 0,003 лк (F/1.6) / 0 лк с ИК
- объектив: моторизированный 5–50 мм
- влагозащита IP67

Время появления на российском рынке: октябрь 2019 г.

Подробная информация: https://www.dssl.ru/products/tr-d2224wdzir7-ip-kamera/

Фирма, предоставившая информацию: DSSL

СИСТЕМЫ БЕЗОПАСНОСТИ НЬЮСМЕЙКЕРЫ

А

ААМ СИСТЕМЗ

111250, Москва, Е-250,
ул. Красноказарменная, 14
Тел.: +7 (495) 921-2227
E-mail: aam@aamsystems.ru
www.aamsystems.ru
См. анонс "И снова лучшие: ААМ Системз, партнер HID Global № 1" на стр. 11
См. стр. 23
См. ст. "Биометрическая идентификация в офисе Lamoda" на стр. 81

АЙТИФРОГ, ООО

190005, Санкт-Петербург,
наб. Обводного канала, 118А, лит. Б, офис 224
Тел.: +7 (812) 677-0761
E-mail: info@itfrog.ru
itfrog.ru
См. стр. 18

АРГУС-СПЕКТР, ООО

197342, Санкт-Петербург,
ул. Сердобольская, 65, лит. А
Тел.: +7 (812) 703-7500
E-mail: mail@argus-spectr.ru
www.argus-spectr.ru, стрелец.рф
См. стр. 20
См. ст. "Умные пожарные извещатели нового поколения" на стр. 112, 113

АСТРОН, ОКБ, АО

140080, г. Лыткарино Московской обл.,
ул. Парковая, 1
Тел.: +7 (495) 215-1382
E-mail: info@astrohn.ru
www.astrohn.com, www.astrohn.ru
См. стр. 47

Б

БЕВАРД, НПП, ООО

117198, Москва,
ул. Миклухо-Маклая, влад. 8, стр. 3
Тел.: +7 (495) 505-6341,
+7 (391) 278-9200
E-mail: moscow@beward.ru
www.beward.ru
См. клапан на 1-й обл.
См. стр. 48
См. ст. "КТОТАМ 112 – уникальная система пропуска спецтранспорта на придомовую территорию" на стр. 68, 69
См. стр. 71

БОЛИД, НВП, ЗАО

141070, г. Королев Московской обл.,
ул. Пионерская, 4
Тел.: +7 (495) 775-7155
E-mail: info@bolid.ru
www.bolid.ru
См. стр. 20
См. ст. "Организация СКУД и УРВ на стороне ERP и других систем" на стр. 90, 91

Г

ГИТ СИСТЕМС, ООО
111123, Москва, шоссе Энтузиастов, 56, стр. 32, офис 429
Тел.: +8 (800) 550-8692
E-mail: info@git.company
www.git.company
См. стр. 18

Д

дормакаба Евразия, ООО
117036, Москва,
ул. Дмитрия Ульянова, 7а
Тел.: 8 (800) 250-1576,
+7 (495) 966-2050
E-mail: info.ru@dormakaba.com
www.dormakaba.com/ru-ru
См. стр. 22
См. стр. 93
См. 3-ю обл.

ДССЛ, ООО
105082, Москва, ул. Бакунинская, 71
Тел.: +7 (495) 783-7287
E-mail: info@dssl.ru
www.dssl.ru
См. стр. 76
См. 4-ю обл.

Л

ЛОКАТОРНАЯ ТЕХНИКА
620049, Екатеринбург,
пер. Автоматики, 1
Тел.: +7 (343) 345-0351,
+7 (343) 345-9411
E-mail: md@loktek.ru
www.mdpautina.ru
См. стр. 15

М

МАЛЛЕНОМ СИСТЕМС, ООО
162610, г. Череповец Вологодской обл., ул. Металлургов, 21б
Тел.: +8 (800) 700-3517,
+7 (8202) 20-1635
E-mail: info@mallenom.ru
https://www.mallenom.ru/
См. стр. 74

О

ОХРАННОЕ БЮРО "СОКРАТ", ООО
664002, Иркутск, пер. Волконского, 2
Тел.: +8 (800) 333-6670,
+7 (3952) 640-663
E-mail: sokrat@sokrat.ru
www.sokrat.ru
См. стр. 49

П

ПРОСОФТ-БИОМЕТРИКС
620149, Екатеринбург,
ул. Зоологическая, 9
Тел.: +8 (800) 770-0246
E-mail: sale@bio-smart.ru
www.bio-smart.ru
См. стр. 16

Р

РЕЛЛАЙН, ЗАО
Тел.: +7 (495) 256-8161
E-mail: adm@relline.ru
www.relline.ru
См. стр. 77

РОСТЕВРОСТРОЙ, ПК, ООО
34111, Ростов-на-Дону,
просп. 40-летия Победы, 306А
Тел.: +7 (863) 206-1686, 269-9938
E-mail: 2699935@rostovturniket.ru
www.rostovturniket.ru
См. стр. 19

Т

ТЕКО-ТД, ООО
420138, Казань, просп. Победы, 19
Тел.: +7 (843) 528-0369
E-mail: info@teko.biz
www.teko.biz
См. стр. 46

Ц

ЦЕСИС НИКИРЭТ, ЗАО (ЦЕНТР СПЕЦИАЛЬНЫХ ИНЖЕНЕРНЫХ СООРУЖЕНИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО И КОНСТРУКТОРСКОГО ИНСТИТУТА РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ)
440067, Пенза, ул. Чаадаева, 62
Тел.: +7 (8412) 37-4048 (служба продаж),
+7 (8412) 37-4050 (секретарь)
E-mail: info@cesis.ru, snabsbit@cesis.ru
www.cesis.ru
www.cesis-proekt.ru
См. стр. 115

A

AKUVOX
115088, Москва,
ул. Угрешская, 2, стр. 102
Тел.: +7 (495) 933-1045,
+7 (495) 788-1788
E-mail: akuvox@inprice.ru
Akuvox-rus.ru
См. стр. 19

AXIS COMMUNICATIONS, ООО
125284, Москва,
Ленинградский просп., 31А, стр. 1, этаж 16
Тел.: +7 (495) 940-6682
www.axis.com
См. стр. 17
См. стр. 48

I

IRON LOGIC
195009, Санкт-Петербург,
ул. Бобруйская, 7
Тел.: +7 (812) 241-1853;
+7 (495) 241-3085
E-mail: marketing@ironlogic.ru
ironlogic.ru
См. стр. 16

P

PERCo
194021, Санкт-Петербург,
ул. Политехническая, 4, корп. 2, стр. 1
Тел.: +7 (812) 247-0452,
+7 (812) 247-0450
E-mail: mail@perco.ru
perco.com
См. стр. 9
См. анонс "Система контроля доступа PERCo-Web: новые возможности" на стр. 11
См. стр. 23

Q

QNAP РОССИЯ
117437, Москва, ул. Островитянова, 37 А
Тел.: +7 (495) 587-7627
E-mail: info@qnap.ru
www.qnap.ru
См. стр. 21

R

REDLINE (СОВРЕМЕННЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ)
194044, Санкт-Петербург,
ул. Гельсингфорсская, 3, лит. И
Тел.: +7 (812) 677-1600
E-mail: project@redline-cctv.ru
www.redline-cctv.ru
См. стр. 75

S

SIKLU
43 Hasivim St., 2nd Floor, Petach Tikva, ISRAEL 49517
Тел.: +972-52-8287476
E-mail: Sales-ru@siklu.com, Rusales@siklu.com
Siklu.com
См. ст. "Гигабитный радиолинк Siklu EH-710TX для передачи потока от камер видеонаблюдения" на стр. 44, 45

V

VIDAU SYSTEMS
129085, Москва, ул. Большая Марьинская, 9, стр. 1 офис 107
Тел.: +7 (495) 687-0017, 777-7464
Факс: +7 (495) 742-0044
E-mail: cctv@vidau.ru
www.everfocus.ru ; www.vidau-cctv.ru
См. ст. "Новые революционные видеорегистраторы для транспорта от EverFocus" на стр. 79

dormakaba

МАСТЕР-СИСТЕМЫ

Безграничные возможности по созданию мастер-систем на базе механических цилиндровых механизмов dormakaba

ООО «дормакаба Евразия»
Россия, Москва, 117036
Ул. Дмитрия Ульянова, 7а
8-800-250-15-76
www.dormakaba.ru

НЕЙРОННЫЕ СЕТИ

В ВИДЕОАНАЛИТИКЕ TRASSIR

Быстрее.

Надежнее.

Точнее.

securika Moscow

Живая демонстрация технологий на стенде: D125

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ!

ДЛЯ НОВЫХ ПАРТНЕРОВ TRASSIR
КОМПАНИЙ ИНТЕГРАТОРОВ
*И МОНТАЖНЫХ ОРГАНИЗАЦИЙ**

AUTOTRASSIR® 5

МОДУЛЬ ТРАНСПОРТНОГО КОНТРОЛЯ

Создание списков автоматического пропуска

Установка действий по типу кузова

Распознавание номеров даже в сложных условиях

* Условия акции узнайте удобным для Вас способом:
Внимание! Количество лицензий ограниченно.

www.trassir.ru/AT5
+7 (495) 104-36-08