ается компанией Groteck с 1993 года

СИСТЕМЫ БЕЗОПАСНОСТИ

диалистов

S&S

февраль – март 2018

НА СТЫКЕ ТЕХНОЛОГИЙ

SIP-ДОМОФОН DKS15120

ДЛЯ АНАЛОГОВЫХ
И ЦИФРОВЫХ СЕТЕЙ

BEWARD

www.beward.ru

Лучшие продукты 2018

ДЛЯ АНАЛОГОВЫХ И ЦИФРОВЫХ СЕТЕЙ

IP-домофон BEWARD DKS15120 с поддержкой SIP-протокола предназначен для организации системы IP-домофонии в уже существующей локальной IP-сети без использования дополнительных приложений, кабелей и оборудования.

ПОДДЕРЖКА 9999 АБОНЕНТОВ

SIP

Многоабонентский SIP домофон BEWARD DKS15120 может быть легко внедрен как в сеть Ethernet, так и в координатно-матричную аналоговую сеть многоквартирного дома на 200 абонентов (опция).

1.3 MEGA PIXEL

Exmor SONY

Угол обзора:
137° (по горизонтали)
103° (по вертикали)

RFID

ОДНОВРЕМЕННАЯ ПОДДЕРЖКА ФОРМАТОВ EM-MARIN И MIFARE

- 8 RFID ключей на одного абонента
- Открытие двери по индивидуальному коду абонента
- Резервное хранилище на 8500 RFID ключей и 1500 кодов
- 8 направлений переадресаций вызова на 1 абонента
- Регистрация RFID ключа по индивидуальному коду абонента

МГНОВЕННЫЙ ЗАПУСК

DKS15120 уже через 1 секунду после подачи питания готов отрабатывать базовый функционал, а именно доступ в подъезд и вызов на аналоговые трубки. Даже обновление прошивки не повлияет на отработку базового функционала.

MEMORY

Сменная память со всеми настройками (USB, предустановлена)

РАСШИРЕНИЕ ФУНКЦИОНАЛА

Подключение к домофону DKS15120 устройств расширения с использованием **RS-232** значительно увеличит его функционал:

- Подключение дополнительных устройств: открытие дверей, ворот, шлагбаумов; включение света, сигнализации и т.п.
- Подключение различных охранных датчиков.

дуплекс | -50°C +60°C | Vandal

- ИК-подсветка до 10 м, **III**-поколение
- Морозоустойчивый 8-символьный дисплей
- Выключатель вскрытия концевой
- Подключение дополнительной двери и считывателя 1-Wire для нее
- Удаленное управление освещением подъезда

www.beward.ru

Издается компанией Groteck с 1993 года

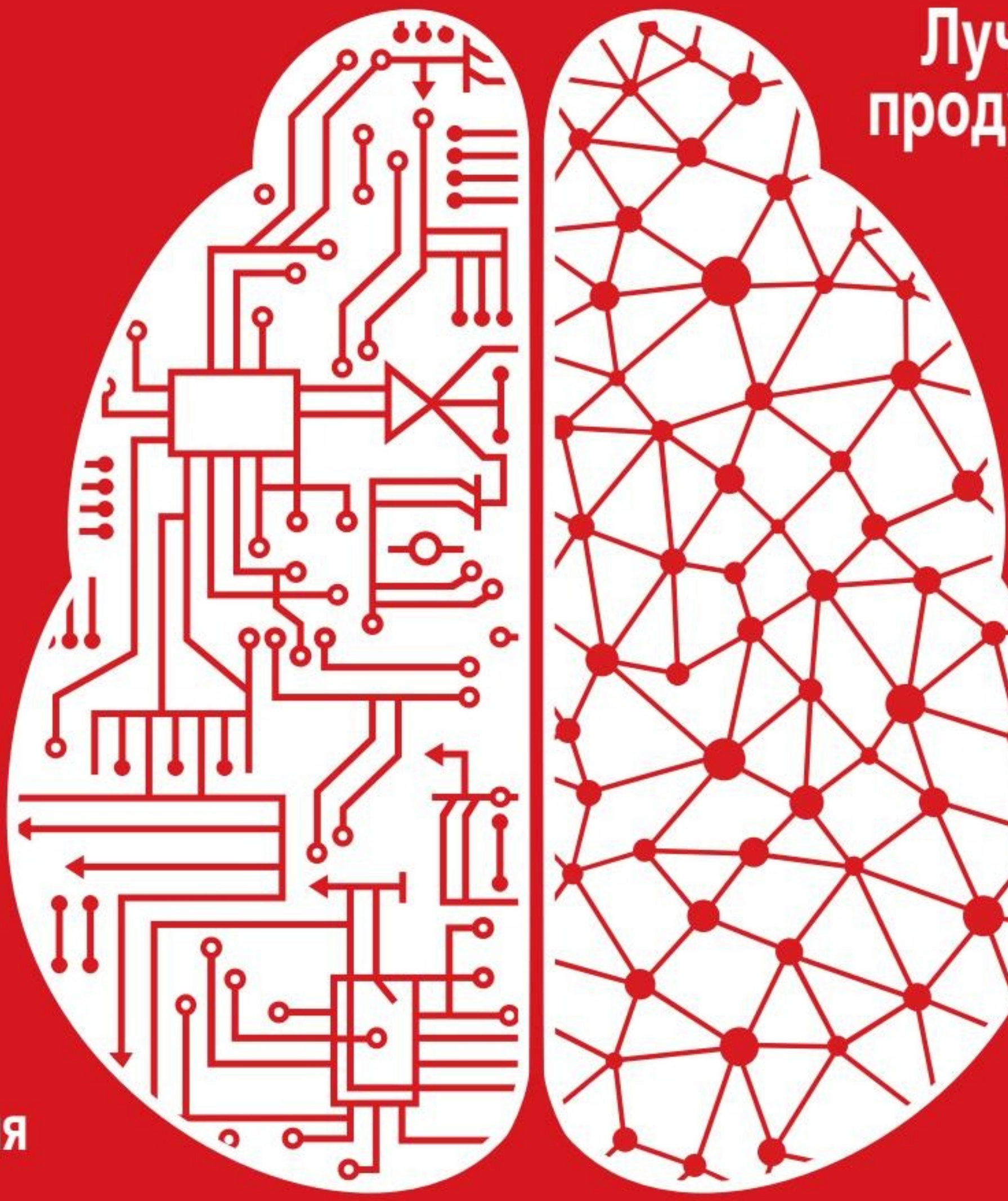
СИСТЕМЫ БЕЗОПАСНОСТИ

Журнал для руководителей и специалистов
в области безопасности
www.all-over-ip.ru

S&S

февраль – март 2018 № 1 (139)

Лучшие продукты 2018



Решения для транспорта

Все дело в мелочах.

Безупречное качество подразумевает превосходное изображение, а также надежность и безотказность устройств. Мы предлагаем комплексную техническую поддержку. Мы сотрудничаем с огромным количеством интеграторов во всех регионах мира и рекордным числом партнеров по программному и аппаратному обеспечению. И мы делаем все, что в наших силах, обеспечения кибербезопасности. Это лишь несколько примеров.

Качество во всем.

Подробную информацию см. на сайте axis.com/quality

AXIS COMMUNICATIONS

Курс на опережающее развитие транспорта

Мы открываем новый деловой сезон двумя направлениями: весенним обзором лучших продуктов и погружением в транспортную безопасность.

Прошедший год стал поистине эпохальным для транспортной сферы, она является одной из первых “гражданских” отраслей, требования к безопасности которой регулируются специальными обязательными нормативными актами. Было принято 15 федеральных законов, которые имеют важное значение для развития транспортной инфраструктуры.
Объем финансовых вложений в транспортный комплекс в 2017 г. составил примерно 1,8 трлн рублей, что составляет 11,3% от общего объема инвестиций в российскую экономику. В сравнении с 2016 г. “аппетит” отрасли вырос на 20%.

При необходимости значительных инвестиций в опережающее развитие транспортной инфраструктуры, а также объективно ограниченных возможностей бюджетов различных уровней активно развивается государственно-частное партнерство. Этот механизм в настоящее время является основным инструментом привлечения средств в транспортные проекты, который к тому же обладает рядом преимуществ перед традиционными государственными закупками. Инвестор, несущий ответственность как за создание, так и за эксплуатацию объектов транспортной инфраструктуры, заинтересован в обеспечении оптимальных технических и ценовых решений.

Эти и другие вопросы обсуждались на конференции “Терроризм и безопасность на транспорте”, которая прошла в рамках форума “Технологии безопасности” 13–15 февраля 2018 г. Мы продолжаем тему на страницах нашего журнала. Авторитетные эксперты рассказывают о тенденциях и делятся своим видением настоящего и будущего систем безопасности в транспортной отрасли, и не только. Вы узнаете:

- о лучших продуктах и решениях индустрии безопасности для транспорта;
- какие инновационные новинки в сфере безопасности приготовила весна;
- о сертификации систем обеспечения транспортной безопасности;
- чем обеспечивается пожарная безопасность РЖД;
- какие новые возможности для транспорта и спорта предлагает видеоидентификация;
- о современных технологиях повышения скорости и надежности передачи данных;
- как подобрать мобильный видеорегистратор;
- о BIM-моделировании для объектов инфраструктуры железнодорожного транспорта;
- зачем нейронные сети промышленности;
- мнения экспертов о платформах для ИБС территориально распределенных объектов;
- почему цифровые технологии меняют будущее транспорта;
- на каких рынках используется машинное зрение и многое другое.

Используйте мнения наших авторов, экспертизу технологических лидеров, адресную информацию для развития вашего бизнеса!

Андрей Мирошкин,
генеральный директор
компании “Гротек”

Наталья Матлахова,
руководитель
направления СБ
компании “Гротек”

Ольга Федосеева,
главный редактор журнала
“Системы безопасности”
компании “Гротек”

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 (139) февраль – март 2018

В НОМЕРЕ

Учредитель и издатель ООО "Гротек"

Журнал "Системы безопасности" № 1 за 2018 г.

Издание зарегистрировано в Комитете РФ по печати

Свидетельство ПИ № 77-16428 от 22.09.03 г.

Для почты: 123007 Москва, а/я 82

E-mail: fedoseeva@groteck.ru; www.secuteck.ru,

тел.: (495) 647-0442; факс 221-0864

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

Цена свободная

События 6

Форум All-over-IP 2018: все меняется, кроме ценностей 6

ТБ Форум 2018: новое качество экспозиции, мощная деловая программа, качественная и интересная аудитория и высокий уровень организации встреч с заказчиками 8

Дайджест 14

Охрана периметра нового качества от "НПЦ "Трезор" 15

50 000 рублей за лучший монтаж. DSSL проводит конкурс #БАШ-МОНТАЖ 17

Спецпроект Лучшие продукты 2018 18

Security and IT Managament 24

Отраслевой фокус Транспорт

Быть оптимистами, верить в собственные силы 24

Максим Соколов, министр транспорта Российской Федерации

Об ИТ-технологиях, работе с подрядчиками, чиповании и роли шофера в транспортной безопасности 26

Константин Коноваленко // X5 Retail Group

Технологии информационного моделирования для создания объектов инфраструктуры железнодорожного транспорта. Практика и перспективы применения 28

Петр Бубнов // СУ-308

Елена Колосова // ООО "К4", Национальная палата инженеров

Кирилл Сухачев // ООО "К4"

Практика внедрения систем видеоидентификации физических лиц на объектах транспортной инфраструктуры 30

Олег Майданский // компания "КРОК"

Видеоидентификация: новые возможности для транспорта и спорта 32

Андрей Хрулев // группа компаний "ЦРТ"

Сертификация систем обеспечения транспортной безопасности: актуальная ситуация на рынке 35

Андрей Зотов // ЗАО НВП "Болид"

Обзор решений спецпроекта "Транспорт" 36

Бизнес, идеи, мнения 44

Секреты демпинга 44

Михаил Бялый // ТД "Актив СБ"

Развитие технологий безопасности службы инкассации Сбербанка 46

Андрей Новиков // ПАО "Сбербанк"

В центре внимания 48

Тест. Облачные Cube IP-камеры 48

Лаборатория климатических исследований CCTVLab

Тест. Мобильные регистраторы для транспорта: в поисках идеального варианта 54

Компания DSSL

СИСТЕМЫ БЕЗОПАСНОСТИ

www.secuteck.ru

№ 1 (139) февраль – март 2018

SECURITY AND SAFETY

Журнал для руководителей и специалистов в области безопасности

В НОМЕРЕ

All-over-IP 60

Транспорту не хватает превентивной безопасности 60
Евгений Ерошин, редактор раздела All-over-IP

Ключевые отличия Stand-alone и мобильного видеонаблюдения, или На что обращать внимание при выборе техники 60
Михаил Жирнов // ООО "БайтЭрг"

Linux неизбежен 62
Мурат Алтуев // компания ITV | AxxonSoft

Современные технологии повышения скорости и надежности передачи данных через глобальные сети 62
Георгий Забадаев // компания IBM

Нейронные сети для задач промышленности и безопасности. Встраиваемые системы машинного зрения нового поколения 66
Борис Вишняков // ФГУП "ГосНИИАС"

Интерком будущего 70
Роман Мишин // независимый эксперт

Рубрика "Цифровая трансформация: AI, IoT, умный город" 72

Новая революция 72
Алексей Коржебин, редактор рубрики "Цифровая трансформация: AI, IoT, умный город"

Город в движении: как цифровые технологии меняют будущее транспорта 72
Виталий Горбушин // компания Oracle

Аналитика как драйвер развития IoT и видеонаблюдения 75
Илья Яськов // компания Seagate

Видеонаблюдение 76

Дорожные штрафы как двигатель видеоаналитики 76
Михаил Арсентьев, редактор раздела "Видеонаблюдение"

Привет из аналогового прошлого. Кибербезопасность и видеонаблюдение 76
Ху Янгжонг // компания Hangzhou Hikvision Digital Technology

Как автоматизировать проектирование систем видеонаблюдения? В поисках волшебного рецепта 78
Евгений Озеров // ЗАО НВП "Болид"

Расширение линейки видеонаблюдения компании BOLID: что нового? 82
ЗАО НВП "Болид"

Видеть сквозь препятствия. Что могут технические системы охраны? 84
Владимир Попов, Константин Аношин // АО "ОКБ "АСТРОН"

Распознавание автомобильных номеров на борту камеры 88
Максим Савельев // компания Hikvision

Техническое обозрение. Мобильные видеорегистраторы 89

Рубрика "Машинное зрение" 94

Век эмоджи, или Как используется машинное зрение на традиционных и новых рынках 94
Андрей Жуков // компания "Техносерв"

Комплексная безопасность, периметровые системы 96

Телега впереди лошади 96
Игорь Васильев, редактор раздела "Комплексная безопасность, периметровые системы"

Автотранспортные КПП. Практика интеграции в систему охраны 98
Сергей Боряк // ООО "Радиорубеж"

СИСТЕМЫ БЕЗОПАСНОСТИ

www.secuteck.ru

№ 1 (139) февраль – март 2018

SECURITY AND SAFETY

Журнал для руководителей и специалистов в области безопасности

В НОМЕРЕ

ОПС, пожарная безопасность 100

Безопасность транспорта под контролем государства 100

Максим Горяченков, редактор раздела "ОПС, пожарная безопасность"

Обеспечение пожарной безопасности железнодорожного подвижного состава: важны качественные, а не количественные результаты 102

Николай Мингалев // ФГП ВО ЖДТ России

Нюансы выбора и правильного расположения громкоговорителей 104

Роман Мишин // независимый эксперт

Пожарная безопасность в ОАО "РЖД" 106

Пресс-служба ОАО "РЖД"

Волоконно-оптические тепловые линейные пожарные извещатели: что предлагает российский рынок? 108

Владимир Фомин // Академия ГПС МЧС России

Рубрика "Беспроводные технологии" 112

В ногу со временем 112

Михаил Левчук, редактор рубрики "Беспроводные технологии"

Беспроводные технологии для обеспечения безопасности на железнодорожном транспорте 112

Василь Кровяков // ООО "СМ-Уфа"

Системы контроля и управления доступом 116

Распределенная многофилиальная СКУД 116

Алексей Гинце, редактор раздела "Системы контроля и управления доступом"

Системы автомобильной идентификации дальнего радиуса действия 116

Александр Фомин // компания "ААМ Системз"

Решения dormakaba для спортивных объектов: высочайший уровень безопасности и комфорта 119

ООО "дормакаба Евразия"

Мнения экспертов. Платформы для интеграции систем безопасности на территориально распределенных объектах с филиальной структурой 120

ГК "Октаграм", ООО "Итриум СПб", компании "КРОК", "ААМ Системз", Bosch Security Systems, ЗАО НВП "Болид", ТП КБПЭ, ООО "АРМО-Системы"

"Дальнобойная" парковочная СКУД: бюджетный комфорт 133

ООО "АРМО-Системы"

Рубрика "Биометрические системы" 134

Осторожность не повредит 134

Василий Мамаев, редактор рубрики "Биометрические системы"

Особенности мультибиометрических технологий 134

Елена Кручинина // независимый эксперт

Данила Николаев // НП "Русское биометрическое общество"

Рубрика "Управление идентификацией" 140

IdM-решения для автоматизации бизнес-процессов: у любой монеты есть две стороны 140

Алексей Плешков // редактор рубрики "Управление идентификацией"

Мнения экспертов. Итоги года в IdM 142

Solar Security, 1IDM, Cisco

Новые продукты 146

Ньюсмейкеры 151

СИСТЕМЫ БЕЗОПАСНОСТИ

www.groteck.com

int@groteck.ru

№ 1 (139) February – March 2018

SECURITY AND SAFETY

Industry Magazine for Security Professionals

FEATURES

Industry Events 6

All-over-IP 2018: Everything Changes But Core Values 6

TB Forum 2018: New Quality of Exhibition, Unparalleled Congress Programme, First-Class Audience, and Exceptional Meeting Service for Connecting Vendors with Customers 8

Industry Digest 14

Advanced Steps to a Better Perimeter Protection from Trezor Russia 15

50,000 RUR for the Best Video Surveillance Installation 17

The Best Security Products 2018 18

Security and IT Managament 24

Transportation Cover Story

Optmism and The Power of Believing in Yourself 24
Maxim Sokolov, Transport Minister of the Russian Federation

The Story of IT Technology, Managing Contractors, Chipping of Retail Goods, and The Role of Truck Drivers in Transportation Security 26
Konstantin Konovalenko // X5 Retail Group

BIM for Railways Infrastructure Development 28
Peter Bubnov // SU-308
Elena Kolosova // K4 Ltd., National Chamber of Engineers of Russia
Kirill Sukhachev // K4 Ltd.

Practical Aspects of Face Recognition for Transportation Applications 30
Oleg Maydansky // CROC

Visual Recognition: New Opportunities for Public Transportation and Sports Industries 32
Andrey Khrulev // Speech Technology Centre

Certification for Transport Security in Russia: Current Situation 35
Andrey Zotov // ZAO NVP Bolid

9 Awesome Security and IT Solutions for Transportation Businesses 36

Business and Ideas 44

Secrets of Dumping 44
Mikhail Byaly // TD Aktiv-SB

Advances in Security Technology for Sberbank Cash Collection Service 46
Andrey Novikov // Sberbank of Russia

Industry Focus 48

Bench Test. IP Cloud Cube Cameras 48
CCTVLab – Climate Research Laboratory

Bench Test. Mobile Video Recorders for Vehicles 54
DSSL

All-over-IP 60

Lacking Proactive Security in Transportation 60
Eugenie Eroshin, Section Editor and Columnist

Key Features of Stand-Alone and Mobile Video Surveillance Solutions 60
Mikhail Zhirnov // ByTerg

Linux Is Inevitable 62
Murat Altuev // ITV | AxxonSoft

Improving Data Transmission Speed and Fault Tolerance over Global Networks 62
Georgy Zabadaev // IBM

Deep Neural Networks to Take On Embedded Vision in Real Industrial and Security Installations 66
Boris Vishnyakov // FGUP GosNIIAS (State Research Institute of Aviation Systems)

The Future of Intercom Technology 70
Roman Mishin // Independent Expert

Digital Transformation: AI, IoT, Smart City 72

The New Revolution 72
Alexey Korzhebin, Section Editor and Columnist

City on the Move: The Digital Future of Transportation 72
Vitaly Gorbushin // Oracle

Big Data Analytics to Drive IoT and Video Surveillance 75
Ilya Yaskov // Seagate Technology

Video Surveillance 76

Traffic Penalties to Drive Video Analytics 76
Mikhail Arsentyev, Section Editor and Columnist

Hello from the Analogue Era. Video Surveillance and Cybersecurity 76
Hu Yangzhong // Hangzhou Hikvision Digital Technology

How to Automate Design Engineering for Video Surveillance? 78
Eugenie Ozerov // ZAO NVP Bolid

BOLID to Expand Its Video Surveillance Product Line 82
ZAO NVP Bolid

Seeing Through Obstructions 84
Vladimir Popov, Konstantin Anoshin // OKB Astron

Doing License Plate Recognition on the Edge 88
Maxim Savelyev // Hikvision Russia

Product Round-Up. Mobile Digital Video Recorders 89

Machine Vision 94

Cool Traditional and New Uses of Machine Vision 94
Andrey Zhukov // Technoserv

Integrated Security, Perimeter Protection 96

Cart Before The Horse 96
Igor Vasilyev, Section Editor and Columnist

Integration of Transportation Checkpoints in a Security System 98
Sergey Boryak // Radiorubezh Ltd.

Fire and Intruder Alarms 100

Transportation Security: Under Government Control 100
Maxim Goryachenkov, Section Editor and Columnist

Fire Safety in Rail Vehicles. Quality vs. Quantity 102
Nikolay Mingalev // Security Department of Russian Railways

Successfully Choosing and Locating Your Loudspeakers 104
Roman Mishin // Independent Expert

Fire Safety at Russian Railways 106

Fiber Optic Heat Detection. What The Market Has to Offer 108
Vladimir Fomin // State Fire Academy of Emercom of Russia

Wireless Technology 112

In Tune with the Times 112
Mikhail Levchuk, Section Editor and Columnist

Wireless Technology for Railway Safety 112
Vasil Krovyakov // SM-Ufa Ltd.

Access Control 116

Distributed Multibranch Access Control 116
Alexey Ginze, Section Editor and Columnist

Long-Range Vehicle Identification Systems 116
Alexander Fomin // AAM Systems

dormakaba Solutions for Sports Facilities: Highest Level of Safety and Comfort 119
dormakaba Eurasia

Expert Opinion. Platforms for Security Systems Integration for Distributed Sites 120
AAM Systems, ARMO-Systems, Bolid, Bosch Security Systems, CROC, Intrium SPb, Octagram, TP KBPE

Long-Range Parking Access Control 133
ARMO-Systems

Biometrics 134

Caution Would Do No Harm 134
Vasily Mamaev, Section Editor and Columnist

What Is Multi-Biometrics 134
Elena Kruchinina // Independent Expert
Danila Nikolaev // Russian Biometric Society

Identity Management 140

IdM Solutions for Business Processes Automation: Any Coin Has Two Sides 140
Alexey Pleshkov, Section Editor and Columnist

Expert Opinion. 2017 Year in Review for IdM/IAM 142
1IDM, Cisco, Solar Security

New Products 146

News Makers 151

Форум All-over-IP 2018: все меняется, кроме ценностей

11-й форум All-over-IP 2018 обновляет свою технологическую адженду, актуализирует мероприятия деловой программы, представляет новые поводы для привлечения аудитории и открывает новые рынки для поставщиков технических решений

Команда All-over-IP начала год с того, что провела несколько исследований, чтобы выявить тренды, которые будут влиять на бизнес участников и посетителей форума в 2018–2019 гг. В соответствии с этими трендами развивается форум All-over-IP в интересах участников и посетителей.

Как меняется рынок

1 Будучи более двух десятилетий преимущественно аппаратноцентричной, индустрия систем безопасности смещает акценты в сторону софтверных решений, аналитики данных и интеграции.

2 Вендорам, которые стремятся сохранять лидерство, потребуется определиться со своей ролью. Производитель симпатичных продуктов? Платформа, позволяющая партнерам зарабатывать больше? Поставщик сервисов? Часть крупных вендоров отказывается от массовой дистрибуции в пользу проектных продаж. Коммерческие интересы связывают с проектами на транспорте, в энергетике, госсекторе, на объектах и мероприятиях с массовым пребыванием людей. Развивают внутренний инжиниринг и оказывают сервисные услуги (аудит объекта, консультации на этапе внедрения).

3 Рынок меняется под влиянием новых трендов: нейросети, искусственный интеллект (AI), глубинное обучение (Deep Learning), Интернет вещей (IoT), биометрическая идентификация, интеллектуальные облачные платформы (SaaS), мобильный доступ, программно-определяемые сети и инфраструктура, перенос ИТ-инфраструктуры в облако, кибербезопасность.

4 Интеграторов систем безопасности зачастую не пускают в проекты по строительству сетей, IoT, кибербезопасности. Грандиозное технологическое обновление, помноженное на варианты развития будущего под влиянием новых трендов, ставит интеграторов, инсталляторов, проектировщиков перед развилкой: на чем зарабатывать в ближайшие пять лет.

5 Перед заказчиками возникают сложные инвестиционные решения. Запросы от потребителей технических средств все больше связаны с IoT, биометрической идентификацией, комплексными системами безопасности, обоснованием стоимости владения (TCO) и получением эффектов для корпоративного и государственного управления. Компетенция вендора в этих вопросах играет решающую роль.

6 Рынок отряхивается от импортозамещения. Хорошая новость для зарубежных вендоров и их российских дистрибьюторов. С 2014 г. импортозамещение в России адекватно не сработало ни в одной из отраслей. Единственный сектор, на который импортозамещение оказывает положительное влияние, это пищевая промышленность. Процесс закупок ТСБ для критически важных объектов, в которых участвуют зарубежные бренды, растягивается во времени, но в конечном итоге закупаются технические средства (в том числе софт), которые решают поставленные задачи и соответствуют требованиям регулятора.

Конференции форума All-over-IP 2018

- **ТРАНСФОРМАЦИЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ: AI, IoT и кибербезопасность**
- **КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ: PSIM и киберфизические системы**
- **IDENTITY MANAGEMENT: от управления доступом к управлению бизнес-процессами**
- **МАШИННОЕ ЗРЕНИЕ: новый виток роста на AI и мониторинге дорожного трафика**
- **CLOUD & IOT CONFERENCE: эволюция городов и зданий**
- **АКАДЕМИЯ СКУД: как перестать внедрять СКУД и начать внедрять ИСБ**
- **CYBER SECURITY ПОКОЛЕНИЯ ГИБРИДНЫХ ВОЙН: защита АСУТП, IoT и облачных сред**
- **БИОМЕТРИЯ: эффекты на гражданских объектах**
- **БИОМЕТРИЯ: эффекты на объектах силовых структур**
- **ИНФРАСТРУКТУРА ЦИФРОВОЙ ЭКОНОМИКИ: сети связи и ЦОДы**
- **ДИСТРИБУЦИЯ В УСЛОВИЯХ КОММОДИЗАЦИИ: как повысить рентабельность бизнеса, на чем зарабатывать**
- **КАК ПРЕУСПЕТЬ В ПРОЕКТНОМ БИЗНЕСЕ: технологические секреты для интеграторов и инсталляторов ТСБ**
- **БИЗНЕС НА КИТАЙСКИХ БРЕНДАХ: тренды и ценность в стиле Восточной Азии**
- **CEO SESSIONS. ПРЕМИУМ-БРЕНДЫ В РОССИИ: измениться или умереть**

Тематические сегменты экспозиции

- **Комплексные/интегрированные системы безопасности**
- **Системы видеонаблюдения**
- **Системы контроля и управления доступом (СКУД)**
- **Машинное зрение**
- **Управление идентификацией (IdM)**
- **ИТ-инфраструктура и сети**
- **Корпоративные коммуникации**
- **Системы хранения данных, дата-центры**
- **Интернет вещей**
- **Кибербезопасность**

Для поставщиков "железа" в области телекоммуникаций рынок сокращается и профессионализируется. Главными закупщиками "железа" для строительства сетей и ЦОДов становятся операторы связи, крупные системные интеграторы и владельцы офисных центров.

Телекоммуникационные подразделения на объектах заказчиков были поглощены ИТ-департаментами. Исключение составляют объекты с нестандартными условиями эксплуатации. Основное число заказчиков переквалифицировалось в покупателей "виртуальной инфраструктуры" и коммуникационных сервисов по хранению данных, управлению IoT, телефонии, доступу в Интернет. Однако виртуализация инфраструктуры не отменяет для вендоров необходимость напрямую работать с ИТ-департаментами и формировать в головах их специалистов правильную идеологию и правильные запросы в адрес поставщиков "железа" и услуг.

Как меняется форум All-over-IP

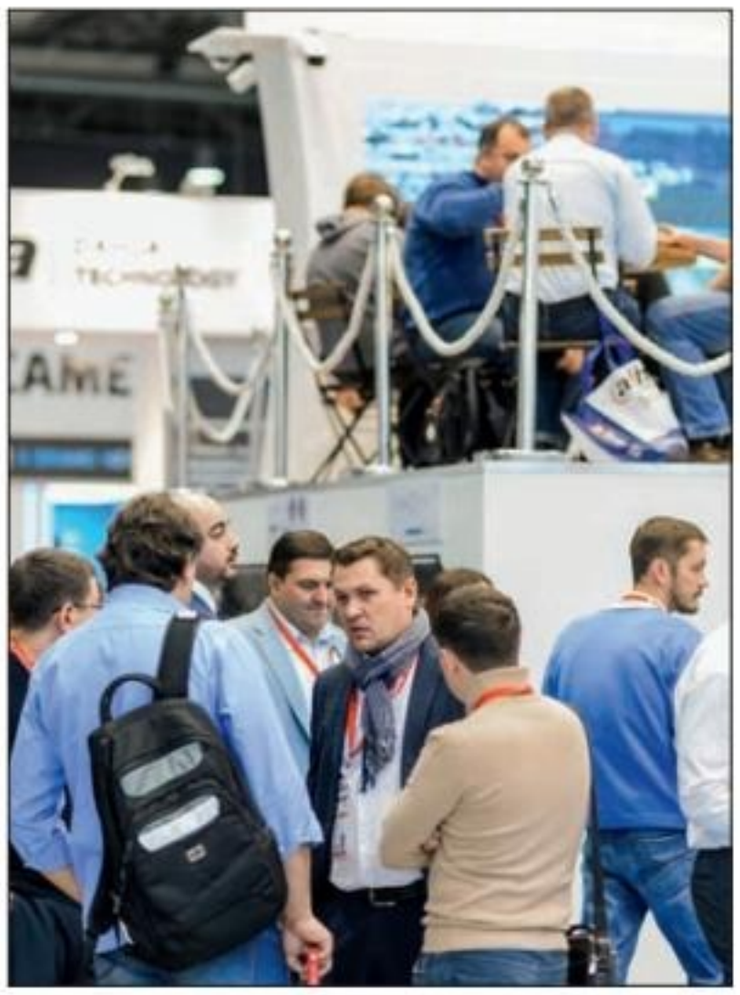
Чем ответит на новые рыночные процессы форум All-over-IP в 2018 г.?

1. Выставка или форум?

Бизнес и жизнь меняют не выставки коммодизированных продуктов широкого потребления, а встречи с людьми, генерящими идеи и создающими ценность. All-over-IP всегда был и остается прежде всего форумом, который строится вокруг выдающихся личностей, передовых трендов, технологических и деловых поводов. Мы видим, как другие мероприятия тиражируют спикеров, которые впервые выступили в России именно на форуме All-over-IP.

Мощная деловая программа форума All-over-IP притягивает передовых участников российского рынка и инновационных покупателей.

Выставочная часть поддерживает форум демонстрацией передовых технологий. Не ширпотреба. Его достаточно и на традиционных выставках. В 2018 г. возвращается программа мероприятий на стендах, которая поможет посетителям формировать ожидания от общения с экспонентами и увеличит число заранее запланированных встреч. События на стендах включаются в общую программу форума; о них широко оповещаются покупатели.



- **Каждый день форума открывают выступления зарубежных и российских гуру на двух больших сценах. Люди, идеи и истории, которые помогают двигаться вперед и зарабатывать.**
- **Конференции подхватывают эстафету. В центре внимания выступлений и дискуссий – эффекты от внедрения технологий для корпоративного и государственного управления.**
- **Мероприятия по дистрибуции помогают партнерам по сбыту найти способы увеличить оборот и рентабельность бизнеса, расширить портфолио и укрепить отношения с вендорами.**
- **Семинары брендов анонсируют флагманские продукты и решения будущего.**
- **События на стендах делают из каждого поставщика центр компетенций и точку притяжения покупателей**

2. СБшники или айтишники?

Безусловно, и те, и другие. Анализ интересов айтишников и СБшников, посещающих форум All-over-IP, показывает, что перед производителями и поставщиками технических решений открываются оба рынка: ТСБ и ИТ. Например: 55,4% ИТ-специалистов, посещающих форум All-over-IP, закупают системы видеонаблюдения; 42,4% ИТ-специалистов закупают СКУД; 36,3% ИТ-специалистов участвуют в закупках интегрированных систем безопасности. Другой пример: 42,5% специалистов по ТСБ из числа посетителей All-over-IP закупают облачные системы; 51,3% внедряют системы на базе беспроводной ИТ-инфраструктуры; 45,2% специалистов по ТСБ участвуют в проектах по интеллектуальному зданию.

3. Инсталляторы или заказчики?

Интеграторы, инсталляторы, проектировщики и монтажники ТСБ и ИТ – это корневая аудитория форума All-over-IP. В 2018 г. мы планируем для них события по дистрибуции. Кроме того, системные интеграторы, инсталляторы, монтажные организации заинтересованы в поиске конкурентных изюминок для интеграционного продукта. Наибольшее внимание получат экспоненты, которые предложат партнерам по сбыту технологии, дающие им новые преимущества среди равных.

Растет интерес к форуму со стороны конечных заказчиков. Поэтому мы продолжим создавать для них специальный контент. Ранее на форуме речь шла о возможностях передовых технологий вообще. О значении новых трендов в целом. Теперь в центр конференций и дискуссий помещается получение эффектов от внедрения новых технологий в различных отраслях. Разговоры об эффектах, в свою очередь, помогут инсталляторам и интеграторам вооружиться правильными аргументами для общения с клиентами. ■

ALL-OVER-IP

21–23 ноября 2018, Москва, Сокольники
www.all-over-ip.ru

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

ТБ Форум 2018: новое качество экспозиции, мощная деловая программа, качественная и интересная аудитория и высокий уровень организации встреч с заказчиками

13–15 февраля прошел XXIII Международный форум "Технологии безопасности" – главная ежегодная встреча руководителей, ответственных за обеспечение безопасности организаций и граждан страны.
Здесь были представлены все основные секторы российской экономики, органы государственного и муниципального управления

В этом году была максимально учтена специфика каждого сектора: транспорт, спортивные и массовые мероприятия, городская инфраструктура, строительные объекты, объекты промышленности, нефтегаза и энергетики, финансового сектора или ритейла.

Национальные интересы

Национальная повестка текущего года отразилась в программе совещаний, встреч и в экспозиции, созданной участниками Организационного комитета и рабочих групп, объединяющих представителей органов власти, регуляторов и крупнейших российских государственных предприятий и корпораций.
Для специалистов каждого направления, каждого сектора российской экономики сформирована отдельная программа: в рамках ТБ Форума 2018 прошли 12 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.

Виктор Николаевич Бондарев, Председатель Комитета Совета Федерации Федерального Собрания Российской Федерации по обороне и безопасности, председатель Оргкомитета Форума

Форум традиционно проходит при поддержке Комитета Совета Федерации по обороне и безопасности и рассматривается нами как конструктивная рабочая площадка, объединяющая государственные структуры, предприятия промышленности, науки, бизнес-сообщество, институты гражданского общества.
Форум предоставляет нам прекрасную возможность продемонстрировать свои передовые достижения, а на конференциях и тематическом круглом столе поделиться опытом, обсудить назревшие проблемы. Для

Комитета Совета Федерации по обороне и безопасности это еще и прекрасная возможность проанализировать ситуацию в различных сферах отрасли безопасности и выработать системные меры, направленные на обеспечение безопасности государства, общества и личности

Практическая направленность

Главное отличие деловой программы 2018 – практическая направленность и поддержка проектов, которые российские потребители реализуют на своих объектах, создание эффективной среды для укрепления межведомственного сотрудничества и совместного создания решений, ценных для российских и иностранных заказчиков.

Владимир Шелепов, заместитель генерального директора по развитию бизнеса Группы "Астерос"
Международный форум "Технологии безопасности" – одно из ключевых ежегодных событий, которое объ-

единяет представителей власти, отраслевые организации и технологические компании, задействованные в обеспечении безопасности инфраструктуры страны. Группа "Астерос" традиционно является участником данного Форума, и одной из основных причин является детально продуманная деловая программа, качественная и интересная аудитория и высокий уровень организации. Слаженная работа, позитивный настрой и установленная организаторами высокая планка – вот три составляющих успеха ТБ Форума

Александр Бабушкин,
технический директор
ГК "ТОНК"
Выставка, как всегда, прошла на высшем уровне. Очень приятно, что Форум посетило такое большое количество представителей регуляторов и высокопоставленных лиц, на мероприятиях освещались актуальные темы. Нам понравилась и подготовительная работа в рамках Форума – встречи с различными заказчиками

При подготовке Форума использована новая концепция проведения выставочной экспозиции. В этом году впервые был успешно проведен Всероссийский смотр технологий и решений для обеспечения безопасности на транспорте, спортивных и массовых мероприятий, городской инфраструктуры и граждан, строительных объектов, объектов промышленности, предприятий нефтегазового и топливно-энергетического комплекса, банковской сферы.

Кто посетил?

Целевые группы заказчиков, которые прибыли на смотр и провели переговоры с участниками:

- руководители объектов транспорта и транспортной инфраструктуры;
- городские, муниципальные и региональные администрации;
- владельцы спортивных объектов и организаторы спортивных и массовых мероприятий;
- руководители по безопасности объектов промышленности, нефтегаза и энергетики;
- директора по безопасности, начальники департаментов ИБ и ПБ банков и финансовых организаций;
- руководители служб безопасности, экономической безопасности, ИБ ритейла и ТРЦ;
- проектировщики и ответственные за безопасность при строительстве объектов.

Талип Полатов,
руководитель направления
ЗАО "Сфера"
Форум получился неожиданно интересным. Не секрет, что в последнее время многие мероприятия выдыхаются. Если в первый день выставки наблюдается большое количество посетителей, то в последующие посетителей мало. На ТБ Форуме посетителей в первый день на нашем стенде было много, во второй день – еще больше, и в третий день у нас состоялась несколько очень важных встреч с заказчиками, например с министром Московской области

ВНИМАНИЕ!
МОНТАЖНИКАМ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

ПОКАЖИТЕ СЕБЯ, ВАШ ПРОЕКТ
И СОРЕВНУЙТЕСЬ ЗА ДЕНЕЖНЫЙ ПРИЗ - 50 000 руб.!

СТАНЬТЕ ИЗВЕСТНЫМ СПЕЦИАЛИСТОМ НА РЫНКЕ ВИДЕОНАБЛЮДЕНИЯ!

Проект #БАШ-МОНТАЖ - это возможность для организаций, занимающихся установкой видеонаблюдения заявить о себе, наглядно продемонстрировать свою работу, поделиться опытом, а так же, возможность выиграть главный денежный приз - **50 000 руб.**

УЧАСТИЕ - БЕСПЛАТНО!

ПРИНЯТЬ УЧАСТИЕ

СЪЕМКА ВИДЕО

Мы самостоятельно снимаем репортаж о Вас и Вашем проекте. После обработки оно публикуется на сайт и социальные сети.

ГОЛОСОВАНИЕ

Ваши коллеги, друзья, подписчики каналов и зрители голосуют за лучший и интересный проект.

НАГРАЖДЕНИЕ

Открытый подсчет голосов, подведение итогов и награждение победителей.

Оставьте заявку удобным для Вас способом:

+7 (495) 182 05 32 ebm@dssl.ru ebm.dssl.ru

Присоединяйтесь, голосуйте и следите за результатами в социальных сетях:

#БАШ-МОНТАЖ

На ТБ Форуме 2018 стартовала годовая серия закрытых встреч регуляторов, заказчиков, интеграторов и разработчиков решений, на которых обсуждаются особенности моделей закупок, специфика требований и технологии, позволяющие эти требования реализовать.

Андрей Дзыгарь, генеральный директор компании Facepass

Мы – IT-стартап, и ТБ Форум стал для нас прорывом сразу на несколько рынков безопасности: госструктур, крупных предприятий, банков, ритейла. За три дня проделана месячная работа отдела продаж. Проведено более сотни встреч с потенциальными заказчиками, партнерами и интеграторами. Формат круглых столов с заказчиками – очень крутое нововведение компании "Гротек". Огромная благодарность организаторам за помощь и советы по организации встреч с интересующими заказчиками. Мы очень довольны результатами ТБ Форума. Несомненно, мы будем рекомендовать его партнерам

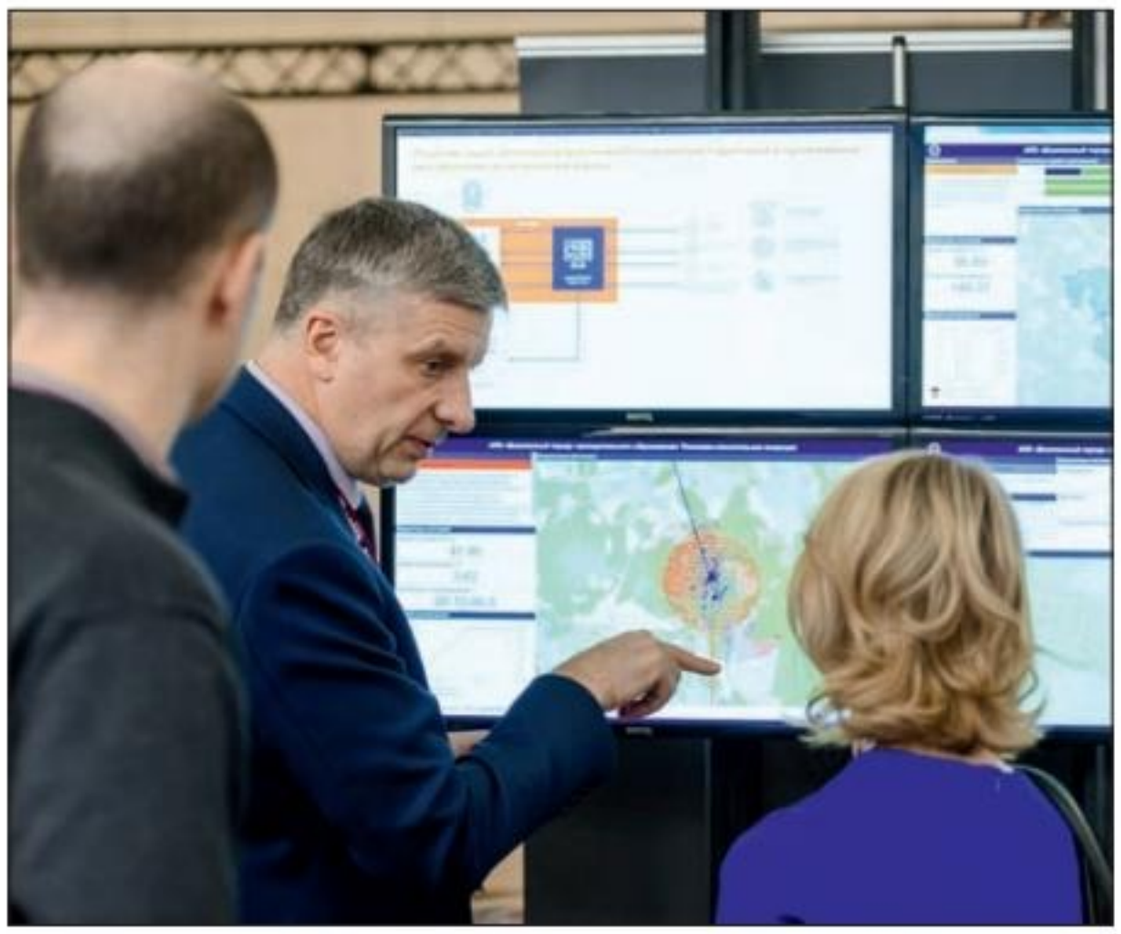
Что нового?

В этом году на ТБ Форуме:

- на 28% больше участников экспозиции – Всероссийского смотра решений и технологий, на который прибывают делегаты из 85 регионов России и стран СНГ;
- деловую программу поддержали партнеры и спонсоры: Группа "Астерос", компания Huawei, РНТ, МТС, Конфидент, МобилитиЛаб, Код Безопасности, Видеоинтеллект, ITV | AxxonSoft, Крок, Прософт-Биометрикс, ИЦБ, Nec, BEWARD;
- практическая направленность конференций, создание эффективной среды для укрепления межведомственного сотрудничества и совместного создания решений для безопасности транспорта, города, спортивных мероприятий, объектов строительства, промышленности, нефтегаза, ТЭК, финансовых организаций и ритейла;
- новые темы конференций и круглых столов: цифровая экономика, BIM-технологии в строительстве, дроны в безопасности, противопожарная защита промышленных объектов;
- в деловой программе – 12 мероприятий;
- 226 спикеров: регуляторы, крупнейшие заказчики, разработчики, эксперты;
- на 30% выше предварительная регистрация посетителей и делегатов;
- специальная программа встреч регуляторов, заказчиков, интеграторов и разработчиков решений, на которых обсуждались особенности моделей закупок, специфика требований и современные технологии.

Максим Насонов, руководитель отдела продаж компании "БайтЭрг"

Второй год подряд мы участвуем в Форуме в таком формате, и нам очень нравится. Нравится, что здесь мы общаемся с аудиторией, которой действительно нужна наша техника. Форум посещают конечные заказчики, которым можно напрямую, без посредников, объяснить, что собой представляют наши решения. Встречи с заказчиками, организованные компанией "Гротек", прошли успешно, заказчики высказали свою заинтересованность, и мы теперь лучше понимаем, куда двигаться дальше, чтобы удовлетворить их запросы ■



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

12–14 февраля 2019

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

ДАЙДЖЕСТ

Подъем рынка видеонаблюдения несмотря на ценовые войны

Благодаря спросу на инновационные и более эффективные технические средства 2017 год был отмечен ростом мирового рынка систем видеонаблюдения. Однако конкурентная среда оказалась крайне непростой для западных и азиатских компаний, поскольку два главных китайских производителя – Dahua и Hikvision – продолжили снижать цены, чтобы не терять темпов увеличения доли рынка, чем вынуждали конкурентов вступать в ценовую гонку. Нет никаких признаков того, что в ближайшее время эта гонка завершится

По оценкам аналитиков компании Memoori, в 2017 г. объем мирового рынка систем видеонаблюдения достиг 15,87 млрд долларов. Рынок будет расти в среднем на 7,5% ежегодно и к 2022 г. составит 22,78 млрд долларов. В последние два года цены на технические средства видеонаблюдения существенно снизились, что и ограничивает рост доходов компаний-поставщиков.

Ценовые войны и альтернативные стратегии

Стратегия наращивания объема продаж коммодизированной продукции, не отличающейся от других брендов, работает плохо. Все более важно предлагать покупателю ценность, которая заключается в обеспечении кибербезопасности и снижении стоимости владения системой (TCO). Это почти не под силу западным вендорам, при максимальном снижении маржи они не могут инвестировать достаточно средств в разработки.

В 2016 г. совокупный объем продаж Dahua и Hikvision превысил 5 млрд долларов. И это уже совершенно иная лига, даже по сравнению с крупнейшими западными производителями. Полный контроль над домашним китайским рынком позволяет им свободно демпинговать на международной арене. Наиболее знаменательные результаты этим компания их разрушительная стратегия дала в США.

Большинство западных вендоров не могут участвовать в ценовых войнах, объемы их продаж не покрывают затраты на разработки. На рынке впервые появились признаки снижения роста продаж двух китайских гигантов, что связано со слабой защищенностью их систем от киберугроз – для покупателей это оказывается важнее низких цен на камеры. Тем не менее западным производителям потребуется поработать над своими стратегиями. Например, сориентироваться на крупных заказчиков, а в некоторых случаях сосредоточиться на небольшом количестве отраслевых сегментов. Альтернативным решением станет консолидация с другими крупными производителями, чтобы получить эффект масштаба

Рабочий способ добиться рентабельности

В течение последующих пяти лет следует ожидать стабильного спроса на системы видеонаблюдения, но также и сложной конкурентной обстановки. В связи с этим следует выделять области применения ТСБ, где фактор цены не является определяющим, а современные технические средства, предлагаемые по разумной цене, способны обеспечить лучшую стоимость владения системой. В этом году компания Axis

Communications показала, что вполне возможно увеличить темпы роста и добиться рентабельности, не ввязываясь в ценовую гонку. Пример Axis Communications не единственный. Даже несмотря на то что ценовая конкуренция замедляется, в ближайшие пять лет множеству небольших производителей придется нелегко, в особенности тем, которые не работают над повышением узнаваемости бренда в конкретных отраслях. Деловые возможности при этом во многом связаны с новой волной развития видеоанализа.

Глубинное обучение – новая волна видеоанализа

Прошедший год ознаменовался появлением многочисленных стартапов, ставших предвестниками новой волны развития технологий видеоанализа. Системы видеоанализа, появившиеся на рынке более десяти лет назад, не оправдали ожиданий, но в последние три года видеоаналитика снова доминирует в заголовках.

Традиционные лидеры рынка видеонаблюдения рассматривают технологии глубинного обучения и искусственного интеллекта (AI) на борту своих устройств как способ выделиться на фоне конкурентов. Такой подход, правда, предполагает высокую вычислительную мощность процессоров. Однако компания ARM уже анонсировала дизайн новых AI-процессоров для оконечных устройств, в том числе умных камер.

Видеокамеры со встроенными технологиями видеоанализа, такими как обнаружение движения, лиц и объектов, обрабатывают изображение в момент съемки и исключают необходимость передавать видеопоток на центральный сервер.

Главные драйверы спроса на видеонаблюдение

За последние пять лет драйверы спроса на системы видеонаблюдения несколько изменились. Контроль безопасности и противодействие террористическим угрозам как в зданиях, так и местах массового скопления людей, а также сокращение потерь по-прежнему остаются первостепенными. Однако потребители очень заинтересованы также превратить видеонаблюдение в инструмент, который повышает производительность их предприятий и дает дополнительную ценность вдобавок к решениям задач безопасности.

Приоритеты корпоративных заказчиков стойко связаны с показателями суммарной стоимости владения системой и возможностями ее масштабирования. В большинстве случаев это достигается только применением IP-решений. Технологии AI не просто увеличивают привлекательность таких решений, а в разы повышают их потенциал.

Через пять лет концепция Интернета вещей в зданиях станет реальностью, сетевые IP-камеры окажутся неотъемлемой частью этих систем. Более того, IP-камеры превратятся в один из важнейших датчиков масштаба здания, транспортных систем и умных городов. ■

По материалам компании Memoori
www.memoori.com

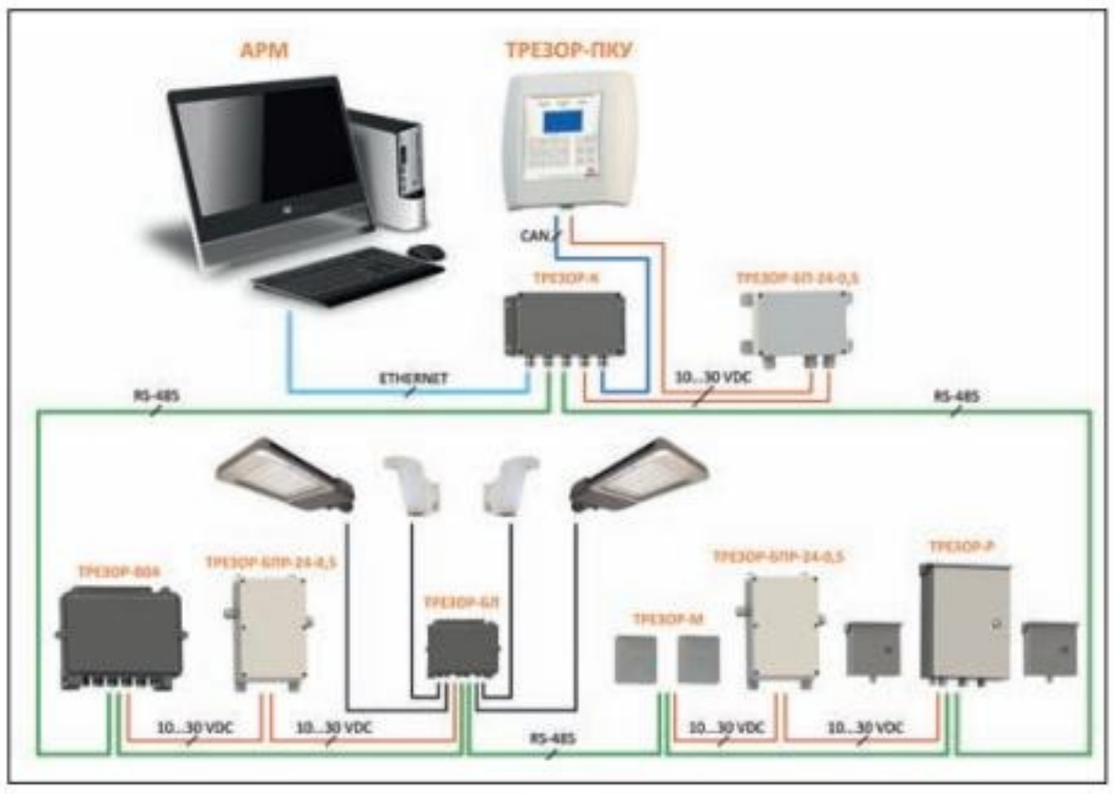
Охрана периметра нового качества от "НПЦ "Трезор"

Научно-производственный центр "Трезор" представляет новую разработку – систему охраны периметра, обеспечивающую максимально высокий уровень защиты от несанкционированных проникновений

Система включает в себя:

- центральный контроллер "ТРЕЗОР-К", который определяет состояние подключенного оборудования по интерфейсу RS-485;
- пульт контроля и управления "ТРЕЗОР-ПКУ";
- блок линейный "ТРЕЗОР-БЛ", позволяющий управлять охранным освещением и другими исполнительными устройствами, а также принимать сигналы извещателей с выходом типа "сухой контакт".

Периметровые извещатели ТРЕЗОР™ подключаются в единую линию связи по интерфейсу RS-485.



Структурная схема новой системы охраны периметра

Конфигурация и работа с событиями

Пульт контроля и управления предназначен для работы в составе системы охраны периметра. При помощи кнопочной клавиатуры выполняется ввод данных для конфигурирования системы. Встроенный дисплей позволяет отображать текущие события и архив.

Линии связи

Центральный контроллер имеет два выхода линии связи RS-485, которая реализована по схеме "кольцо" для повышения надежности системы. Линия связи CAN позволяет объединять в одну систему до 32 контроллеров. Выход Ethernet предназначен для подключения контроллера к локальной сети и АРМ с программным обеспечением (перспективная разработка).

Управление исполнительными устройствами

Линейный периметровый блок предназначен для управления исполнительными устройствами, охранным освещением посредством исполнительных реле на "плате выхода". Для подключения извещателей с выходом типа "сухой контакт" предусмотрена "плата входа". На плате линейного блока расположены два выхода для питания извещателей.

Электропитание

Для электропитания оборудования в системе предусмотрены блоки питания "ТРЕЗОР-БП-24-0,5" и резервированный "ТРЕЗОР-БПР-24-0,5" с возможностью установки двух АКБ 12 В/4,5 Ач. ■

Адрес и телефоны
ООО "НПЦ "ТРЕЗОР"
см. стр. 152 "Ньюсмейкеры"

7 главных трендов рынка видеонаблюдения 2018

От искусственного интеллекта (AI) и глубинного обучения до прорывов в защите данных – новые тренды видеонаблюдения меняют привычные способы взаимодействия людей, организаций и машин, а также стимулируют новую революцию в развитии индустрии систем безопасности

Британская исследовательская компания IHS Markit опубликовала семь главных трендов 2018 г. для рынка систем видеонаблюдения.

1. AI и глубинное обучение

Видеоанализ на основе глубинного обучения оформляется в готовые для применения продукты с удобными пользовательскими интерфейсами и сценарным подходом. Например, алгоритмы распознавания лиц на базе глубинного обучения используются в приложениях по поиску в видеоархивах пропавших людей. Новые возможности откроются компаниям, предлагающим видеоаналитику на основе глубинного обучения для решения отраслевых задач.

2. Конфиденциальность и GDPR

В 2018 г. новые дискуссии ожидаются на тему персональных данных и методах, которыми индустрия видеонаблюдения защищает собираемые данные. Во многом эти дискуссии вызваны вступлением в силу в мае текущего года европейского закона о защите персональных данных (GDPR). Закон заменит существующие аналогичные документы каждой страны – участницы Евросоюза и регулирует данные, накапливаемые системами видеонаблюдения.

3. Китай против всего остального мира

В 2018 г. доля Китая составит почти половину (46%) от мирового объема рынка видеонаблюдения. Однако китайский рынок обладает рядом уникальных особенностей. По большому счету, существуют два рынка видеонаблюдения: китайский и весь остальной мир.

4. Технологии обнаружения дронов

Гражданские дроны доступны для широкого круга потребителей за пару сотен долларов. Для их использования не нужно ни обучение, ни лицензия. Поэтому применение беспилотных летальных аппаратов представляет собой проблему безопасности для контролируемых воздушных пространств. Обнаружение дрона может обернуться сложной задачей. Отныне любой заказчик, желающий обеспечить защиту периметра, должен принимать во внимание возможные угрозы с неба.

5. Отказоустойчивость

Рынок видеонаблюдения до сих не придавал большого значения вопросам восстановления систем после отказа и резервированию данных. Однако с ростом числа пользователей и повышением роли видео в деятельности организаций следует ожидать увеличения спроса заказчиков на технологии восстановления после отказа, обеспечения избыточности данных и их резервного копирования.

6. Судебная видеоаналитика как сервис

За последние два года удалось обеспечить достаточный уровень точности судебной видеоаналитике с помощью технологий глубинного обучения. Для целей видеоанализа все чаще будут одновременно использоваться несколько источников видеоархивов для обработки посредством технологий глубинного обучения.

7. Программа Сюэ Лианг

Программой Сюэ Лианг предполагается подключить все камеры городского видеонаблюдения в Китае к центральной платформе на уровне региона или государства и создать механизм для обмена данными между гос службами. Ожидается, что производители систем видеонаблюдения начнут массово добавлять в свои линейки оборудование, готовое к подключению к ЦОД и поддерживающие облачные технологии. ■

По материалам компании IHS Markit
www.ihs.com

Компания dormakaba вошла в топ-100 мировых лидеров в области технологий

В январе 2018 г. агентство Thomson Reuters, ведущий мировой источник новостей и информации, обнародовало список "Топ-100 мировых лидеров в области технологий" за 2018 г., в который вошла компания dormakaba как единственный представитель своей отрасли

О рейтинге "Топ-100 мировых лидеров в области технологий"

Первая за всю историю комплексная оценка компаний – лидеров в сфере технологий. Результаты основаны на 28-факторном алгоритме, который позволяет объективно анализировать перспективы компаний в современной изменчивой бизнес-среде. Согласно методологии, деятельность компаний оценивалась по восьми ключевым параметрам: финансовые показатели, корпоративное управление и доверие инвесторов, риски и устойчивость, соблюдение законов и правовых норм, инновационность, отношение к персоналу и социальная ответственность, воздействие на окружающую среду, репутация. Топ-100 компаний – это лучшие производители, выбранные среди 5000 передовых технологических компаний в мире

В отчете агентства Thomson Reuters "Топ-100 мировых лидеров в области технологий" за 2018 г. содержится всесторонний анализ отраслевых лидеров и определены самые передовые и успешные в технологическом и финансовом плане компании.

Президент компании dormakaba Рит Кадоно отметил: "Мы гордимся, что оказались в этом рейтинге вместе с такими компаниями, как Microsoft, Amazon и IBM. Высокие оценки показателей, рассмотренных в исследовании, подтверждают правильность нашего подхода к устойчивому росту с соблюдением баланса между финансовыми результатами, инновациями и социальной ответственностью". ■

Тренды рынка СКУД 2017–2022

За последние пять лет рынок СКУД стал намного более привлекательным для бизнеса. В 2016 и 2017 гг. темпы роста продаж СКУД в мире превосходили показатели остальных сегментов рынка ТСБ, отчасти благодаря переходу на IP-технологии, повышению характеристик продукции и эффективности управления системами

Рынок систем контроля доступа на распутье. Шагнет ли он в направлении открытых систем или будет какое-то время пренебрегать отраслевыми стандартами? 2017 год ознаменовался несколькими интригующими сделками по слиянию и поглощению и приходом на Запад двух крупнейших китайских производителей.

Лидерство по темпу роста

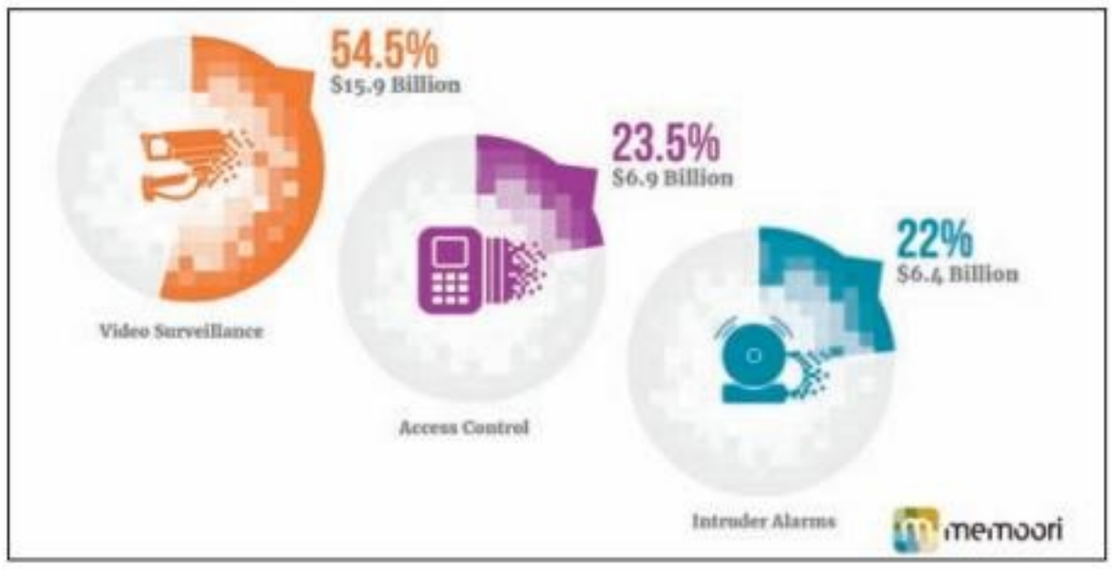
Производители СКУД внимательно прислушивались к потребностям партнеров по сбыту, в результате в 2017 г. мировой рынок технических средств контроля доступа достиг 6,858 млрд долларов. Рост к 2016 г. составил почти 7%. В период 2016–2017 гг. рынок СКУД превосходил по темпам роста и рынок видеонаблюдения, и рынок охранной сигнализации. По итогам 2018 г. ожидается аналогичная картина.

Темп роста рынка СКУД в мире будет составлять 8,04% до 2022 г. и через пять лет достигнет 10,1 млрд долларов. Такую динамику будут стимулировать продажи облачных решений СКУД (ACaaS), биометрии, IdM-решений, беспроводных замковых систем, а также распространение сетевых IP-СКУД

Бизнес на продаже систем контроля доступа по объему меньше бизнеса в сегменте видеонаблюдения, но рынок СКУД созрел, чтобы двигаться дальше и охватывать новые технологии, которые будут стимулировать спрос.

Радужные прогнозы и облачный горизонт

Прогнозы на будущее СКУД радужные, но на горизонте присутствует и облачность. Во-первых, производители СКУД не спешат приводить свою продукцию в соответствие со стандартами ONVIF. Во-вторых, два крупнейших китайских вендора, которые создали невероятную конкурентную среду для западных брендов видеонаблюдения, активно инвестируют в развитие СКУД. Открытые стандарты помогли бы им получить и нарастить долю рынка за счет как модернизации объектовых систем, так и внедрения новых. Переход на IP-технологии, развитие биометрических технологий и интеграция с IdM-системами повышают потенциал рынка СКУД. Роль открытых стандартов не менее значима, но производители и интеграторы не слишком настроены ими воспользоваться. Если вендоры СКУД продолжат идти по пути закрытых систем, это негативно скажется на росте бизнеса. Закрытые системы подразумевают ограниченный функционал, центральные серверы с дорогостоящей кабельной системой, а также ограничения по интеграции и масштабированию. Индустрия с интересом ожидает последствий от сделки по приобретению компанией HID Global OEM-поставщика контроллеров и ПО Mercury: перейдет ли Mercury на открытые стандарты или останется приверженцем закрытых систем?



Мировые продажи техническим средств безопасности по итогам 2017 г.

Интеграция с IdM и облачные решения

Интеграция СКУД и IdM-систем приобретает все большую актуальность в связи с вступлением в силу в Евросоюзе нового закона о защите персональных данных (GDPR) в мае 2018 г. Действие этого закона распространяется и на данные, собираемые и обрабатываемые в СКУД.

Контроль доступа как сервис (ACaaS) набирает популярность. Со снижением цен растет количество проектов по сетевым IP-СКУД, а технологии подтверждения личности играют все более важную роль. Облачные СКУД привлекают заказчиков, в особенности тех, кто не располагает собственными ИТ-компетенциями.

Концепция ACaaS избавляет пользователя от необходимости содержать ИТ-департаменты, а также поддерживать серверную и сетевую инфраструктуру. Этот подход снижает стоимость владения системой без потери функционала. ■

По материалам компании Memoori
www.memoori.com

50 000 рублей за лучший монтаж
DSSL проводит конкурс #БАШ-МОНТАЖ

Компания DSSL запустила уникальный проект #БАШ-МОНТАЖ. Представляем нашего первого участника конкурса – компанию "Центр Мониторинга – СБ". Проект, о котором рассказал генеральный директор Юрий Гергель, уже запущен. Сейчас можем только сказать, что это достаточно большая работа городского масштаба. Другие наши участники готовятся к съемкам, и в скором времени мы их представим. Принять участие в конкурсе может любая компания-инсталлятор

Проект #БАШ-МОНТАЖ создан с целью предоставить компаниям, занимающимся установкой систем видеонаблюдения, возможность заявить о себе, наглядно продемонстрировать свою работу и степень квалификации, а также выиграть денежный приз.

Проект вызвал большой интерес не только в Московском регионе, поэтому были разработаны рекомендации для компаний из других городов. Об этом подробно написано на сайте проекта, где можно оставить заявку, и с вами свяжутся наши специалисты.

Как это работает?

Съемочная группа компании DSSL выезжает на объект, на котором участники устанавливают систему видеонаблюдения/безопасности, и снимает весь процесс. Во время съемки участники рассказывают об оборудовании, почему выбрали именно его, зачем установили камеру именно так, а не по-другому, и т. д.

Готовый видеосюжет выкладывается в соцсетях, по истечении месяца подсчитывается активность зрителей относительно каждого сюжета, на основании чего и выбирается победитель.

Масштабная целевая аудитория

Мы будем регулярно продвигать проект в том числе в журнале "Системы безопасности", на сайте компании DSSL и делать рассылку среди наших подписчиков. Таким образом, суммарная аудитория зрителей проекта – десятки тысяч специалистов и потенциальных клиентов вашей компании.

Проект уже стартовал, получил положительные оценки и вызвал большой интерес у представителей бизнеса, закупающего оборудование для систем видеонаблюдения и контроля доступа.

Розыгрыш призов

Поскольку проект демонстрирует высокую популярность, мы хотим пригласить еще больше участников, которые смогут не только бесплатно прорекламировать свою компанию и получить новых клиентов, но и принять участие в конкурсе среди своих коллег и получить шанс выиграть приз в 50 000 рублей. Приз разыгрывается ежемесячно среди четырех участников – шансы выиграть очень высоки.

Ознакомиться с подробностями конкурса можно на сайте: www.ebm.dssl.ru.

Оставить заявку на участие в проекте можно на сайте, а также написав письмо на электронную почту ebm@dssl.ru или позвонив по телефону +7 (495) 182-05-32. ■

Большое будущее датчиков на рынке видеонаблюдения

По оценкам компании Frost & Sullivan, в 2016 г. мировые продажи датчиков для применения в системах безопасности и видеонаблюдения составили 6,267.9 млн долларов. Крупнейшая доля в этом объеме принадлежит датчикам изображения – 23%. Ожидается, что к 2023 г. рынок достигнет 12,012.1 млн долларов

Согласно Frost & Sullivan, Интернет вещей (IoT) открывает новую эпоху сетевого подключения в цифровом мире, обеспечивая для критически важных отраслей экономики защищенную передачу данных, аналитику и управление по сети. Для поставщиков IoT-датчиков открываются возможности в сегменте безопасности, в частности в связи с потребностями в удаленных сервисах и более удобном доступе к устройствам.

Северная Америка и страны EMEA лидируют по объему рынка вследствие устаревающей ИТ-инфраструктуры. Однако Азиатско-Тихоокеанский регион растет наиболее быстрыми темпами благодаря стремительному развитию инфраструктуры, экономическому росту и благоприятствующему нормативно-правовому регулированию со стороны государства.

Поставщикам IoT-датчиков придется столкнуться и с трудностями, среди которых: конкуренция, ведущая к снижению цен, а также коммодизация продукции и отсутствие общепризнанных стандартов.

Тренды Интернета вещей

Отчет Frost & Sullivan отражает глобальные тренды Интернета вещей и Промышленного Интернета вещей (IIoT) и их влияние на системы безопасности и видеонаблюдения на объектах промышленности, коммерческой недвижимости, оборонной сферы, в государственных учреждениях, а также на ИТ-инфраструктуру и системы автоматизации зданий.

Рост Интернета вещей способствует развитию требований по безопасности; особые перспективы видятся в сферах робототехники, систем биометрической идентификации и RFID-систем. Будущее систем безопасности и видеонаблюдения – за автоматизацией и роботизацией. Устойчивый спрос сохраняется на дроны и автоматически управляемые транспортные средства со стороны оборонной сферы, государственных ведомств и коммерческих предприятий.

Повышение интереса к биометрическим системам идентификации в СКУД наблюдается в коммерческом и жилищном секторах. Новый революционный технологический всплеск следует ожидать с появлением облачных интерактивных сервисных платформ в сегменте жилья и коммерческих зданий, особенно в части решения задач безопасности. Они открывают возможность для распространения новых сервисов, предоставляемых по защищенным каналам связи.

Три больших прогноза

Frost & Sullivan выдвигает три больших прогноза развития направления IoT-датчиков на рынках систем безопасности и видеонаблюдения.

1. Интернет вещей создает предпосылки для конвергенции индустрий. Частным случаем IoT является межмашинное взаимодействие (M2M), создающее предпосылки для более эффективного принятия решений. Датчики образуют физический уровень IoT-архитектуры.
2. Развитие коммуникационных протоколов обеспечит взаимодействие автономных систем и стандартизацию, особенно в системах защиты периметра, охранной сигнализации и СКУД.
3. Ритейл, здравоохранение и финансовый сектор станут основными покупателями датчиков для систем биометрических идентификации. ■

По материалам портала SecurityWorldMarket www.securityworldmarket.com

ИННОВАЦИОННАЯ ВЕСНА

ЛУЧШИЕ ПРОДУКТЫ 2018

УНИКАЛЬНЫЕ ТЕХНОЛОГИИ ДЛЯ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ

Seagate Technology

Запись видео высокого разрешения без пропуска кадров 19

Накопители SkyHawk AI разработаны для высоких рабочих нагрузок в круглосуточно работающих системах видеонаблюдения и идеально подходят для сетевых видеорегистраторов с расширенными функциями аналитики.

Производитель: Seagate Technology

"Интегра-С"

Геоинформационная система высокого уровня 19

Интеграционная платформа "Интегра-Планета-4D" – это единственная в мире система, в которой все объекты, датчики, устройства и даже видеоизображение привязаны к географическим координатам и времени.

Производитель: Консорциум "Интегра-С"

"ААМ Системз"

Система безопасности последнего поколения 20

Кластерный контроллер СКУД и ОС ASP-4 может быть центральным контроллером кластера, дверным контроллером СКУД, охранной или релейной панелью, управлять лифтом. 256 считывателей на кластер.

Производитель: APOLLO

AHI CARRIER FZC

Недорогая адресно-аналоговая АПС 20

Сетевая АПС GST-IFP8-RU на 8 шлейфов с возможностью построения сети из 64 панелей. Более 123 000 адресных устройств на одну систему. Предназначена для коммерческого строительства.

Производитель: Gulf Security Technology

PERCo

Комфортный учет рабочего времени 21

Система PERCo-S-20 – удобный инструмент управления рабочим временем сотрудников для администраций и кадровых служб. Принцип гибкого графика обеспечивает личный контроль отработанного времени и повышает производительность труда.

Производитель: PERCo

PERCo

Эффективное управление предприятием 21

Система контроля доступа и учета рабочего времени PERCo-Web повышает уровень безопасности предприятия, обеспечивает рост производительности труда и рост прибыли. Предназначена для бизнес-центров, промышленных предприятий, офисов и др.

Производитель: PERCo

ПК "РостЕвроСтрой"

Повышенная защищенность от несанкционированного входа 22

Полноростовые турникеты-шлюзы ПРШ1/3 и ПРШ2/4 универсальны и могут работать как обычные полноростовые турникеты с высокой пропускной способностью. Перестройка режима работы занимает не более 30 мин.

Производитель: ООО ПК "РостЕвроСтрой"

"БИК-Информ"

Взрывобезопасное опорно-поворотное устройство 22

Устройство PTR-407Ex из нержавеющей стали позволяет устанавливать и позиционировать камеры видеонаблюдения в условиях Крайнего Севера ("холодный старт" при -61 °С), взрывоопасных и агрессивных средах.

Производитель: ООО "БИК-Информ"

НВП "Болид"

Переход от релейных на информативные системы 23

Дымовой оптико-электронный линейный пожарный извещатель "С2000-ИПДЛ" позволяет сделать систему АПС более надежной за счет сокращения блоков питания, линий электропитания.

Производитель: ЗАО НВП "Болид"

Безопасность в руках отечественных производителей!

Интеграционная платформа "Интегра-Планета-4D"

ЧТО УНИКАЛЬНОГО

1 Привязка к координатам и времени
Это единственная в мире система, в которой все объекты, датчики, устройства и даже видеоизображение привязаны к географическим координатам и времени.

2 Глобальное решение
На базе "Интегра-Планета-4D" стало возможным построение цифрового государства.

3 Открытые коды
Система работает под управлением ОС с открытыми исходными кодами Linux и др. (распоряжение Правительства РФ от 17 декабря 2010 г. № 2299-р).

ЗАЧЕМ ПОКУПАТЬ

4 Для небольших и крупных объектов
Система применима для работы как с небольшими объектами, так и с территориально протяженными, такими как города, государства.

5 Оперативное реагирование
Внедрение системы позволяет сократить время принятия решения, а соответственно уменьшить время реагирования.

6 Работа со сторонним оборудованием
Позволяет интегрировать любое оборудование, которое имеет открытые протоколы передачи данных.

ПОЧЕМУ ОЦЕНЯТ

7 Интеграция с любыми ГИС
Это геоинформационная система высокого уровня. Система поддерживает интеграцию с любыми другими ГИС – как общедоступными, так и специализированными.

8 Привязка видеоизображения к географическим координатам и времени
При получении координат и времени события система выводит видеоизображение со стационарных камер, контролирующих эту зону. Поворотные камеры производят соответственное позиционирование.

Цена рассчитывается под конкретный объект
Производитель: Консорциум "Интегра-С" см. стр. 151 "Ньюсмейкеры"

Гибкость, надежность, безопасность

Накопители SkyHawk AI для систем видеонаблюдения

ЧТО УНИКАЛЬНОГО

1 Производительность: бесперебойная запись видеоданных высокого разрешения при одновременном использовании этих данных для видеоаналитики
Первый специализированный накопитель для решений в области видеонаблюдения, использующих искусственный интеллект. Накопитель записывает высококачественное видео высокого разрешения без пропуска кадров, при этом позволяет без потери производительности проводить аналитику записанных данных.

2 Работа с искусственным интеллектом
Диск разработан специально для систем видеонаблюдения с технологией искусственного интеллекта.

3 Конкурентов нет
Единственное в своем роде решение AI.

ЗАЧЕМ ПОКУПАТЬ

4 Для расширенной видеоаналитики
Накопитель идеально подходит для сетевых видеорегистраторов с расширенными функциями аналитики.

5 Круглосуточный режим
Накопитель справляется с высокими рабочими нагрузками в круглосуточно работающих системах видеонаблюдения.

ПОЧЕМУ ОЦЕНЯТ

6 Запись без пропуска кадров
Микропрограмма ImagePerfect AI, записывающая высококачественное видео высокого разрешения без пропуска кадров.

7 Емкость до 10 Тбайт
Позволяет создавать масштабируемые системы высокой емкости для видеонаблюдения.

Производитель: Seagate Technology
Ценовой сегмент: Средний (25 000 руб.) см. стр. 152 "Ньюсмейкеры"

ASP-4 – новое слово в системах доступа

Кластерный контроллер СКУД и ОС от APOLLO

ЧТО УНИКАЛЬНОГО

1 Создание кластеров
До 32 контроллеров ASP-4 могут объединяться в кластер и получать информацию обо всех событиях в нем. Вход и выходы можно связывать друг с другом в пределах всего кластера.

2 Повышение надежности СКУД и ОС
Возможность программирования ключевых алгоритмов на уровне "железа".

3 Масштаб
256 считывателей на кластер.

ЗАЧЕМ ПОКУПАТЬ

4 Для любых объектов
Подходит для любых объектов, где требуется система безопасности последнего поколения, включающая СКУД и ОС, вне зависимости от отраслевой принадлежности.

5 Унификация
Один ASP-4 может быть центральным контроллером кластера, дверным контроллером СКУД, охранной или релейной панелью, управлять лифтом.

6 Индивидуальная пользовательская логика
Скрипты позволяют программировать сложные реакции и собственную логику работы на уровне контроллера и кластера.

ПОЧЕМУ ОЦЕНЯТ

6 Высокий уровень безопасности
Шифрации на основе TLS-протокола. OSDP для защищенного подключения считывателей. Встроенное ПО на основе ОС Linux.

7 Много задач – одно устройство
До 256 считывателей в кластере, подключенных по OSDP-интерфейсу. Не надо держать в ZIP множество узкоспециальных контроллеров и модулей, один ASP-4 может конфигурироваться в соответствии с текущей задачей.

Розничная цена: от 11 000 руб. (на точку доступа)
Предоставил информацию: "Компания "ААМ Системз"
Производитель: APOLLO (США) см. стр. 151 "Ньюсмейкеры"

Качество по доступной цене

Пожарная панель GST-IFP8-RU

ЧТО УНИКАЛЬНОГО

1 Большая емкость
Сетевая пожарная панель на 8 шлейфов с возможностью построения сети из 64 панелей. 8 адресных шлейфов по 242 адресным точкам, общая емкость одной панели – 1936 точек.

2 Высокая надежность
Сокращение числа ложных срабатываний.

ЗАЧЕМ ПОКУПАТЬ

3 Для строительных объектов
Панель GST-IFP8-RU предназначена для объектов коммерческого строительства.

4 Создание автономной системы
Недорогая адресно-аналоговая АПС с возможностью построения сетевой инфраструктуры и централизованной автономной системы АПС и АПЗ.

ПОЧЕМУ ОЦЕНЯТ

5 Электронное программирование
Адреса и типы адресных детекторов и модулей программируются электронным способом.

6 Большое количество адресных устройств
Более 123 000 адресных устройств на одну систему.

Ценовой сегмент: Низкий (стоимость одного извещателя – 1000 руб.)
Представляет информацию: AHI CARRIER FZC
Производитель: Gulf Security Technology см. стр. 152 "Ньюсмейкеры"

Комфорт сотрудников при снижении затрат на учет рабочего времени

Система PERCo-S-20

ЧТО УНИКАЛЬНОГО

1 Гибкий график
Позволяет совместить стремления руководителей повысить производительность труда и создать комфортный климат для сотрудников.

2 Без нарушений дисциплины
Сотрудники управляют своим рабочим временем, не нарушая дисциплину. Время, потраченное на опоздания, уходы раньше и перерывы, можно отработать.

3 Табель учета в 1С
Применение гибкого графика рабочего времени не исключает возможность получать в 1С табель учета в формате, предусмотренном законодательством.

ЗАЧЕМ ПОКУПАТЬ

4 Снижение затрат
Гибкий график снизит затраты на учет в государственных учреждениях, малых и средних офисах компаний и на многих других объектах.

5 Удобство для кадровых служб
Администрация и сотрудники кадровых служб оценят наличие удобного инструмента для управления рабочим временем сотрудников.

ПОЧЕМУ ОЦЕНЯТ

6 Личный контроль отработанного времени
Принцип гибкого графика – отработка сотрудником положенного времени при возможности прийти позже или уйти раньше.

7 Четкий баланс
Гибкий график с накоплением задолженности позволяет сотруднику закрыть неотработанное за отчетный период время оправдательным документом.

8 Допустимые пределы отклонений
Отклонения от графика работы в установленных руководством пределах не считаются нарушениями дисциплины.

Ценовой сегмент: Средний
Производитель: PERCo
см. стр. 152 "Ньюсмейкеры"

Удобный инструмент управления предприятием

Система контроля доступа и учета рабочего времени PERCo-Web

ЧТО УНИКАЛЬНОГО

1 Эффективное управление
PERCo-Web – это удобный инструмент для эффективного управления предприятием. Система предназначена для усиления безопасности и повышения дисциплины труда персонала.

2 Работа в любом браузере
Подключение к системе аналогично входу на сайт. Работать с ней можно в любом браузере, используя любые платформы, в том числе и мобильные.

3 Интеграция с биометрией
PERCo-Web работает с биометрической идентификацией. Сложность подделки отпечатка пальца обеспечивает надежную защиту от прохода по чужому пропуску.

ЗАЧЕМ ПОКУПАТЬ

4 Универсальное решение
Гибкая архитектура позволяет системе успешно работать в бизнес-центрах, на промышленных предприятиях, в офисах, учреждениях и на других объектах.

5 Рост прибыли
Внедрение системы повышает уровень безопасности предприятия, обеспечивает рост производительности труда, что ведет к росту прибыли.

6 Контроль дисциплины
Руководитель контролирует дисциплину сотрудников в удобное время, используя компьютер, планшет или смартфон.

ПОЧЕМУ ОЦЕНЯТ

7 Не требуется установка ПО
Благодаря Web-технологиям система не требует установки ПО на рабочие места пользователей, информация хранится на сервере компании.

8 Бесплатно для штата до 100 сотрудников
Бесплатный пакет ПО позволяет организовать контроль доступа на предприятии со штатом не более 100 сотрудников.

Ценовой сегмент: Средний
Производитель: PERCo
см. стр. 152 "Ньюсмейкеры"

Полноростовые турникеты-шлюзы ПРШ1/3 и ПРШ2/4 Безопасность реальна!

ЧТО УНИКАЛЬНОГО

1 Универсальность
В случае необходимости могут работать как обычные полноростовые турникеты с высокой пропускной способностью.

2 Оперативность изменения режима работы
Перестройка режима работы турникета (шлюз – турникет и обратно) занимает не более 30 мин.

3 Принцип действия
В однопроходном трехлопастном турникете-шлюзе ПРШ1/3 предусмотрен дополнительный релейный сигнал "Человек в шлюзе", который позволяет обеспечить работу турникета в режиме шлюза, исключающую несанкционированный проход людей. В двухпроходной четырехлопастной модели ПРШ2/4 работа турникета в режиме шлюза, исключающая несанкционированный проход людей, обеспечивается преграждающими дугами, которые препятствуют входу людей в соседние секторы турникета-шлюза.

ЗАЧЕМ ПОКУПАТЬ

4 Для режимных объектов
Потенциальные потребители – режимные объекты.

5 Универсальность
Многофункциональность, повышенная защищенность от несанкционированного входа.

ПОЧЕМУ ОЦЕНЯТ

6 Запатентованные технологии
Конструкции турникетов-шлюзов защищены патентами РФ.

7 Удобные габариты
ПРШ1/3 – 1500x1500x2450 мм;
ПРШ2/4 – 2210x1500x2450 мм.

Ценовой сегмент: Средний
(ПРШ1/3 – 375 613 руб. с НДС, ПРШ2/4 – 711 676 руб. с НДС)
Производитель: ООО ПК "РостЕвроСтрой" см. стр. 152 "Ньюсмейкеры"

Безопасность, безотказность, быстрота

Взрывобезопасное опорно-поворотное устройство из нержавеющей стали PTR-407Ex

ЧТО УНИКАЛЬНОГО

1 Работа в суровых условиях
Возможность устанавливать и позиционировать камеры видеонаблюдения в условиях Крайнего Севера ("холодный старт" при -61 °С), взрывоопасных и агрессивных средах.

2 Улучшенные эксплуатационные показатели
Класс взрывозащиты 1Ex dIIBT6 Gb, угол поворота 360 град., диапазон рабочих температур -61…+50 °С, скорость поворота до 35 град., точность позиционирования +/-0,3 град.

ЗАЧЕМ ПОКУПАТЬ

3 Области применения
Химическая и нефтехимическая отрасли, добыча и транспортировка нефти и газа, морские суда, буровые платформы, речные и морские акватории.

4 Соотношение качества и цены
Российский производитель. Разработка под задачи СБ с учетом климатических и эксплуатационных условий на объектах.

ПОЧЕМУ ОЦЕНЯТ

5 Собственная разработка и производство
Разработана и применена интеллектуальная система подогрева для безаварийной эксплуатации изделия в условиях Крайнего Севера.

Производитель: ООО "БИК-Информ" см. стр. 151 "Ньюсмейкеры"

Повышение надежности системы АПС по доступной цене

Дымовой оптико-электронный линейный пожарный извещатель "С2000-ИПДЛ"

ЧТО УНИКАЛЬНОГО

1 Расширение функциональных возможностей
Расширяет функциональные возможности адресной пожарной сигнализации ИСО "Орион" на базе контроллера С2000-КДЛ.

2 Повышение надежности
Система АПС станет более надежной за счет сокращения блоков питания, линий электропитания.

3 Прямая интеграция
Прямая интеграция в широко распространенную систему ИСО "Орион".

ЗАЧЕМ ПОКУПАТЬ

4 Для помещений большой площади
Торгово-развлекательные центры с атриумами, складские комплексы, цеха промышленных предприятий, имеющие большую протяженность или высоту потолков.

5 Лучшее соотношение "цена/функционал"
Лучшее соотношение "цена/функционал" среди отечественных производителей.

6 Снижение стоимости
Переход от релейных на информативные системы с одновременным снижением стоимости оборудования и материалов.

ПОЧЕМУ ОЦЕНЯТ

7 Следование современным тенденциям
Учитывалась современная тенденция – переход на адресные системы и извещатели (ИПДЛ, пламени и т.п.).

8 Важнейший технический параметр
Изменяемая дальность действия – от 5 до 120 м, определяется типом отражателя.

Производитель: ЗАО НВП "Болид" см. стр. 151 "Ньюсмейкеры"

Компания Axis представляет новое программное обеспечение для простого управления и упреждающей защиты от кибератак

Axis Communications объявила о выпуске инструмента AXIS Device Manager, который позволяет легко, безопасно и без лишних затрат выполнять все основные задачи управления при установке и эксплуатации оборудования на территории заказчика. Кроме того, AXIS Device Manager помогает проактивно защищать оборудование и сети в современном мире с его растущим уровнем угроз. Приложение можно использовать для управления примерно двумя тысячами сетевых камер, устройств контроля доступа и аудиоустройств Axis на одном объекте и несколькими тысячами устройств на нескольких объектах.

ПО AXIS Device Manager разработано на базе популярной программной платформы AXIS Camera Management. Оно демонстрирует стремление компании Axis создавать для своих клиентов простые в установке и недорогие в эксплуатации системы, а также решения для защиты оборудования и сетей от киберугроз.

Вот лишь некоторые функции управления оборудованием, которые реализует ПО AXIS Device Manager:

- автоматическое назначение IP-адресов;
- установка, настройка, замена и обновление любых устройств;
- копирование настроек между тысячами устройств;
- подключение к большому количеству серверов и систем;
- поддержка точек восстановления и возврата к заводским настройкам;
- обновление прошивок оборудования;
- работа с учетными записями и паролями;
- установка и обновление сертификатов HTTPS и IEEE 802.1x.

Борьба с киберугрозами

В современном мире постоянно совершенствующихся технологий и в условиях все более изощренных действий киберпреступников чрезвычайно важно обеспечить ежедневное динамичное управление инфраструктурой безопасности. Новое программное обеспечение AXIS Device Manager значительно повышает безопасность оборудования благодаря централизованному управлению учетными записями, паролями и сертификатами, а также повышению защищенности устройств в соответствии с руководством компании Axis по усилению защиты. Это дает системным интеграторам и администраторам возможность легко и без лишних затрат внедрять важные функции управления безопасностью систем.

"Возможность эффективно контролировать, устанавливать, настраивать и защищать все устройства в сети экономит огромное количество времени и сил. AXIS Device Manager – это идеальный инструмент для управления всеми устройствами Axis на всех стадиях жизненного цикла, – объясняет Ола Леннартссон, менеджер по продукции подразделения управления системами компании Axis Communications. – В современном динамичном мире любые статичные устройства и сети не просто несовременны, но и уязвимы для киберугроз. Поэтому важно, чтобы у наших клиентов был инструмент для простого, оперативного и эффективного управления всеми устройствами в сети. Именно таким инструментом является AXIS Device Manager".

ПО AXIS Device Manager заменяет собой приложение AXIS Camera Management. Его можно бесплатно скачать на сайте AXIS Device Manager. ■

Быть оптимистами, верить в собственные силы

Интервью об итогах 2017 г.

Аэропорт "Платов" в Ростове-на-Дону построен с нуля

Максим Соколов
Министр транспорта
Российской Федерации

– Максим Юрьевич, расскажите об основных результатах работы транспортного комплекса в 2017 г.

– 2017 год, как и любой другой, стал непростым для транспортного комплекса. Но в целом отрасль справилась с поставленными задачами, можно говорить о позитивных тенденциях ее развития. Так, воздушным транспортом перевезены свыше 100 млн пассажиров. Показатель является рекордным для истории как российской, так и советской гражданской авиации. Рост воздушных перевозок составляет около 20%.

Успешно отработала железнодорожная отрасль. Перевозки пассажиров показывают уверенный рост, по итогам года количество перевезенных граждан в пригородном и дальнем сообщении значительно превысило 1 млрд человек.

Можно отметить ряд важных проектов по развитию транспортной инфраструктуры. С нуля построен новый аэропорт "Платов" в Ростове-на-Дону. Он полностью обеспечит потребности болельщиков на предстоящем ЧМ-2018. В январе открылся совершенно новый аэропорт "Рощино" в Тюмени, полностью завершена реконструкция аэродрома Волгограда, инфраструктуры в аэропортах Калининграда, Нижнего Новгорода, Самары, Екатеринбурга и Саранска. За счет частных инвестиций построены новые аэровокзальные комплексы в аэропортах Анапы, Перми, Красноярска.

Активно велось дорожное строительство по всей стране, вводились новые и реконструированные участки федеральных трасс, приводились в нормативное состояние региональные автодороги. С использованием средств системы "Платон" введены Затонский мост в Уфе, новый Борский мост в Нижнем Новгороде, Ворошиловский мост в Ростове-на-Дону и Свердловский мост в Пензе. В рамках проекта "Безопасные и качественные дороги" до 52% выросла доля улично-дорожной сети городских агломераций в нормативном состоянии. Более чем на 46% удалось сократить количество мест концентрации ДТП.

Сильным инструментом в условиях дефицита бюджета для нас, транспортников, является механизм государственно-частного партнерства (ГЧП). В ноябре стартовал ГЧП-проект по строительству автомобильного обхода Хабаровска. Продолжают реализовываться и другие ГЧП-проекты: скоростная автодорога М-11 Москва – Санкт-Петербург и ЦКАД в Московской области, которые являются составными частями коридора "Европа – Западный Китай". Во многих регионах готовятся новые масштабные проекты с привлечением частных инвестиций. Значимым является строительство восточного выезда из Уфы, который поддержан на высоком государственном уровне. Это строительство мостового перехода в Пермском крае, комплексное развитие аэропорта Хабаровска, аэровокзального комплекса в Петропавловске-Камчатском, международного морского терминала для приема круизных судов в Калининграде и ряд других проектов.

– Все ли аэропорты готовы принимать команды и болельщиков, которые приедут в Россию на ЧМ-2018?

– В настоящее время ведется активная модернизация аэропортовой инфраструктуры, в том числе в рамках подготовки к предстоящему чемпионату.

Для транспортного обеспечения ЧМ предусмотрено использование 13 аэропортов в 11 городах-участниках. И в целом работы идут по графику. Уже полностью завершена подготовка аэродромной инфраструктуры в аэропортах Сочи, Казани, Внуково и Пулково. Открылся новый терминал аэропорта "Гумрак" в Волгограде. Введена 1-я очередь нового терминала международного аэропорта Калининграда.

Как я уже говорил, введен в эксплуатацию аэропорт "Платов". Там стартовали регулярные пассажирские перевозки. Новый аэропорт в полной мере обеспечит потребности болельщиков в период чемпионата.

В аэропортах "Домодедово", "Шереметьево", "Храброво", а также Нижнего Новгорода, Саранска, Самары, Екатеринбурга завершается реконструкция объектов, необходимых для обеспечения проведения чемпионата мира по футболу, и к маю 2018 г. данные аэропорты будут готовы принимать команды и болельщиков, прибывающих на матчи в соответствующие города.

В целом отмечу уверенные темпы развития нашей аэропортовой и аэродромной инфраструктуры, которая к началу чемпионата мира по футболу в полной мере обеспечит комфорт и безопасность для всех участников соревнований.

– Можно ли то же самое сказать о дорожной инфраструктуре? Какие объекты были построены специально для проведения чемпионата? Сколько в них вложено средств?

– В рамках подготовки к ЧМ-2018 на софинансирование из федерального бюджета дорожной инфраструктуры предусмотрено более 32 млрд рублей.

Из 12 мероприятий по строительству и реконструкции дорог к чемпионату реализованы пять. Два из них – в Саранске: построена новая автомобильная развязка в городе, реконструирована автомобильная дорога к аэропорту. Реконструирована автодорога от Калининграда до границы с Польшей. В Ростове-на-Дону построены два объекта: автодорога, которая связала новый аэропорт "Платов" и магистраль "Дон", и магистральная улица, обеспечивающая подъезд к стадиону.

В Санкт-Петербурге перед Кубком конфедераций открыли движение на путепроводной развязке на пересечении Пулковского шоссе с Дунайским проспектом, которая обеспечивает подъезд к аэропорту "Пулково".

В целом завершение строительства объектов в установленные сроки к чемпионату не вызывает сомнений.

Строительство Крымского моста по-прежнему остается в центре внимания общественности

– По данным на начало декабря, за время работы системы "Платон" уже собрано более 38 млрд рублей. Планируются ли какие-то корректировки в работе системы? Снизилось ли количество неплательщиков?

– Результаты работы "Платона" спустя два года после запуска системы говорят сами за себя. На ремонт дорог и строительство мостов собрано порядка 40 млрд рублей. Число транспортных средств, зарегистрированных в системе, уверенно приближается к отметке в 1 млн. За 2017 г. прирост составил более 150 тыс. большегрузов. Большинство российских перевозчиков получили бесплатные бортовые устройства. Положительно зарекомендовала себя система внесения платы через маршрутные карты, но ее используют в основном иностранные грузоперевозчики.

Напомню, что система создана на основе ГЧП. На сегодняшний день в ней зарегистрированы перевозчики из более чем 70 стран – всего свыше 155 тыс. большегрузов нерезидентов. Благодаря системе "Платон" дополнительные средства на российские дороги поступают за счет транзитного транспорта.

15% собранной платы приходится на иностранных перевозчиков. С учетом перспективного развития транспортных коридоров поступления в дорожный фонд будут только возрастать, это позволит более высокими темпами развивать дорожную сеть России.

Отмечу, что за первые два года работы системы учтены и полностью реализованы все предложения грузоперевозчиков. Введена постоплата, сохранен льготный тариф, модернизированы сервисы системы для дополнительного удобства пользователей и максимально упрощено получение информации для предоставления ФНС при использовании права на налоговый вычет.

Продолжается плановая работа по усилению контроля за нарушителями, что также отвечает требованиям законопослушных перевозчиков. Система контроля полностью развернута на всех федеральных трассах, работают около 500 рамных конструкций и 100 спецавтомобилей.

Передача полномочий по выявлению нарушителей от МВД России Ространснадзору позволит сконцентрировать контроль за соблюдением законодательства в ведении одной структуры и обеспечить равные конкурентные условия для предпринимателей в сфере грузоперевозок.

– В центре внимания общественности по-прежнему остается строительство Крымского моста...

– Выполнение работ по основным мостовым конструктивам моста – опорам и пролетам автодорожной части – составляет почти 100%. Полностью готовы все 288 опор, в том числе 85 опор в морской акватории. Собрано более 100 тыс. т металлоконструкций пролетных строений под автодорогу – это около 95% от проекта. Ведется формирование дорожного полотна.

С момента подписания госконтракта в феврале 2015 г. строительство профинансировано более чем на 170 млрд рублей (более 75% от суммы контракта). На данный момент заказчиком строительства приняты выполненные работы на сумму более 111 млрд рублей – это 50%.

Несмотря на то что основные конструктивы автодорожного моста готовы, у строителей еще много задач по обустройству автодороги. Движение транспорта будет открыто только после того, как строители обеспечат необходимые условия для безопасного движения по мосту.

– А как обстоят дела с развитием речных перевозок?

– В 2016 г. в рамках Госсовета приняты важные системные решения по развитию внутреннего водного транспорта. С учетом этого в 2017 г. на содержание ВВП и судоходных гидротехнических сооружений дополнительно выделено 4,5 млрд рублей. За счет этого повышены категории содержания путей на участках протяженностью более 1 тыс. км, увеличены сроки навигации на 1,5 тыс. км внутренних водных путей.

Это позволило не только остановить падение грузооборота, но и привлечь новую грузовую базу. Уже в этом году с наземных видов транспорта переключено более 5 млн т грузов (нефтепродукты, минерально-строительные грузы, зерновые и другие). Так, например, на реке Белая переключение составило почти 900 тыс. т.

Естественно, это работа не одного года. Нужно восстановить водные пути, стабильно поддерживать их габариты. Необходимо и дальше финансировать содержание внутренних водных путей в соответствии с нормативом. К сожалению, на 2018 г. проектом федерального бюджета необходимых ассигнований на это не предусмотрено.

Развитие перевозок внутренним водным транспортом сдерживает и наличие инфраструктурных ограничений. На Единой глубоководной системе существуют "узкие места", где глубины значительно меньше, чем на остальных участках. По итогам Госсовета стартовали два важнейших для водного транспорта проекта. В 2016 г. приступили к проектированию Багаевского гидроузла, а 2018-м начнется его строительство. Полным ходом идет проектирование и Нижегородского гидроузла.

Для отрасли критически важно построить эти объекты. Именно они позволят на всем протяжении Единой глубоководной системы обеспечить достижение единой четырехметровой глубины и рост провозной способности речного флота более чем в два раза.

Ликвидация инфраструктурных ограничений на внутренних водных путях создаст понятные, прозрачные условия для грузо- и судовладельцев. Условия, когда можно планировать свою деятельность, заключать долгосрочные контракты на перевозку. Результатом этого мы видим рост перевозок по реке, переключение грузопотоков на водный транспорт, снятие нагрузки с автомобильных дорог.

– Есть ли уверенность, что транспортный комплекс сохранит тенденцию роста?

– Надо быть оптимистами, верить в собственные силы, не пасовать перед трудностями. А потенциал у отрасли большой! ■

www.mintrans.ru

Публикуется с сокращениями

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

Об ИТ-технологиях, работе с подрядчиками, чиповании и роли шофера в транспортной безопасности

Департамент безопасности транспорта компании X5 Retail Group был образован в 2013 г. в структуре Дирекции по транспорту (в то время Управление). Его основная цель – создание и поддержание на должном уровне системы безопасности компании, обеспечивающей безопасное функционирование автотранспортных предприятий и хеджирующее риски потерь как при доставке товара, так и в деятельности самой Дирекции по транспорту

Константин Коноваленко
Директор департамента безопасности транспорта Дирекции по транспорту компании X5 Retail Group

Департамент безопасности транспорта состоит из подразделений безопасности региональной (городской) доставки, подразделения безопасности федеральных и межфилиальных перевозок и претензионного отдела.

Приоритетные бизнес-задачи

Основными задачами департамента являются:

- обеспечение и поддержка работы транспортных подразделений компании по направлению "безопасность" (закупки, списания, хищения ГСМ, кадровая безопасность, операционная поддержка подразделений АТП, логистических площадок, взаимодействие с правоохранительными органами);
- минимизация потерь при доставке ТМЦ как собственным, так и наемным транспортом (все бизнес-процессы, касающиеся нарушений правил перевозки и сохранности перевозимых грузов);
- выявление рисков необоснованных затрат.

Кроме того, сотрудники активно участвуют в проектной деятельности и внедрении новых процессов и ИТ-систем в работу департамента.

Транспортный парк компании

Автопарк компании состоит из более 3000 грузовиков, распределенных по 18 АТП. Основу парка составляют автомобили городской доставки марки Isuzu, Iveco, Hino, MAN грузоподъемностью 5–20 т и 700 грузовиков КАМАЗ, Mercedes, которые обеспечивают межфилиальные перевозки. Все собственные транспортные средства оборудованы устройствами защиты от проникновения и системами контроля, установленными на производстве, а тестируются и активизируются по прибытии транспортного средства в АТП. Кроме того, мы регулярно опробуем на своих автомобилях вновь появляющиеся системы безопасности. Так, в настоящее время заканчиваем тестирование обновленной системы контроля открытия дверей КУНГа. В старом решении использовались простые датчики (гирконы), что не способствовало устойчивой работе системы в связи с их ненадежностью. Обновленная система работает на NFC-технологии, когда между двумя небольшими устройствами происходит обмен информацией на очень коротком расстоянии. К сожалению, все комплектующие производятся за рубежом, а хотелось бы получить рабочую модель на отечественных изделиях.

ИТ-решения для управления транспортными перевозками

В наше время без ИТ-систем нельзя решить ни одной полновесной задачи, поэтому и наша компания активно применяет предлагаемые решения. Главная цель как подразделения безопасности, так и бизнес-подразделений одна: свежие овощи и фрукты и другая продукция должны поступить в магазины X5 вовремя и хорошего качества. Бизнес-подразделения отвечают за доставку, а мы – за сохранность. Синергия целей и подходов позволяет нам всем выполнять главную задачу и при этом минимизировать риски.

Для управления и контроля этого многообразия перевозок мы используем как стандартные общепримяемые решения типа TMS (Transportation Management System) и Yard Management, так и разработанные специально для нас. Одним из них является система оперативного мониторинга (СОМ), которая создана под бизнес-требования нашей компании и позволяет в режиме онлайн контролировать основные параметры доставки по каждой машине (включая работающие с нами по контракту) по всем АТП и распределительным центрам, а также логистическим площадкам. Несмотря на то что это операционная система, предназначенная для контроля и управления транспортом, в нее вшиты функции контроля систем безопасности, установленных на транспортных средствах и необходимых для выявления нарушений.

С точки зрения безопасности мы обладаем ИТ-системой с широкими аналитическими возможностями и простым интерфейсом, что позволяет получать в онлайн-режиме данные о нарушениях и быстро принимать по ним решения. Предоставляемая системой информация ложится в основу служебных проверок и претензий к перевозчикам. Система очень простая и дает возможность в кратчайшее время научить работать в ней новых сотрудников.

Мы понимаем, что собственный автопарк – это мощный, хотя и не дешевый рычаг помощи в цепочках поставок для наших торговых сетей, однако и без наших партнеров и коллег – транспортных компаний – нам не обойтись.

В настоящее время мы активно работаем как с региональными, так и крупными федеральными компаниями. В принципе, мы готовы к сотрудничеству со всеми перевозчиками, даже с ИП, владеющими 1–2 машинами, которые работают, как и мы, по принципам "открытость – эффективность – ответственность".

Помимо проверенных решений по заключению договоров с крупными компаниями, у нас в X5 активно внедряется сервис GoCargo, он наиболее привлекателен для средних и малых транспортных фирм, работает через мобильное при-

ложение и схож по принципам работы с приложением Uber.

Взаимодействие с подрядными организациями

Так как компания работает не только с собственным транспортом, но и с привлекаемым, то мы включены и в решение спорных вопросов с контрагентами. В 2015 г. после прихода новой команды мы изучили ситуацию с доставкой продуктов привлеченным транспортом. Уровень сервиса был недостаточным, а с условием того, что доставляли продукты питания, так и вовсе плохим, особенно в части соблюдения температурного режима. Требования СанПиН соблюдались не всеми.

Для изменения ситуации в 2016 г. мы реализовали проект "Паспортизация", в рамках которого сотрудниками безопасности в регионах работы были обследованы более 2000 транспортных средств, по итогам работы допущено к перевозкам около 1600 автомобилей. Все это позволило повысить уровень соблюдения температурного режима до 93–95%. Стало меньше претензий по доставке товара, уменьшились потери. Вот так решение, казалось бы не относящееся к функции безопасности, но придуманное и внедренное нами, положительно сказалось на выполнении целевых задач департамента.

С 2017 г. мы помогаем коллегам и проверяем автотранспорт, работающий через мобильное приложение GoCargo. Обычно это не занимает более 15 минут, достаточно подать транспорт к ближайшему РЦ, где есть сотрудник безопасности, и он проверит автомобиль на готовность к работе.

Нововведения в транспортной логистике

В ближайшие несколько лет транспортная логистика будет развиваться в трех направлениях. Нас ждет рост собственного парка сетевых компаний и их активный переход на транспорт, использующий смешанные виды топлива (газ – дизель, электричество – дизель, бензин – газ и т.д.). Это реально снижает издержки транспорта, ведь основные затраты транспортные компании несут на топливе, около 40–45% в тарифах. Применение смешанной системы питания двигателя существенно снизит затраты предприятий. У нас сейчас 100 автомобилей, оборудованных для работы на газомоторном топливе. Их эксплуатация несущественно отличается от эксплуатации машин с дизельными двигателями. Будут развиваться проекты по перевозке продуктов железнодорожным транспортом, особенно в удаленные регионы. И неминуем рост доли наемного транспорта в регионах с привлечением ИТ-технологий.

Роботизированный склад – наше будущее

Перспективным сейчас выглядит внедрение системы чипования в цепочку поставки "поставщик – склад – транспорт – магазин". Для этого государству необходимо только разработать "правила игры" и договориться с производителями. Основные элементы системы уже повсеместно применяются в повседневной жизни: чипы в билетах, в обуви, в шубах; считыватели – на границе и таможенных постах. Роботизированные склады эксплуатируются уже много лет. Внедряется электронный документооборот.

Представьте: выезжает от поставщика грузовик с товаром, на выезде с предприятия товар сканируется (проезд сквозь рамку) и автоматически списывается с остатков, по системе EDI (электронный документооборот) направляется на склад приемки. Там операция сканирования повторяется, товар ставится на приход, а так как каждая упаковка имеет метку, то роботизированный склад распределяет товар, формирует грузоместа согласно заявке, направляет товар на загрузку. По приезде в магазин – та же рамка, товар сразу ставится на остатки. При такой схеме существенно оптимизируются расходы склада, становится прозрачной как для регулятора, так и для владельцев работа поставщиков, складов, магазинов. Видны остатки, понятно планирование, а списания и потери локализируются и стремятся к нулю.

В заключении хочется сказать, что еще 7–10 лет – и всю нашу деятельность, в том числе безопасность, окутают ИТ-технологии, без которых мы уже сейчас не можем обходиться. ■

Автопарк компании X5 Retail Group состоит из более 3000 грузовиков

Профессия водителя будет востребована еще как минимум 20–30 лет

Крепче за баранку держись, шофер!

Как ни странно, главная проблема сейчас – люди. В настоящее время в государстве отсутствует как таковая система подготовки высококачественных профессионалов-водителей. Многие из них ушли в собственный бизнес, другие по возрасту уже на пенсии, и на рынке образовался большой дефицит водителей категории Е, да и с водителями категории С достаточно много проблем.

Сейчас приходит водитель с категорией В–С по документам, получает новую машину, в течение 2–3 месяцев ее разбивает/ломает и уходит…

Я всегда вспоминаю своих дедов. Оба прошли всю войну. Оба – шоферы (слово "водитель" воспринимали как ругательное). Я помню, как они меня водили в АТП, куда приходили молодые ребята и получали не новую машину, учились, сдавали на классность, после чего им давали ключи от более современных автомобилей, и т.д.

Сейчас многие скажут, что это устаревающая профессия. Ничего подобного. При размерах нашего государства профессия водителя будет востребована еще как минимум 20–30 лет

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

Технологии информационного моделирования для создания объектов инфраструктуры железнодорожного транспорта

Технологии информационного моделирования (BIM-технология) активно развиваются во всем мире. Выбор области их приоритетного применения в конкретной стране напрямую зависит от стратегии ее экономического развития. Для России огромное значение имеет транспортная инфраструктура, в частности железные дороги. Эта важнейшая отрасль развивается уже без малого 200 лет, поэтому на один проект создания участка железной дороги с нуля приходится множество проектов реконструкции существующих объектов инфраструктуры железнодорожного транспорта. Они выполняются в условиях движения поездов, пассажиров, городского транспорта, а также наличия различных инженерных сетей – городских и железнодорожных

Петр Бубнов
Главный инженер СУ-308

Елена Колосова
Директор по развитию ООО "К4", вице-президент Национальной палаты инженеров, к.т.н.

Кирилл Сухачев
Генеральный директор ООО "К4", к.т.н.

BIM-технологии позволяют обладать информацией об объекте на всех стадиях его жизненного цикла – от подготовки исходных требований до вывода из эксплуатации включительно. Это дает всем участникам жизненного цикла объекта как новые преимущества, так и новые обременения. В этом особенность любой новой технологии, и BIM здесь не исключение. Строительная организация получает, во-первых, возможность оценки и согласования справедливой цены на СМР, которая зависит не только от корректной стоимости строительных материалов, но и от справедливого учета факторов, влияющих на условия производства работ. А во-вторых, появляются новые перспективы по организации и обеспечению безопасности работ, особенно в проектах реконструкции существующих объектов железнодорожной инфраструктуры. Очевидным обременением является необходимость заплатить за услуги инженера-консультанта, который позволит запустить применение нужной части BIM-технологий в компании. Ведь полный арсенал BIM-технологий вряд ли нужен кому-то, кроме застройщика/эксплуатирующей организации.

Безопасность проведения реконструкции

Проект реконструкции существующего объекта часто отличается от проекта строительства нового объекта наличием еще одной стороны – эксплуатирующих организаций, в том числе службы движения, дирекции инфраструктуры, ревизорского аппарата и других применительно к нашей тематике. Ее задачей является прежде всего обеспечение запланированных эксплуатационных показателей на данном участке дороги (столько-то таких-то поездов в сутки). Но любая реконструкция нарушает этот годами сложившийся порядок. Появляются строительная техника и стройматериалы, рабочие, которым нужно время и место на производство работ. Возникает проблема согласования "окон", где строительной организации выгодно получить "окна" максимального размера, а службе движения – оставить их такими, как требует утвержденное расписание движения поездов. Рассмотрение и согласование "окон", тем более продолжительных, всегда занимает много времени. Продолжительных "окон" требуют многие технологические операции: монтаж пролетных строений, укладка путей, установка разгрузочных пакетов и многие другие. В процессе согласования продолжительности "окна" строитель постоянно пытается "впихнуть невпихуемое", выполняя требования безопасности производства демонтажных и строительно-монтажных работ. К ним относятся и очевидные требования типа сохранности инфраструктуры: нельзя допустить зацепление грузом контактной сети или повреждение экскаватором подземных коммуникаций. Отдельная важная тема – это безопасность движения поездов на реконструируемом участке. Ведь типичная ситуация, приводящая к чрезвычайным ситуациям в ходе реконструкции железных дорог – это нарушение габарита к соседнему пути. В этом случае грузоподъемный механизм, экскаватор и т.д., поворачиваясь, противовесом задевает подвижной состав, проходящий по соседнему пути, последствия чего могут быть не только печальными, но даже трагическими.

Эффективно решить все эти задачи позволяет визуальная модель организации строительства (так называемая 4D/5D/6D), являющаяся компонентом BIM-технологий.

От безопасности к справедливой стоимости СМР

В ноябре 2016 г. вышел ряд постановлений Правительства РФ об обязательной проверке достоверности сметной стоимости строительства Главгосэкспертизой для объектов, финансируемых за счет средств компаний с государственным участием. Разумеется, объекты транспортной инфраструктуры попали в их число. Согласно постановлению Правительства Российской Федерации № 1452 от 23.12.2016 г., информация о ценах на строительные ресурсы размещается в федеральной государственной информационной системе ценообразования в строительстве (ФГИС ЦС), создание, ведение и развитие которой поручено Главгосэкспертизе России. Информацию об отпускных ценах в эту систему передают сами предприятия-производители. Поэтому сегодня стоимость СМР определяется исключительно в рамках государственных норм регулирования, а стоимость материалов принята по фактическим данным производителей.

И заказчику, и подрядчику во все времена выгодно определить справедливую стоимость строительства, потому что первому она позволяет заработать и развиваться дальше, а для второго снижает риск того, что он не справится совсем или как минимум придет за дополнительным финансированием. Раньше "справедливая" стоимость не декларировалась открыто, но часто достигалась "ухаживанием" за стоимостями материалов, трудоемкостью и физическими объемами. Сегодня данная практика

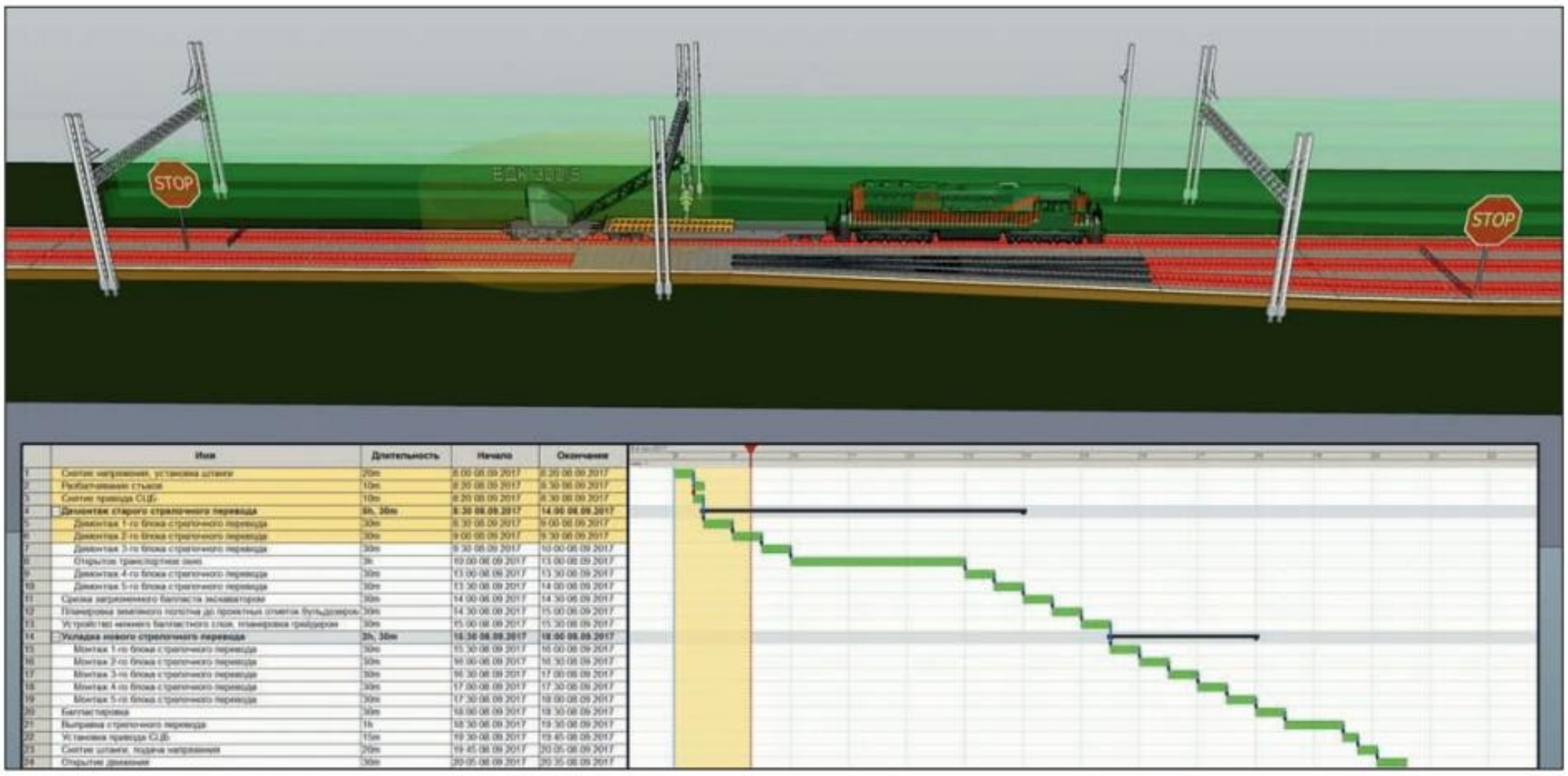


Рис. 1. Пример применения технологии визуального планирования при реконструкции участка железнодорожного полотна действующей ветки

постепенно уходит в прошлое. Поэтому для обоснования реальной стоимости остается скрупулезная проработка технологии СМР с учетом всех вышеозначенных ограничений. И именно в этом технология информационного моделирования является самым сильным инструментом.

Рассмотрим примеры. МДС 81-33.2004, основной документ в ценообразовании в строительстве, а также технические части сборников ГЭСН предполагают уточнение сметных расценок путем применения поправочных коэффициентов к сметным нормам использования машин и механизмов и фонду оплаты труда. Так, например, использование коэффициента "работа в окно" на железной дороге напрямую зависит от продолжительности этой работы: до двух, четырех и свыше четырех часов соответственно. Традиционный метод определения коэффициента – это возможная продолжительность "окна", указанная службой движения. Однако в данном случае не учитываются работы, связанные с выездом рабочего поезда, снятием напряжения и другими мероприятиями, не относящимися к самой работе (вспомогательными). Здесь моделирование всей технологической цепочки позволяет рассчитать реальное время производства работ в "окно" и применить справедливый коэффициент. Причем "чистый" календарно-сетевой график в данном случае помогает слабо, потому что, во-первых, он не учитывает пространственные ограничения, а во-вторых, большинству сотрудников службы движения разобраться с ним будет затруднительно. Визуальная модель организации строительства (часть BIM-технологий) неизмеримо нагляднее покажет все особенности данной технологической цепочки.

Другой пример – это производство СМР в условиях движения поездов. Очень значимый коэффициент может применяться, согласно Технической части, только в пределах 4 м от оси пути и/или 6 м от головки рельсов, а также в случаях, когда части механизмов или монтируемых элементов попадают в эту зону. Здесь визуальное моделирование технологических цепочек строительных процессов также становится крайне значимым, потому что позволяет точно рассчитать и показать, где именно этот коэффициент применим и почему.

Таким образом, применение технологий информационного моделирования строительной организацией может быть не просто рентабельным, но и окупиться буквально в первом крупном проекте. Сложно, как обычно, решиться. А кроме того, сложно получить основу для применения данной технологии в строительстве – 3D-модель объекта.

О трехмерном проектировании

Наличие 3D-модели объекта строительства или реконструкции – необходимое условие для создания и применения визуальной модели организации строительства. Однако не все просто в этом вопросе. Проблема в том, что проектировщики не могут в полной мере почувствовать преимущества от перехода на трехмерные САПР взамен "плоских" систем автоматизированного черчения без проведения значительных технических, организационных и социальных преобразований, вне всякого сомнения затратных и трудных. Поэтому далеко не все проектные организации, даже заявившие о переходе к трехмерному проектированию, могут продемонстрировать практические результаты. Следовательно, далеко не всегда строительная организация может рассчитывать на получение 3D-модели от проектировщика. Это не ставит крест на применении ею BIM-технологий, но требует дополнительных затрат – поднятия 3D-модели по плоским чертежам.

Это была плохая новость. А хорошей новостью является то, что для целей разработки организационно-технологических решений в части СМР полная 3D-модель, из которой можно напечатать РД, не нужна. Вполне достаточно более грубой (менее детализированной) модели, создать которую можно гораздо быстрее и менее накладно (в обоих случаях в разы). Сделать самим или заказать на рынке такую модель уже не проблема. Зато появляется возможность использовать для себя все вышеописанные преимущества, не дожидаясь, пока застройщик и проектировщик договорятся о форме выпуска проектной продукции.

Будущее наступает сегодня

Информационное моделирование открывает новую страницу в развитии всего строительного комплекса. Эти технологии могут привнести прозрачность во взаимоотношения заказчика и подрядчика, хотя, сказать по правде, именно этот тезис сегодня пугает многих участников строительных проектов больше, чем необходимость вложения финансовых средств в освоение новых инженерно-управленческих технологий. Но рано или поздно осознание потребности прозрачности победит (лучше рано – иначе нас сомнут более прозорливые западные и восточные "партнеры"). Однако строительные организации, в отличие от проектировщиков, могут себе позволить меньшими усилиями войти в мир информационного моделирования уже сегодня и получить существенное повышение эффективности своего бизнеса за счет оптимизации организационно-технологических решений и недопущения дополнительных работ и аварийных ситуаций. Но для этого нужна воля и, разумеется, некоторые финансовые средства.

Конференция "Информационное моделирование в строительстве как основа безопасности инвестиций", которая была организована Национальной палатой инженеров в рамках Форума "Технологии безопасности 2018", еще раз показала, что движение в направлении внедрения технологий информационного моделирования идет. А акцент интереса перемещается с проектировщиков в сторону застройщиков и строительных организаций. ■

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

Практика внедрения систем видеоидентификации физических лиц на объектах транспортной инфраструктуры

В данной статье рассмотрим практические аспекты создания систем видеоидентификации физических лиц на объектах транспортной инфраструктуры. Материал основан на опыте ряда проектов в различных городах России

Олег Майданский
Руководитель направления интеллектуальных городских систем компании "КРОК"

Рис. 1. Система видеоидентификации физических лиц – это целый комплекс технологий

Ключевые вопросы практической реализации проектов по видеоидентификации можно разделить на следующие категории:

1. Предубеждения заказчика.
2. Последствия самостоятельных попыток создания систем без интегратора.
3. Очевидные сложности технического характера.
4. Неочевидные сложности технического характера.
5. Вопросы развития созданной системы.

Работа с предубеждениями

Одно из главных достижений на сегодня – тот факт, что заказчики в принципе верят в работоспособность систем биометрической идентификации. Еще два года назад многие говорили: "Это действует только в "тепличных" условиях, либо в лаборатории с идеальным освещением и тщательно выверенными углами установки камер". Мы довольно быстро пришли к выводу, что эффективнее всего провести "боевую" демонстрацию системы на объекте или все таки в лаборатории, но в условиях, приближенных к реальным. Это сразу снимает все предрассудки и сомнения.

В нашей лаборатории в настоящее время собраны пять различных решений, способных доказать эффективность видеоидентификации. К счастью, все меньше и меньше остается людей, которые не знают слово "биометрия" или не воспринимают всерьез возможности видеоидентификации физических лиц.

Постановка задач

Первый вариант постановки задачи от заказчика зачастую звучит лаконично: "Хотим систему распознавания лиц. Давайте работать". В процессе работы формулировка обрастает необходимыми условиями: "Хотим систему биометрической видеоидентификации физических лиц на крупном объекте транспортной инфраструктуры, АРМ для сотрудников нескольких силовых ведомств с различающимися функциями, но система должна удовлетворять и тех, и других". Это уже картина реальной системы, в которой уже можно увидеть реальные условия и ограничения. Если пропустить их на старте проекта, то до успешного завершения проект можно и не довести.

Старт проекта без интегратора

Если заказчик пытается внедрить систему видеоидентификации самостоятельно, скорее всего, он не задается такими вопросами:

- Какая инфраструктура обеспечит бесперебойную работу системы с требуемой производительностью?
- Как вписать создаваемую систему в существующий ИТ-ландшафт организации?
- Какие компоненты должны входить в систему и как и на чем их развернуть?

Система видеоидентификации физических лиц, как правило, не существует в автономном контуре. Ее приходится вписывать в существующие инфраструктурные и ИТ-системы заказчика, причем на этом этапе очень легко выйти далеко за пределы бюджета – без каких-либо гарантий приемлемого результата. Система, эффективность которой не превышает 10–20% от расчетных значений из-за конфликтов или ограничений с существующей ИТ-инфраструктурой – суровая быль проектной жизни.

Информационная безопасность

Некоторым заказчикам неочевидно, что необходимо защищать и саму систему, и данные, которые в ней обрабатываются, хотя в этой части действует целый комплекс норм и стандартов соответствующих регуляторов. У нас есть опыт, когда приходилось сообщать об этом заказчику, который уже сформировал бюджет самостоятельно, попросту упустив этот момент. Пришлось учесть эти дополнительные затраты – иначе систему просто не допустили бы к эксплуатации.

Телеком

Ошибки при расчете характеристик каналов связи и телеком-инфраструктуры способны свести к минимуму эффективность системы видеоидентификации. Чтобы не было задержек и "зависаний" при передаче информации, чтобы камеры срабатывали своевременно и система обеспечивала заявленную вендором производительность (например, одна секунда на распознавание), очень важно правильно рассчитать требования к каналам связи. Это несложная операция, но почему-то на данном этапе происходит колоссальное количество ошибок.

В итоге у большинства заказчиков не хватает ни рук, ни экспертизы, чтобы грамотно решить эти вопросы. Системный интегратор, как правило, уже "пробежал по всем этим граблям" и имеет достаточный опыт, чтобы обеспечить максимальную отдачу от проектных инвестиций.

Состав инфраструктуры

Казалось бы, система видеоидентификации физических лиц – это видеокамеры с функцией распознавания. На деле это целый комплекс технологий (и соответствующих подсистем), каждая из которых решает свою задачу. Недостаточное внимание хотя бы к одной из компонент решения – и система так и останется недоделанной.

Системы виртуализации

Позволяют уменьшить требования к серверному оборудованию и существенно уменьшить капитальные инвестиции. Обязательный пункт при создании высоконагруженных решений, к которым относится и видеоидентификация.

Ориентирование на местности

Каждый объект имеет индивидуальный набор характеристик и ограничений, игнорирование которых приведет к провалу проекта.

Расположение камер

Это один из ключевых моментов, от которого зависит достижение заявленных показателей распознавания. Заказчик, как правило, полагает, что достаточно хорошо знает свой объект, чтобы идеально расположить камеры. В нашей практике было уже несколько случаев перепроектирования решений после того, как мы на практике показали, почему камеры нельзя ставить там, где "в глаза не бросится". Важнейшая задача безопасности – это полный контроль лиц, которые прибывают на объект транспортной инфраструктуры и убывают с него. Расположение камер и технических средств должно быть подобрано таким образом, чтобы перекрыть все возможные точки входа и выхода, учитывая потоки движения пассажиров. Смысл в системе мгновенно теряется, если существует коридор или дверь, в которую человек может войти/выйти, не будучи распознанным. В оптимальном случае рекомендации вендора и интегратора должны учитываться еще на стадии предпроектного обследования, и на конкретном объекте транспортной инфраструктуры это должен быть самый первый шаг.

Освещение

В половине случаев на рубежах контроля мы столкнулись с недостатком освещенности. Собственники объектов транспортной инфраструктуры всегда следовали нашим советам. Иногда в местах установки камер приходилось усиливать уже имеющиеся лампы, где-то мы монтировали новые светильники. Эти детали крайне желательно выявить при предпроектном обследовании, чтобы заранее закладывать в перечень проектных работ.

Сезонный фактор

Летом и зимой солнце движется по-разному – это напрямую влияет на эффективность системы. Если объект сдается в осенне-зимний период, летом на входных группах с большими окнами велика вероятность получить существенную засветку. Заказчик скажет, что камеры не работают – а нужно было заранее узнать/спрогнозировать, как меняется освещенность с учетом смены времен года, либо заранее предупредить заказчика об этом явлении и отдельно проконтролировать работу системы в момент смены времен года.

Скорость реакции – залог успеха

Рассмотрим самые "живые" вопросы, с которыми мы сталкиваемся почти на всех объектах.

Крепление камер

Стандартные крепежи камер, даже самых продвинутых, могут не подойти в некоторых случаях. Практически всегда мы используем доработанные авторские решения, чтобы камеры не дребезжали, не расшатывались со временем и, если их случайно заденут, их сдвиг был незначительным или вообще отсутствовал. Промышленно выпускаемых крепежей, удовлетворяющих данным условиям, мы, к сожалению, пока не встречали.

"Подарки от средств ИБ"

Не раз и не два выяснялось, что доступная к использованию версия средств информационной безопасности еще не прошла сертификацию регулятора. Начинается кропотливая работа интегратора и поставщика ПО – либо ускорить сертификацию, либо сделать "даунгрейд" до той версии, которая сертифицирована. С организационной точки зрения это довольно сложный этап, на котором необходимо добиться, чтобы в системе не оказалось несертифицированных элементов.

Рис. 2. Видеоидентификация физических лиц на транспорте является отличным подспорьем для силовых ведомств

Вандалоустойчивость

До сих пор встречаются люди, которые будут пытаться сбить, покорежить, сломать камеры. Если камеры установлены в переходе или в инженерном сооружении с недостаточным контролем движения пассажиров, это произойдет скорее раньше, чем позже. Необходимо использовать соответствующие вандалоустойчивые кожухи. Однако буквально единицы имеющихся в продаже промышленных антивандальных кожухов применимы на объектах, где развертываются системы видеоидентификации. Нам приходилось заказывать такие кожухи в спецмастерских.

Эстетика

Несколько раз уже практически на сдаче системы мы получали замечания, что камеры "пугают своим видом/размерами". КРОК – ответственная компания, поэтому мы подбирали минимальные по размерам и максимально аккуратные кожухи, в которые можно упаковать камеры с теми объективами, которые подходят для данной локации и данного рубежа охраны.

Ремонт на объекте

В 30% случаев, когда план работ согласован, все проектные чертежи разработаны, деятельность кипит и до сдачи проекта остаются считанные дни, на объекте вдруг начинается ремонт. Здесь нет универсальных рекомендаций по реагированию на это событие. Естественно, приходится договариваться с ремонтными организациями, выяснять что именно и как они будут изменять на объекте, согласовывать взаимные действия. Сейчас, научившись на первых подобных случаях, мы заранее проговариваем с собственниками объектов их планы по ремонту.

Что делать после того, как система внедрена?

Итак, все работает, как нужно, сотрудники силовых ведомств довольны, объект транспортной инфраструктуры защищен. Что будет происходить дальше?

1. Скорее всего, сотрудники силовых ведомств с течением времени захотят расширения системы, потому что видеоидентификация оказывается отличным подспорьем для решения их задач.
2. Камеры будут задевать. Вибрации несущих конструкций в ряде случаев неизбежны. В результате возможна расфокусировка камер, о чем надо заранее предупреждать заказчика.
3. Сеть будет падать, особенно на территориально распределенных площадках. Здесь нет вины провайдера, оператора или интегратора – просто системы периодически сбоят, а поставщики телеком-услуг вынуждены периодически отключать/перезапускать свое оборудование. Об этом надо помнить на переговорах с провайдером – собрать контакты, обсудить вопросы связнности, организовать подписание регламента между провайдером и заказчиком о том, что работы, которые затрагивают сегменты сетей и связаны с функционированием территориально разнесенных площадок, следует в обязательном порядке согласовывать с владельцем системы.
4. Инфраструктурное ПО тоже может периодически отказывать, как по "классическим" причинам (проходила уборщица и шваброй выдернула шнур сервера), так и по сложно диагностируемым, когда при очередном обновлении операционной системы средства ИБ вдруг перегружают каналы связи. Неспециалисту в этих ситуациях разобраться очень непросто.

Вывод один: либо заказчик готов развивать свою компетенцию и поддерживать работоспособность системы самостоятельно, либо ему нужно заранее думать об услуге технической поддержки со стороны специализированной организации. По нашему опыту, без отлаженного процесса эксплуатации и технической поддержки работоспособность комплексной системы, пусть даже идеально внедренной, неизбежно начнет деградировать уже после первого года такой бесконтрольной эксплуатации. ■

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

Видеоидентификация: новые возможности для транспорта и спорта

В России и во всем мире активно развивается применение биометрических технологий для видеоидентификации в сферах транспорта и спорта, причем Россия является одним из мировых лидеров по внедрению таких решений. Какие новые возможности привнесут эти технологии на транспортные и спортивные объекты?

Андрей Хрулев
Директор по специальным проектам группы компаний "ЦРТ"

Транспорт сегодня – один из ключевых потребителей технологий биометрической видеоидентификации, и если проанализировать мировой опыт применения биометрических технологий в этой области, можно выделить несколько основных сценариев и кейсов применения.

Обеспечение безопасности на транспорте

В разных странах существуют свои нормативные акты в данном направлении. В России это целая серия документов, в частности постановление Правительства РФ № 969, в рамках которого субъекты транспортной инфраструктуры на определенных категориях транспортных объектов должны внедрять технологии видеоидентификации с целью обеспечения транспортной безопасности. Конечными потребителями таких решений являются полиция, силовые структуры и службы безопасности.

Автоматизация регистрации пассажиров и проверка личности при выходе на посадку

Это кейс, который в последние два года очень активно применяется в мире, а в России идет его активное обсуждение. Серьезным стимулом к реальному практическому внедрению видеоидентификации на объектах транспорта стал недавний приказ Минтранса, по которому электронный посадочный талон был полностью приравнен к печатному. Логично: если посадочный талон электронный и его не обязательно распечатывать, то почему бы не поднимать его из базы по предъявленной биометрической характеристике? В связи с этим в мире развивается концепция "биометрических тоннелей", по которым пассажир проходит через аэропорт к самолету. Например, пассажир предъявляет паспорт на автоматических стойках регистрации и выхода на посадку, а по изображению его лица тут же подтягивается электронный посадочный талон (штрих-код не надо искать в телефоне и показывать) и вся необходимая информация о его билете. Заодно система проверяет, что перед ней именно владелец билета. Тем самым мы исключаем неприятные инциденты – например, не так давно у одной уважаемой авиакомпании пассажир улетел из Лос-Анджелеса вовсе без билета. Применение биометрии позволяет исключить такие ситуации и полностью гарантировать, что пассажир сможет оперативно сесть на тот борт, на который он купил билет.

Автоматический паспортный контроль

За рубежом системы автоматического паспортного контроля используются достаточно активно: в мире уже более 2 тыс. внедрений таких систем. К сожалению, в России пока нет ни одного подобного объекта, но мы надеемся, что в ближайшие год-два это изменится. Ведь утомительную процедуру паспортного контроля на международные рейсы, на которые нужно было прибывать за 2–3 часа, благодаря автоматизации пассажир может пройти фактически за пару минут, просто "предъявив" свое лицо и паспорт системе. При этом обеспечены и безопасность, и комфорт пассажира.

Процедура паспортного контроля в России сейчас проходит следующим образом: пассажир стоит перед пограничником, дает свой паспорт, и по нормативу максимум за две минуты (а по факту – гораздо больше) пограничник должен осуществить проверку паспорта по всем необходимым базам данных, а также сверить лицо пассажира с фото в документе. Это делается очень быстро, сумбурно и далеко не всегда качественно, потому что провести тщательную проверку в течение одной-двух минут невозможно.

С внедрением информационных систем, в том числе содержащих биометрические технологии, проверка делается заблаговременно: выгружаются данные из информационных систем авиакомпании, пассажир проверяется за 2–4 часа до отправления рейса. А когда он приедет в аэропорт, единственное, что нужно будет сделать, – удостовериться в том, что это именно тот пассажир, который прошел проверку. На этот вопрос отвечает биометрическая система, которая таким образом повышает и безопасность в аэропорту, и скорость прохождения паспортного контроля. Во всем мире этот сценарий, который гарантирует возможность быстрого прохода всех аэропортных формальностей не за два часа, а за несколько минут, принято называть Fast Track.

Практическая реализация

На российском рынке предлагаются системы, которые обеспечивают функционал видеоидентификации, решая вопросы безопасности в местах массового скопления людей.

Как они работают? Традиционно система начинается с "глаз", и этими "глазами" является камера. Они устанавливаются в местах структурированного потока людей. Если мы говорим о распознавании по лицу, то оно произойдет только в том случае, если лицо попало в кадр. Камеры располагаются у кромки металлодетектора, турникета, коридора – везде, где поток людей относительно структурирован. Когда человек попадает в поле зрения камеры, система производит цикл математических обработок, в ходе которого из видеопотока извлекается изображение лица, затем кодируется в биометрический шаблон, содержащий уникальные характеристики лица. Эти биометрические шаблоны в последующем сопоставляются с данными, которые хранятся в базах, например спис-

Рис. 1. Биометрия на транспорте

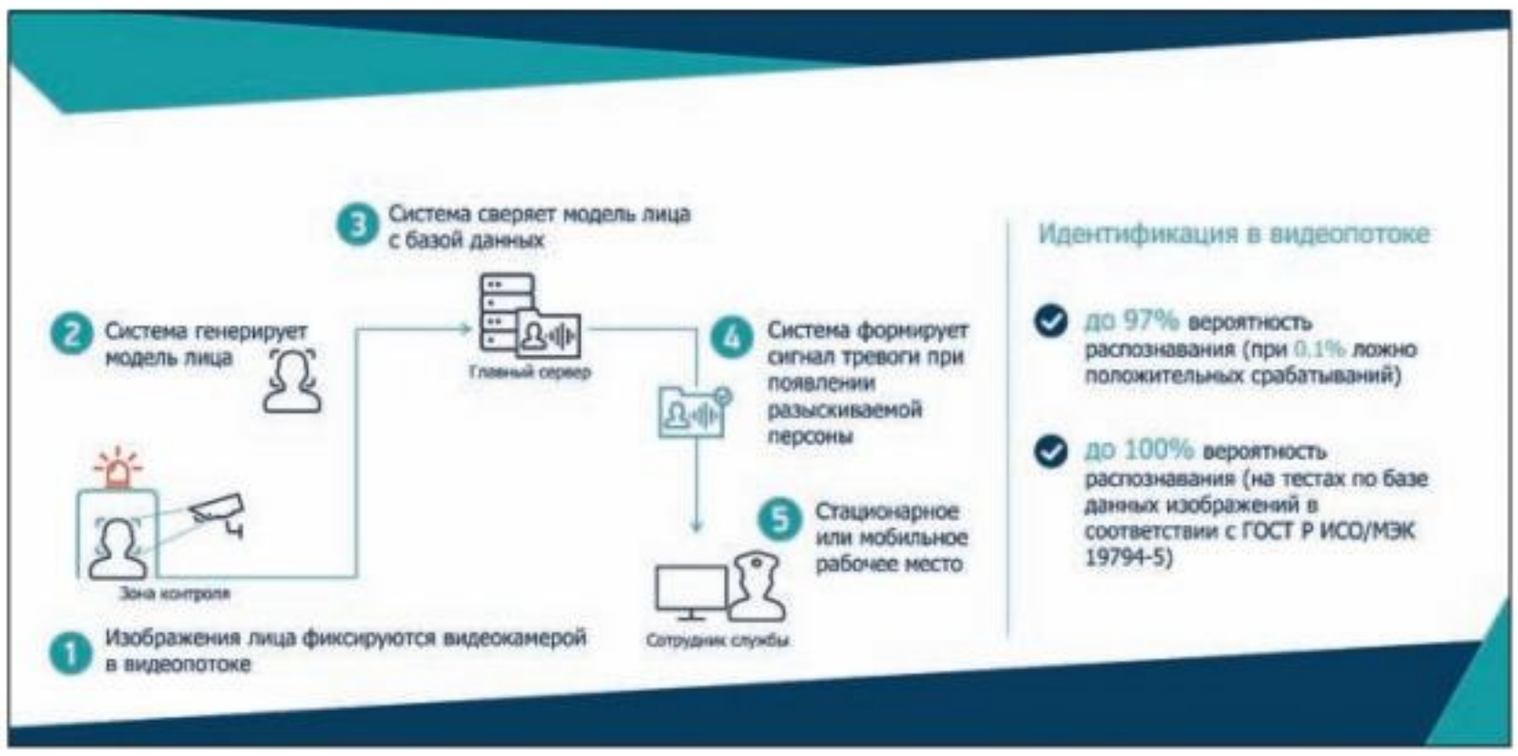


Рис. 2. Видеоидентификация по лицу. Принцип работы

ках розыска. По результатам проверки принимается решение о необходимости информирования заинтересованных служб по каждому конкретному пассажиру.

К примеру, в аэропорту в досмотровой зоне видеокамера смотрит непосредственно на рамку металлодетектора и в поле зрения камеры попадают пассажиры, которые прибывают в аэропорт с улицы либо со стороны прибывшего воздушного судна. Таким образом решается вопрос идентификации всех гостей аэропорта.

Нормативная база

В России уже достаточно подробно проработана нормативная база по биометрическим системам, начиная от федеральных законов и заканчивая конкретными постановлениями правительства, которые регламентируют все вплоть до конкретных функциональных характеристик. С какой вероятностью необходимо идентифицировать пассажира, какие допустимы ошибки, кто является функциональным потребителем, по каким протоколам необходимо осуществлять взаимодействие, – все эти вопросы за прошедшие годы были очень подробно рассмотрены. В целом сейчас можно говорить о том, что нормативная база подготовлена и внедрение биометрических технологий в вопросах безопасности выполняется полностью на легальной основе.

Обеспечение безопасности на спортивных объектах

Вопрос видеоидентификации на спортивных объектах в России проработан лучше, чем в других странах. Возможно, это связано с особенностями российских болельщиков – одних из самых рьяных фанатов в мире. Поэтому внедрение на стадионах решений видеоидентификации – это как раз тот самый случай, когда биометрия применяется для решения конкретных задач, которые стоят перед футбольным клубом.

1. Прежде всего футбольный клуб должен не допустить проход на стадион болельщиков, имеющих запрет на посещение спортивных мероприятий. Мы знаем, что в России действует Федеральный закон № 78-ФЗ (в народе – "закон о болельщиках"), согласно ему введено понятие списка лиц, которым по решению суда запрещено посещение спортивных мероприятий (хулиганов). То есть фанаты, совершившие очень серьезное правонарушение, за которое не отделаться обычным штрафом, включаются в федеральный реестр хулиганов и на определенный срок им запрещено посещать спортивные мероприятия по всей России. В этом случае биометрическая система как раз позволяет решить данный вопрос: даже если такой человек каким-то образом раздобудет билет, он все равно не сможет попасть на стадион, потому что его лицо находится в соответствующем черном списке.

2. Для многих клубов актуальна проблема передачи абонементов. Существуют фанатские программы с абонементами, по которым болельщик может попасть на любой матч по специальным тарифам. Разумеется, клубу не выгодно, если абонемент попадет в руки перекупщиков, которые будут по своим ценам пускать в клуб других болельщиков.

Здесь биометрия тоже может прийти на помощь. Даже если человек не включен в черный список болельщиков, но пользуется не своим персональным абонементом (с июня 2016 г. действует новая редакция ФЗ о болельщиках, в соответствии с которой организатор спортивных мероприятий имеет право продавать персональные билеты по паспорту), то во время верификации система определяет, что перед ней не владелец абонемента, и турникет не открывается.

3. Самый главный эффект, которого позволило достичь внедрение биометрии, – воспитательный. Другими словами – неотвратимость несения ответственности. Если человек не очень сильно проштрафился на стадионе, вместо того чтобы включить его в федеральный черный список, его заносят в так называемый серый список клуба. Если в следующий раз он придет на матч, система сигнализирует о том, что он находится в этом "сером списке", и стюард сделает ему предупреждение, что при повторном нарушении правил он попадет в черный список. Эта воспитательная мера действует достаточно серьезно и позволяет клубам радикально снижать количество правонарушений. Кроме того, если Российская футбольная Премьер-Лига или Российский футбольный союз признают, что правонарушение серьезное и связано с недостаточным обеспечением безопасности, которое обязан обеспечить клуб, то на клуб налагаются большие штрафы – от нескольких сотен тысяч до нескольких миллионов рублей. Самый большой штраф на сегодняшний день – 4 млн рублей, что сопоставимо со стоимостью внедрения самой системы.

Таким образом, внедрение комплексов видеоидентификации на стадионе позволяет снижать количество штрафных выплат, и по факту на футбольных объектах данные системы часто окупают себя за 1–2 футбольных сезона – за счет сокращения штрафов и монетизации абонементов.

Проверка по черному списку

На сегодняшний день черный список администрируется Министерством внутренних дел и высылается каждому стадиону в отдельности. Идет процесс создания системы видеоидентификации Российской футбольной Премьер-Лиги, в рамках которой будет разработана так называемая карта болельщика, и эта база данных станет единой. В нее также войдет подсистема биометрической идентификации – болельщик, вступая в ряды фанатов и получая карту болельщика, предоставляет свои биометрические данные, которые используются для того, чтобы его "привязать" к конкретному абонементу. Так, карта болельщика является персонализированной – только он имеет право ей пользоваться. И в случае, если он проштрафился, его карта и его лицо попадают в тот самый черный список и некоторое время он не сможет посещать спортивные мероприятия. Соответственно, проштрафившись на одном стадионе, болельщик может быть уверен, что на другой стадион, где есть подобная система видеоидентификации, его не пустят.

Интеграция с билетно-кассовыми системами

Система осуществляет сбор картотеки зрителей для проведения юридических расследований и последующей идентификации.

Каждый человек, который входит на стадион, даже если он добропорядочный болельщик, на время проведения матча попадает в базу данных. Его фотография привязана к конкретному билету (с указанием трибуны, сектора и места). Если во время матча происходит некий инцидент на определенном месте чаши стадиона, то служба безопасности имеет возможность мгновенно получить фотографии (просто указав на карте, где произошел инцидент) и информацию о людях, которые сидят в данной зоне. Эти данные будут использованы для того, чтобы опросить свидетелей, присутствовавших непосредственно на месте возникновения инцидента, и установить виновного.

Этот инструментарий позволяет клубам эффективно находить конкретных виновных, существуют реальные юридические прецеденты, когда клуб, используя такую информацию в суде, переносил ответственность с юридического лица (с себя), на конкретное физическое лицо – нарушителя, который платил штраф и оказывался в черном списке. Клуб в этом случае не платил штраф, что говорит о возможностях окупаемости системы.

Рис. 3. Видеоидентификация на стадионе

Опыт реализации на стадионах

Конструктивно система может быть выполнена в разных вариантах – с полноростовыми или полуростовыми турникетами либо вообще без турникетов, с разными конструктивными особенностями. Например, в одном из южных регионов при внедрении решения просили ни в коем случае не блокировать турникет (в связи с агрессивным нравом болельщиков) – там при обнаружении человека из черного списка просто загоралась красная лампочка, и человека отводили из толпы в сторону.

На большинстве стадионов работает сценарий, который реализован в казанском ледовом дворце "Татнефть Арена". Считыватель установлен непосредственно на турникет и обеспечивает возможность контроля билета по штрихкоду, QR-коду или RFID-метке с одновременной видеофиксацией лица.

Очень важный вопрос, который приходится решать в самом начале внедрения системы, – это скорость идентификации. Биометрия – технология достаточно ресурсоемкая, и так или иначе с момента появления человека в кадре до принятия решения проходит определенное время. Если использовать классический подход (сначала считывается билет, поднимается информация о человеке, фиксируется лицо и проверяется по базе данных), то это добавляет 2–3 секунды к процедуре проверки. Но 2–3 секунды, помноженные на количество болельщиков (на крупных аренах и стадионах их от 10 до 50–80 тыс.), превращаются в очень существенную цифру. Чтобы этого избежать, был применен опыт работы на транспорте: каждый болельщик идентифицируется еще до того момента, как он отсканировал билет. Камера его уже видит, она его уже идентифицирует, а когда он подносит свой билет, происходит просто уточнение информации по билету, и турникет мгновенно открывается. То есть никаких задержек, связанных с внедрением биометрических технологий, дополнительно не возникает. Это позволяет очень эффективно использовать их для быстрого прохода болельщиков на стадион.

Вопросы защиты базы данных

В ФЗ-152, который регулирует область использования персональных данных, есть особая статья, которая говорит о том, что в случаях, связанных с вопросами обеспечения государственной безопасности в интересах правоохранительных органов, согласие на персональную обработку таких данных от субъекта не требуется. Мы рассматриваем как раз такой случай. Вопросы транспортной безопасности и безопасности массовых мероприятий подразумевают, что МВД может не спрашивать согласия на обработку персональных данных. Транспортная и спортивная безопасность являются элементами общественной безопасности, и если болельщик является добропорядочным гражданином и его нет в черном списке или в списке розыска, то никакие его данные в этих системах не хранятся. А данные видеонаблюдения, если человек просто попал в поле зрения камеры, персонализированной информацией не являются.

Однако данные надо защищать, с согласия они были получены или без него. Поэтому в системе предусмотрено безопасное локальное хранение информации, а также механизмы разграничения уровней доступа для пользователей системы. Эти вопросы решаются в обязательном порядке применительно к конкретным внедрениям и в зависимости от того, какие сценарии используются.

Получение данных по иностранным болельщикам

Предстоящий ЧМ по футболу будет проходить не в рамках российского законодательства – и отдельным постановлением правительства стадионы выведены из поля действия российской юрисдикции и подчинены международным правилам, в частности FIFA. На сегодняшний день FIFA не требует проведения биометрической идентификации, в отличие от российских лиг (Российский футбольный союз, Российская футбольная Премьер-Лига, Континентальная Хоккейная Лига). Поэтому в рамках ЧМ по футболу биометрическая идентификация выполняться не будет. Будут применены классические способы – на основании карты болельщика, которая выдается в авторизированных центрах с соответствующей проверкой, и вопроса получения данных по иностранным болельщикам не возникнет. По завершении ЧМ все стадионы, которые в нем участвуют, снова подпадут под российскую юрисдикцию и на них будет применяться современный подход к идентификации.

Корреляция видеоидентификации и безопасности

Обеспечение спортивной безопасности – это чрезвычайно емкий вопрос, который учитывает не только идентификацию. В нем задействованы и досмотр при проходе, и эффективная работа клуба со своими болельщиками. В данном случае биометрия является одним из инструментов. Понимание со стороны болельщика, что он находится под определенным контролем и в случае, если он совершит определенное правонарушение, его личность будет раскрыта и это может быть использовано в последующем для того, чтобы ограничить его проход на стадион, создает воспитательный эффект. Сам факт наличия этой системы (в последующем применении всего комплекса мер) приводит к положительной динамике.

Вопросы внедрения транспортной и спортивной безопасности активно обсуждаются по линиям и МВД, и администраций городов. Появляются определенные регламенты, дополняется нормативная база. И очевидно, что в России идет тот же процесс, что и во всем мире. Мы уверены, что когда такая база будет окончательно сформирована, а биометрические системы будут обязательно устанавливаться повсюду, мы получим положительную динамику в сфере безопасности на транспортных и спортивных объектах. ■

Рис. 4. Видеоидентификация в аэропорту

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

Сертификация систем обеспечения транспортной безопасности: актуальная ситуация на рынке

В связи с усилением угроз и актов со стороны международного терроризма становится все более актуальной задача защиты объектов транспортной инфраструктуры (железнодорожных и автовокзалов, аэропортов), являющихся одними из самых распространенных мест массового скопления людей. В 2018 г. в Российской Федерации будет проведен чемпионат мира по футболу FIFA. Это событие, несомненно, приведет к резкому увеличению пассажиропотока. Учитывая сложившиеся условия, особенно остро встала необходимость оснащения транспортных узлов качественными техническими средствами безопасности

Андрей Зотов
Инженер ЗАО НВП "Болид"

Правительство Российской Федерации приняло постановление № 969 от 26 сентября 2016 г., утвердившее требования к функциональным свойствам технических средств обеспечения транспортной безопасности и правила их обязательной сертификации.

Классификация оборудования

Согласно постановлению, средства обеспечения транспортной безопасности были скомпонованы по назначению, образовав 10 направлений:

1. Технические системы и средства сигнализации.
2. Технические системы и средства контроля доступа.
3. Технические системы и средства досмотра.
4. Технические средства видеонаблюдения.
5. Технические системы и средства интеллектуального видеонаблюдения.
6. Технические системы и средства видеозаписи.
7. Технические системы и средства аудиозаписи.
8. Технические средства связи, приема и передачи информации.
9. Технические средства оповещения.
10. Технические системы сбора и обработки информации.

Для каждого типа оборудования существует своя форма сертификата соответствия и должны проводиться отдельные испытания.

Уровни контроля и управления

Помимо независимых друг от друга решений, предусмотрен "верхний" уровень контроля – система сбора результатов технического мониторинга. При этом почти для каждой из систем прописаны требования обеспечения:

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

Таким образом, станет возможно оперативно передавать информацию о происшествиях на различных объектах в единый центр управления, что должно увеличить скорость реагирования соответствующих служб обеспечения безопасности.

Обязательная сертификция

После вступления в силу постановления № 969 любая организация, производящая технические средства безопасности для использования на объектах транспорта, обязана получить сертификат соответствия, а любые решения по безопасности объектов транспортной инфраструктуры должны реализовываться с применением только сертифицированных систем и средств. Что касается объектов транспорта с уже установленными техническими решениями безопасности, то они могут столкнуться с обязательностью процедуры проверки на соответствие требованиям постановления № 969 и получить сертификат по схеме № 4. Очевидно, что таких объектов не один и не два, а сотни.

В нашей стране существует большое количество отечественных разработок в области безопасности – от отдельных датчиков до интегрированных систем охраны, объединяющих в себе охранную сигнализацию, контроль доступа, видеонаблюдение и др. Например, в крупнейшей в России выставке по теме безопасности Securika/MIPS-2017 участвовали более 100 отечественных компаний-производителей, каждая из которых, несомненно, желает получить сертификаты соответствия своей продукции требованиям транспортной безопасности и тем самым открыть для себя новый рынок сбыта.

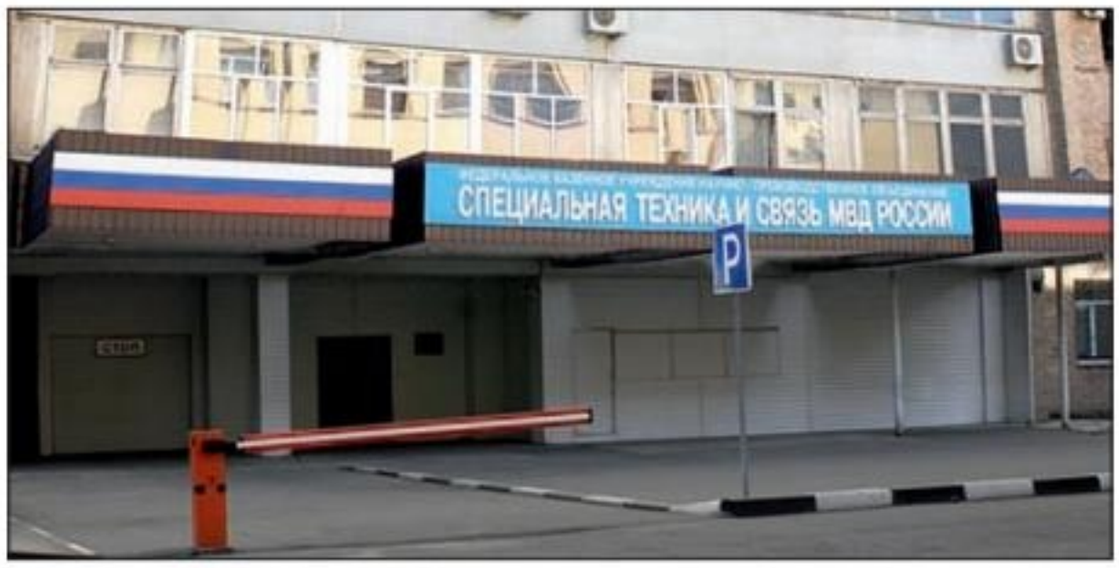
19 организаций – производителей охранных систем получили сертификаты соответствия на свои изделия. В числе первых были компании ООО "Трансте-лесофт", ЗАО "Интегра-С", ЗАО "ЮМИРС", ООО "ВЛИБОР Системс", ЗАО НВП "Болид"

Рост количества заявок

Как известно, органом по сертификации охранных систем определено ФКУ НПО "СТиС" МВД России, имеющее аккредитованную лабораторию на проведение испытаний. В связи с большим количеством ведомственных объектов на них буквально навалился огромный фронт работ: на данный момент подано 176 заявок на сертификацию. Несмотря на это, уже сегодня 19 организаций – производителей охранных систем получили сертификаты соответствия на свои изделия. В числе первых были компании ООО "Трансте-лесофт", ЗАО "Интегра-С", ЗАО "ЮМИРС", ООО "ВЛИБОР Системс", ЗАО НВП "Болид". По информации компании "Болид", к ним почти ежедневно поступают запросы со стороны руководителей объектов транспорта о планах по проведению сертификации, так как ее продукция либо уже установлена и эксплуатируется на многочисленных объектах транспорта различного назначения и ведомственной принадлежности, либо планируется к применению на строящихся объектах.

Две стороны одной медали

Многие производители задаются вопросом о необходимости и целесообразности вмененной сертификации. Ведь, с одной стороны, это значительная по затратам процедура, которая может повлиять на повышение стоимости продукции и, как следствие, на величину расходов по оснащению объектов. С другой стороны, сертификационные требования, как правило, не приводят к необходимости совершенствования качественных параметров серийно выпускаемых изделий, то есть их эффективность никак не изменилась. Какой будет эффект от данной кампании – покажет время. ■



Органом по сертификации охранных систем определено ФКУ НПО "СТиС" МВД России, имеющее аккредитованную лабораторию на проведение испытаний

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

Безопасность и автоматизация

Биометрия по венам ладони + контроль отсутствия алкогольного опьянения

BioSmart PV-WTC – это надежное интеграционное решение биометрической идентификации пользователя с последующей экспресс-проверкой содержания паров алкоголя в выдыхаемом им воздухе. Наличие многократной, в течение рабочего дня, экспресс-диагностики персонала на отсутствие признаков алкогольного опьянения уменьшает вероятность возникновения нештатной ситуации, повышается производительность труда, уменьшается производственный травматизм.

Производитель: "Прософт-Биометрикс"

Автоматизация оплаты проезда

Оптимизация сбора оплаты проезда, а именно применение транспортных турникетов в составе систем платного доступа, позволяет сократить количество безбилетников. Турникет-трипод PERCo-TTR-10A, выполненный из нержавеющей стали, соответствует всем современным требованиям, предъявляемым к преграждающему устройству для транспорта: компактность, комфортность прохода, надежность, вандалозащищенность и виброустойчивость.

Производитель: PERCo

Видеонаблюдение в крайне суровых погодных условиях

Сетевая камера WV-SUD638 AeroPTZ гарантирует высокую надежность в сложных погодных условиях, устойчивость к реагентам и соляному ветру. Встроенные стеклоочиститель и антиобледенитель позволяют вести наблюдение на объектах транспортной инфраструктуры в любую погоду. Камера соответствует стандартам IP67, IP66, IK10 и благодаря специальному покрытию корпуса не подвержена коррозии.

Производитель: Panasonic

Автоматическое принятие решений высокой степени сложности

Комплекс безопасности реального времени АПК "Феникс" (Kedacom) со встроенным искусственным интеллектом и носимыми регистраторами позволяет "проникать" в каждый уголок объекта и дает системе значительно больший информационный поток, необходимый для принятия решения. Оценка ситуации на объекте, распознавание лиц и предметов, методики поведения каждого объекта в зоне видимости выполняются системой автоматически.

Производитель: Kedacom Technology
Представляет: ООО "Видеоконтроль"

на объектах транспорта

Анализ дорожно-транспортной ситуации

Камера DHI-ITC231-RU1A – это проверенное решение для управления загрузкой дорог, сокращения нарушений ПДД, аварий и жертв. Обеспечивает снижение времени на реагирование при изменении транспортной ситуации, особенно в городах с высокой плотностью городского потока, предоставляя точные статистические данные (время, дата, период сбора статистики, полоса движения, трафик, нагрузка, средняя скорость прохождения, длина очереди).

Производитель: Dahua Technology

Видеонаблюдение на пассажирском транспорте

Виброзащищенная камера Apix-FishEye/E6 ICM Industrial с малой высотой и углом обзора 360 град. имеет хорошую защиту от вибрации, перепада температур и запыленности. Металлический корпус, соответствующий степени IP54, надежно защищает камеру от повреждений и исключает попадание брызг и стекающей воды внутрь. Предназначена для применения в вагонах метро, электропоездах и на автотранспорте.

Производитель: EVIDENCE
Представляет: ООО "СТА"

Технологии самообучающейся видеоаналитики

Инновационная система видеонаблюдения от AVIGILON сокращает время реагирования на происшествия и расширяет возможности их расследования. Avigilon Appearance Search – это новаторская поисковая система с использованием искусственного интеллекта и глубокого обучения, которая обрабатывает многие часы отснятых видеоматериалов, позволяя оперативно найти нужного человека или транспортное средство на всей территории объекта.

Производитель: AVIGILON
Представляет: компания "АРМО-Системы"

Универсальное ПО для видеонаблюдения на транспорте

ПО TRASSIR обеспечивает видеонаблюдение, интеллектуальное видеонаблюдение, видеозапись и аудиозапись и соответствует требованиям транспортной безопасности РФ. Работает как в составе линейки видеорегистраторов TRASSIR, так и на собственном сервере или виртуальной машине. Позволяет эффективно модернизировать уже существующие и морально устаревшие аналоговые системы видеонаблюдения до уровня, отвечающего современным требованиям транспортной безопасности.

Производитель: DSSL

Видеокамера как автономная система контроля доступа

IP-камера B2230L с встроенной системой распознавания автономеров является оптимальным решением для обеспечения доступа автомобиля на охраняемую или частную территорию. Не нужно приобретать дополнительное ПО, серверы или лицензию – все необходимое уже присутствует в модели. Решение BEWARD с точностью до 98% распознает автомобильные номера СНГ, двух- и трехзначных регионов.

Производитель: НПП "Бевард"

СПЕЦПРОЕКТ ТРАНСПОРТ

BioSmart PV-WTC – биометрическая идентификация по венам ладони и экспресс-диагностика на алкогольное опьянение

Представляет компания "Прософт-Биометрикс"

PROSOFT BIOMETRICS

BIOSMART®

Ключевые преимущества

Надежное интеграционное решение биометрической идентификации пользователя с последующей экспресс-проверкой содержания паров алкоголя в выдыхаемом им воздухе.

В русле трендов

Обязательное медицинское освидетельствование проходят сотрудники определенных категорий профессий за 1 час или за 30 минут до начала смены. Например, экипажи воздушных судов, бригады пассажирских поездов, водители автотранспортных средств, диспетчеры организации воздушного и железнодорожного движения и метрополитена, работники аэропортов, выполняющие работы по обслуживанию воздушных судов, аэродромов и авиапассажиров, и многие другие.

Отсутствие подобного контроля в течение рабочего дня (после перерыва на обед, в конце рабочей смены, при выходе на маршрут или перед въездом на территорию аэродрома) не позволяет выявить возможность употребления спиртных напитков в рабочее время.

Наличие оперативной и доступной диагностики во время рабочей смены дает возможность кардинально изменить ситуацию.

Новый подход к решению задач

Регулярная, в течение рабочего дня, экспресс-диагностика на отсутствие признаков алкогольного опьянения уменьшает вероятность возникновения нештатной ситуации. На проведение такой диагностики не требуется дополнительных затрат, а время прохождения процедуры занимает не более 10 секунд.

Сам факт постоянного и повсеместного контроля на отсутствие алкогольного опьянения приводит к повышению самодисциплины сотрудников. Автоматизированные системы не устают, не ошибаются, и с ними невозможно договориться.

Экономическая эффективность

Как правило, большинство аварийных случаев на транспорте возникает по причинам человеческого фактора. С января по ноябрь 2017 г. по вине нетрезвых водителей в России погибли чуть больше 3,8 тыс. человек (в 2016 г. – 4,6 тыс.), еще 22,9 тыс. были ранены (в 2016 г. – 25,7 тыс.).

Наличие многократной, в течение рабочего дня, экспресс-диагностики персонала на отсутствие признаков алкогольного опьянения уменьшает вероятность возникновения нештатной ситуации, повышается производительность труда, уменьшается производственный травматизм.

Исключаются спорные случаи со страховой компанией, когда страховая отказывает в выплате денежной компенсации, ссылаясь на возможное наличие признаков алкогольного опьянения у застрахованного лица. ■

Появление на рынке	2017 г.
Ценовой сегмент	Средний

Потребители

Аэропорты, автомобильный транспорт

Проекты

ПАО "Северсталь", "Деловые линии"

см. стр. 152 "Ньюсмейкеры"

Турникет-трипод для транспорта PERCo-TTR-10A: современные технологии контроля оплаты проезда

Представляет компания PERCo

Появление на рынке	II квартал 2018 г.
Ценовой сегмент	Средний

Ключевые преимущества

Одно из основных преимуществ транспортного турникета PERCo – это наличие привода, который обеспечивает высокую надежность турникета, большой ресурс и комфорт для пассажиров.

В русле трендов

Оптимизация сбора оплаты проезда – важнейшая задача любого транспортного предприятия, осуществляющего пассажирские перевозки.

Турникет PERCo, выполненный из нержавеющей стали, соответствует всем современным требованиям, предъявляемым к преграждающему устройству для транспорта, – компактность, комфортность прохода, надежность, вандалозащищенность и виброустойчивость. Эти характеристики подтверждены испытаниями на ресурс, вибрацию, разрушающими испытаниями.

Безопасность пассажиров обеспечат автоматические планки "Антипаника", позволяющие в экстренной ситуации мгновенно освободить путь к выходу. Турникет может работать в широком диапазоне температур от -40 до +55 °С.

Потребители

Пассажирский транспорт

Новый подход к решению задач

От правильности организации сбора оплаты напрямую зависят доходы транспортных компаний. Автоматизация оплаты проезда, а именно применение транспортных турникетов в составе систем платного доступа, позволяет сократить количество безбилетников. Систему практически невозможно обмануть, исключается не только возможность безбилетного проезда, но и человеческий фактор, когда водитель может взять плату за проезд с пассажира и оставить ее себе, не передавая в бюджет транспортной компании.

Экономическая эффективность

Экономическую эффективность оснащения пассажирского транспорта турникетами можно рассчитать на следующем простом примере. За смену в среднем на одном маршруте перевозится 2500 пассажиров. Статистика показывает, что не менее 15% пассажиров поедут "зайцем", а еще 10% оплаты водитель не положит в кассу. Получается, что при стоимости проезда 40 рублей транспортная компания на одном маршруте за смену недополучит 25 000 рублей. ■

см. стр. 152 "Ньюсмейкеры"

Сетевая камера WV-SUD638 AeroPTZ для крайне суровых погодных условий

Представляет ООО "Панасоник Рус"

Появление на рынке	2017 г.
Ценовой сегмент	Средний

Ключевые преимущества

Высокая надежность в сложных погодных условиях, устойчивость к реагентам и соляному ветру. Система гибридной стабилизации, встроенные стеклоочиститель и антиобледенитель. Работа при ветровой нагрузке до 80 м/с за счет специальной аэродинамической конструкции, которая уменьшает сопротивление воздуха для большей визуальной стабильности.

В русле трендов

Обеспечение беспрерывного видеонаблюдения с высоким качеством изображения, независимого от погодных условий. Долгий срок службы. Защита корпуса камеры от морской коррозии.

Потребители

Морские порты, автодороги, аэропорты, железнодорожный транспорт

Проекты

Порт "Морской фасад"

Новый подход к решению задач

1. Встроенные стеклоочиститель и антиобледенитель позволяют вести наблюдение на объектах транспортной инфраструктуры в любую погоду.
2. Технология SAS стабилизирует изображение, что снижает нагрузку на оператора.
3. Высокое разрешение (Full HD – 1080p, 60 кадр/с) и 30-кратное оптическое увеличение повышают информативность изображений.
4. Адаптивная ИК-подсветка (до 150 м), которая автоматически настраивается в зависимости от угла обзора камеры, позволяет вести наблюдение при отсутствии освещения.
5. Соответствует стандартам IP67, IP66, IK10.

Экономическая эффективность

Снижение стоимости обслуживания. Благодаря специальному покрытию корпуса камера не подвержена коррозии. ■

см. стр. 152 "Ньюсмейкеры"

АПК "Феникс" (Kedacom) – комплекс безопасности реального времени со встроенным искусственным интеллектом

Представляет ООО "Видеоконтроль"

Ключевые преимущества

Искусственный интеллект системы в реальном времени оценивает и анализирует по широкому спектру параметров сигналы от (до) тысяч камер, а также от переносных мобильных видеорегистраторов (в том числе по мобильным каналам связи), предоставляя данные об обстановке на объекте.

В русле трендов

Классические системы безопасности в некоторой степени являются "пассивными", поскольку даже поворотные камеры с трансфокаторными объективами не могут дать полную и детальную информацию по 100% объекта, а существующие системы анализа данных не обладают возможностью нейронного (глубинного) обучения. Решения на основе искусственного интеллекта с носимыми регистраторами позволяют "проникать в каждый уголок объекта" и дают системе значительно больший информационный поток, необходимый для принятия решения.

Появление на рынке	Ноябрь 2017 г.
Ценовой сегмент	Средне-высокий

Потребители

Любые объекты транспортной инфраструктуры

Проекты

- **Ситуационный центр Службы спасения в Южной Корее (аналог МЧС России). Удаленное наблюдение и управление аварийно-спасательными операциями с применением мобильных носимых видеорегистраторов.**
- **Инкассация (провинция Цзянсу, Китай). Наблюдение в реальном времени за машинами инкассации, их передвижением (по карте) и действиями каждого инкассатора.**
- **Школьные автобусы в Дубае, ОАЭ. Наблюдение в реальном времени за автобусами, идентификация лиц.**

Новый подход к решению задач

Все решения высокой степени сложности, включая оценку ситуации на объекте, распознавание лиц и предметов, методики поведения каждого объекта в зоне видимости, выполняются системой автоматически. Носимые регистраторы, передающие видео и аудио в реальном времени, позволяют детализировать любую сцену в любом участке объекта, что значительно ускоряет оперативность действий по поддержанию порядка на объекте и решение текущих штатных и нештатных ситуаций.

Экономическая эффективность

Осенью 2017 г. на VI саммите БРИКС в городе Сямэнь (провинция Фуцзянь, КНР) АПК "Феникс" обрабатывал информацию от более чем 20 000 камер в реальном времени, что позволило получить более 20 млн уникальных идентификационных меток по опознаванию лиц и объектов. Точность распознавания составила более 99%. ■

см. стр. 151 "Ньюсмейкеры"

Сверхчувствительная дорожная камера DHI-ITC231-RU1A

Представляет компания Dahua Technology Rus

Ключевые преимущества

Камера DHI-ITC231-RU1A – это проверенное решение для управления загрузкой дорог, сокращения нарушений ПДД, аварий и жертв:

- точность захвата транспортного средства и его классификация – более 95%;
- скорость распознавания номерного знака составляет более 90% при скорости ниже 80 км/ч;
- захват до трех полос одной камерой.

В русле трендов

- Использование новых алгоритмов анализа информации (Deep Learning).
- Снижение времени на реагирование при изменении транспортной ситуации, особенно в городах с высокой плотностью городского потока.

Новый подход к решению задач

- Широкий диапазон определения типов транспортных средств: легковой автомобиль, грузовики различных типов, микроавтобус, мотоцикл, пешеход.
- Статистические данные по каждой полосе: время, дата, период сбора статистики, полоса движения, трафик, нагрузка, средняя скорость прохождения, длина очереди. ■

см. стр. 152 "Ньюсмейкеры"

Появление на рынке	2018 г.
Ценовой сегмент	Высокий

Потребители

Предназначена для видеонаблюдения за движением на дорогах, измерения потока трафика, занятости дорог, средней скорости, статистики очереди на пунктах оплаты.
Поддерживает определение номеров мотоциклов

APIX FishEye/E6 ICM Industrial – виброзащищенная камера с малой высотой и углом обзора 360 град.

Представляет компания "СТА Плюс"

Появление на рынке	Ноябрь 2017 г.
Ценовой сегмент	Средний

В русле трендов

Чтобы обеспечить безопасность пассажиров, персонала и имущества перевозчиков, системой видеонаблюдения должны быть оборудованы не только объекты инфраструктуры, но и сами транспортные средства.

К устройствам, устанавливаемым в салонах наземного транспорта или вагонах подвижного состава, предъявляются серьезные требования. Так, видеокамеры должны характеризоваться:

- устойчивостью к вибрации и резкой смене температур;
- компактным размером и вандалозащищенностью;
- широким углом обзора;
- хорошей чувствительностью и устойчивостью к неравномерному освещению;
- высоким разрешением, позволяющим детально изучать лица или оставленные предметы;
- поддержкой современных форматов сжатия с целью экономии места на мобильных устройствах записи.

Потребители

Пассажирский транспорт (вагоны метро и электропоездов, автотранспорт)

Новый подход к решению задач

Apix FishEye/E6 ICM Industrial получила хорошую защиту от вибрации, перепада температур и запыленности. Металлический корпус, соответствующий степени IP54, надежно защищает камеру от повреждений, а также исключает попадание брызг и стекающей воды внутрь камеры.

Врезной монтаж позволяет устанавливать камеру практически вровень с потолком транспортного средства.

Для подключения камеры к бортовой сети питания и сети передачи данных предусмотрены надежные индустриальные разъемы. В первом случае это экспресс-клеммы WAGO, позволяющие моментально подключить провода без применения какого-либо инструмента, даже примитивной отвертки. Зажим надежно фиксирует провод питания и не позволяет ему выпасть при сильной тряске. Во втором случае это промышленный RJ-45 Ethernet, устойчивый к механическим воздействиям и вибрационной нагрузке.

Экономическая эффективность

Одна камера типа "рыбий глаз" способна заменить минимум две обычные камеры, а ее надежность позволит сократить затраты на обслуживание. ■

см. стр. 152 "Ньюсмейкеры"

Инновационная система видеонаблюдения высокой четкости с самообучающейся видеоаналитикой от AVIGILON

Представляет компания "АРМО-Системы"

Появление на рынке	2017 г.
Ценовой сегмент	Высокий

Ключевые преимущества

Решение Avigilon помогает концентрировать внимание на том, что важно. Видеоанализ на основе глубокого обучения искусственного интеллекта (AI) – ключ к решению задач отрасли. Применение технологий искусственного интеллекта в видеоаналитике Avigilon дает пользователям мощные инструменты для эффективного принятия решений.

Инновационная поисковая система

Технология Avigilon Appearance Search – это новый способ поиска видеоданных в архиве. Новаторская поисковая система с использованием искусственного интеллекта и глубокого обучения обрабатывает многие часы отснятых видеоматериалов, позволяя оперативно найти нужного человека или транспортное средство на всей территории объекта. Она сокращает время реагирования на происшествия и расширяет возможности их расследования, помогая собрать видеодоказательства и с высокой точностью реконструировать события.

Новый подход к решению задач

Операторам не нужно часами просматривать архивы видеоданных, пытаясь найти тот или иной инцидент. Технология самообучающейся видеоаналитики Avigilon использует сложные алгоритмы на основе видеошаблонов, чтобы распознавать перемещения и внешний вид людей и транспортных средств, игнорируя "ненужные" действия. Технология Teach-by-Examples позволяет оценивать точность сигналов тревоги для самообучения системы.

Потребители

Аэропорты, вокзалы

Проекты

King Abdulaziz International Airport (Саудовская Аравия) – один из крупнейших аэропортов в мире

В русле трендов

Компаниям требуются все более совершенные программно-аппаратные инструменты для работы с растущими объемами видеоданных. ПО ACC позволяет управлять видеоданными, поступающими от камер Avigilon – от 1 до 5 Мпкс и от 4K до 7K. Простой интерфейс ПО дает возможность персоналу с минимальной подготовкой оценивать события и реагировать на них. Наряду с этим высокую надежность видеосистем обеспечивают Avigilon HD NVR. Все модели используют технологию записи HDSM, имеют ПО ACC и 3-летнюю гарантию.

Экономическая эффективность

Один из компонентов решения – камера высокой четкости 5K (16 Мпкс) серии Pro, наиболее мощная в этом сегменте односенсорная камера с функциями видеоаналитики. Благодаря технологии HDSM™ 2.0 камера гарантирует зону охвата, соответствующую зоне охвата 53 аналоговых камер VGA, и обладает превосходным качеством изображения в сочетании с экономией полосы частот. Данная камера идеально подходит для установки на привокзальных площадях или для контроля территории аэропортов, в том числе взлетно-посадочных полос. ■

см. стр. 151 "Ньюсмейкеры"

ПО TRASSIR для системы видеонаблюдения, соответствующей требованиям транспортной безопасности РФ

Представляет компания DSSL

TRASSIR®
ЭКОСИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

Потребители
Транспортные и пересадочные узлы, пути сообщения, транспорт

Проекты
ОАО "РЖД", российский аэропортовый холдинг "Аэропорты регионов"

Появление на рынке	I квартал 2018 г.
Ценовой сегмент	Средний

Ключевые преимущества

ПО работает как в составе линейки видеорегистраторов TRASSIR, так и на собственном сервере или виртуальной машине. Обеспечивает видеонаблюдение, интеллектуальное видеонаблюдение, видеозапись и аудиозапись.

В русле трендов

Решение работает в компаниях РЖД и "Аэропорты регионов" и создано с учетом их потребностей, а также в соответствии с требованиями постановления Правительства РФ от 26 сентября 2016 г. N 969 по обеспечению транспортной безопасности в Российской Федерации.

Новый подход к решению задач

Это технологически продвинутое, экономически выгодное и современное универсальное решение, которое отвечает требованиям, предъявляемым к обеспечению транспортной безопасности в РФ.

Экономическая эффективность

Экономическая эффективность выражается в возможности разворачивать ПО для видеонаблюдения в рамках виртуальной инфраструктуры. Такой подход избавляет компании от необходимости нести расходы на создание, поддержание и обслуживание собственных вычислительных мощностей, а также содержание штата IT-сотрудников. Использование профессиональной системы видеонаблюдения TRASSIR позволяет эффективно модернизировать уже существующие и морально устаревшие аналоговые системы видеонаблюдения до уровня, отвечающего современным требованиям транспортной безопасности в РФ. Применение ПО TRASSIR в транспортной отрасли экономически выгодно потребителям, поскольку существенно сокращает расходы на внедрение, так как пусконаладка системы производится удаленно. ■

см. стр. 151 "Ньюсмейкеры"

Автономная система контроля доступа с IP-камерой B2230L

Представляет "НПП "Беверд"

Ключевые преимущества

Система по распознаванию автономеров уже встроена в саму видеокамеру. Таким образом, не нужно приобретать дополнительное ПО, серверы или лицензию.
Все необходимое уже присутствует в модели, а стоимость окончательного решения по распознаванию номеров уже заложена в цену камеры.

Появление на рынке	II квартал 2018 г.
Ценовой сегмент	Средний

В русле трендов

Сейчас для обеспечения доступа автомобиля на охраняемую или частную территорию существует несколько путей: водитель останавливает авто, сам открывает ворота, подносит ключ, разговаривает с охранником. Без участия водителя – охранник, который откроет ворота, или ПО, нуждающееся в серверных мощностях и покупке ключей. Современный ритм работы требует, чтобы все задачи, включая СКУД, решались максимально оперативно и с минимальными затратами. А следовательно, камера, сама распознающая автономера подъезжающих автомобилей и дающая команду на открытие ворот, является оптимальным решением.

Новый подход к решению задач

Решение BEWARD с точностью до 98% распознает автомобильные номера СНГ 2- и 3-значных регионов. ПО настроено именно на распознавание автономеров, а значит исключаются ложные срабатывания от телефонных номеров на корпусе машин или каких-то иных объектов в кадре.
Поддерживается распознавание номеров на автомобилях, движущихся на скорости до 10 км/ч. В камере реализована поддержка функции аппаратного WDR 120 дБ, тем самым решается проблема съемки при засветке изображения от автомобильных фар. Формат кодирования видео – H.265, позволяющий сжать размер видео в архиве в 2 раза.

Потребители
Парковка, промышленность и др. (автоматический контроль доступа на закрытую или частную территорию)

Экономическая эффективность

В настоящее время для обеспечения распознавания номеров проезжающего на контролируемую территорию транспорта требуется приобретение IP-видеокамеры, сервера, обрабатывающего изображения, профессионального ПО. Таким образом, задача распознавания номеров сводилась к совместному использованию различных структур, зачастую никак не связанных компаний.
Решение, предлагаемое BEWARD, не требует каких-либо дополнительных настроек и вложений и решает задачу распознавания номеров за счет мощностей самой видеокамеры. ■

см. стр. 151 "Ньюсмейкеры"

Международный форум

21-23.11.2018

ALL-OVER-IP

ТОЛЬКО БИЗНЕС - НИЧЕГО ЛИШНЕГО

Генеральный спонсор:

axxonsoft

MEMBER OF ITVGROUP

www.all-over-ip.ru

Секреты демпинга

В жизни каждого менеджера случаются минуты, когда он вдруг осознает, что пора перестать горбатиться на чужого дядю и что время подумать о собственном бизнесе. В этот момент он же заражает своей идеей кого-нибудь из своих коллег, они вместе пишут заявления об увольнении, не забывая перед этим скачать из 1С клиентскую базу. Самое первое, что ребята начинают делать на своем новом рабочем месте, – демпинговать. В этой статье будет рассмотрено, почему через демпинг проходили практически все компании, какие виды демпинга бывают и почему демпинг – это плохо

Михаил Бялый
Генеральный директор ТД "Актив-СБ"

Многие известные фирмы начинали с демпинга. Например, в демпинге правительство США обвинило в 80-е гг. компанию Sony – она предлагала произведенные в Японии телевизоры на американском рынке за 180 долларов, хотя на родных островах такая же модель стоила 333 доллара. Сегодня Sony нельзя отнести к разряду дешевых производителей, демпинг с ее стороны был временным явлением.

Когда Hikvision стал выходить на российский рынок IP-видеонаблюдения, то были выбраны пять – шесть самых популярных позиций IP-камер, на которые рублевые цены явно не соответствовали их долларовому эквиваленту в китайском прайс-листе. Цены на "убойные" камеры были явно ниже их реальной стоимости, что вызвало нервную дрожь у многих присутствующих на тот момент на российском рынке конкурентов. Но со временем рынок наполнился еще более дешевыми моделями камер, и тогда в ход пошел HiWatch, а Hikvision стал исключительно "профессиональной линейкой".

Постоянно удерживать цены на низком уровне можно, если только ты являешься производителем или имеешь эксклюзивы на поставку какой-либо продукции. Но когда твой "портфель" состоит из широко представленных в твоем регионе брендов и ты вырастаешь до определенных объемов, становясь дилером или дистрибьютором, это значит, что ты вынужден соблюдать ценовую политику производителей. Узкий смокинг официального представителя сковывает твои движения, и ты вынужден поднимать цены. Если ты успел обзавестись собственным брендом или заключил с кем-то из поставщиков эксклюзивные соглашения, то процесс ценообразования продолжает находиться в твоих руках.

В противном случае тебе остается только смотреть, как клиенты уходят в небольшие фирмы, не связанные с производителями никакими обязательствами. И вот парадокс: условия по закупке у них хуже, а продают они больше.

Но есть на рынке и компании, так называемые дискаунтеры, которые умудряются, даже вырастая, демпинговать по всем брендовым направлениям.

Неджентльменский демпинг

Бывший сотрудник одного такого крупного дискаунтера описал правила, существующие в компании, следующим образом:

1. При выходе за стойку на тебя по умолчанию навешивается так называемая "материальная ответственность" – все, что попало к тебе в руки, ты купил. Если в коробке некомплект, а такое случается часто, ибо товар "левый", то ты отвечаешь персонально – минусом в заработной плате.
2. Политика тотального обмана и впаривания – принцип работы "хорошего" сотрудника в такой компании. Нагреть работягу, который пришел на свои скромные доходы купить сыну комп, или бабулю, выбирающую внучке фотоаппарат, или женщину, которой нужна хорошая флешка, – все это норма. И чем циничнее ты "опустил" клиента, тем больше твой авторитет среди старожилов.
3. Периодически даются установки, что продавать. Например, серую партию с высоким процентом брака. Неуверенного клиента нужно переключить на этот товар, врать о его свойствах не запрещено.
4. Сплошные подставы. Складские воруют, менеджеры воруют и т.д. Забирая товар со склада, нужно внимательно следить за целостностью упаковки – и при малейшем подозрении проверять. В китовом комплекте фотоаппарата можно недосчитаться объектива 20К – стоимость потом вычитается из твоей зарплаты.
5. Заработная плата напрямую зависит от того, сколько человек ты обманул: наибольший бонус приходит от товара, реальная стоимость которого в разы ниже продажной цены. Например, когда при покупке фотоаппарата клиенту впаривается корейская SD-карта за 1000 – 1500 рублей, которая на радиорынке стоит 100 рублей.

Любой нормальный человек, поработав в таком магазине пару недель, поймет, в чем дело, и уволится (что, кстати, здесь не так просто).

Как видно из этого описания, демпинг не всегда работает в белых перчатках и не все компании, даже вырастая, готовы от него отказаться.

Продажа заведомо неисправного или нелегально вывезенного оборудования – это нарушение не только правил торговли, но и законодательства.

При недобросовестной конкуренции на рынке начинается "слив" товара и внешне порядочными компаниями.

Каким из советов (часть первая) готовы будут воспользоваться ребята на стартапе, сказать трудно. Но они откроют ООО, найдут бесплатный "движок" для сайта, "допилят" его за пару десятков тысяч рублей. По отчетам, предусмотрительно взятым с предыдущей работы, и по статистике с wordstat.yandex.ru будет определен основной ассортимент. Вопрос о наполнении сайта вручную будет отвергнут на корню, так как требует много времени и денег. Самым простой способ – "сграбить" чужой сайт, выкачав с него описание и картинки, и даже цены. Среди фрилансеров найдется исполнитель, который за 10 тыс. рублей допишет существующий у него "парсер", и через 24 часа выкачанная с сайта-донора база данных будет у наших героев на рабочем столе. Такой способ не подходит для тех сайтов, которые будут продвигаться в "органическом" поиске, так как поисковики "склеивают" одинаковый контент и в выдаче всегда будет только сайт-первоисточник. Но наших героев это не волнует, ведь ловить клиентов они собираются по-другому.

Как мы видим из второй части советов, в демпинге нет ничего сложного. Главное – следить за ценами и не улететь "в минус", так как маржа минимальная. Хотя можно снова "парсить" какой-нибудь чужой сайт, вытягивая из него цены и импортировать к себе, не забывая проставлять

Вредные советы. Часть первая. Закрытый демпинг

Если цены ты не можешь официально опустить,
Значит, должен предложить ты покупателю откат.
Есть еще одно решение: что-то надо "подарить".
Например, по счету нужно: камеры, а к ним кронштейн.
В счете камеры оставь ты, а кронштейны так отдай.
Можно поступить иначе: разработать договор
О неразглашении данных , в том числе и в накладных.
А за нарушенье – штрафы, чтоб клиент вдруг не "спалил".
Есть еще удачный способ демпинг скрыть от лишних глаз.
Создается сеть партнеров, в регионах, например.
Ты партнеру продаешь все, накрутив процентов пять.
Твой партнер имеет цены лучше рыночных в разы.
Ты же со своих партеров получаешь оборот,
Требуемый для закупок с самой низкою ценой.
Для торгов другой прием есть, всем участникам знаком:
Если тендер решил выиграть, но за тендером следят,
Запусти ИП "Палёный", пусть в торгах играет он.
И пусть он роняет цены: ты же вроде не при чем.

Вредные советы. Часть вторая. Открытый демпинг
Если вдруг решил, что самый умный ты из конкурентов,
То на сайте ставь ты цены ниже всех, хотя б на рубль.
И пойдет все как по маслу: подключаешь Яндекс.Маркет,
Ставку делаешь хоть рубль, все равно ведь покупатель
По цене отсортирует.
Твое место будет первым, впереди официалов.
Ну а чтобы покупатель был уверен, что ты лучший,
Прикупи на контент-бирже отзывы на Яндекс.Маркет.
Рейтинг свой поднимешь сразу.
И тебе это поможет, даже если кто-то двойку
Сгоряча вдруг да поставит. Потерять ее несложно
Среди купленных пятерок.
Есть еще одна примочка, тоже Яндекса: Советник.
Это лучший твой помощник.
Вот представь: сайт конкурента тратит время, тратит деньги
На создание контента.
И по этой вот причине в поиске на первых строчках
Он всегда по всем запросам.
Но завидовать не стоит, потому что есть Советник.
Всем клиентам он подскажет, что есть цены подешевле.
Покупатель переходит на страницу демпингера: у него цена-то ниже.

скидку. Зачем делать лишнюю работу, занимаясь обработкой кучи прайсов от поставщиков, если можно все сделать разом и на халяву?

Неужели все так просто? Есть, конечно, свои подводные камни. Вас может отключить от Яндекс.Маркета служба контроля качества. В зависимости от выбранной вами модели размещения на Яндекс.Маркете: "оплата за заказ на Маркете" (CPA) или "оплата за переход а магазин" (CPC) – для этого у вас должно быть зафиксировано две или четыре критичные ошибки соответственно.

К критичным ошибкам на Яндекс.Маркете относятся:

- неприемлемое качество (например, неверно указан срок или стоимость доставки);
- прочие проблемы качества (например, магазин подозревается в мошенничестве или у магазина повторяющиеся технические ошибки);
- дублирующие магазины;
- сайт временно недоступен.

Ошибкой также считается ситуация, в которой вместо товара в предложении покупателю предлагают другой. "А что в этом плохого? – скажете вы. – Клиенту предлагается аналог с теми же свойствами". Ничего плохого здесь нет с точки зрения продавца. Действительно, многие бренды систем видеонаблюдения выпускаются в Китае на одних и тех же заводах, поэтому часто без шильдика их не различить. Покупателю разницы нет, а на "своем" бренде у продавца заработки на порядок выше. Ну и что, что бренд-приманка вложился в свою "раскрутку", и поэтому он пользуется популярностью, и клиент приходит именно за ним. На него скидок нет, статус дилера по нему тоже не дают. Значит, можно самим привезти "фигзнаеткакойвижн" и предлагать его.

Но даже если магазин отключат от Яндекс.Маркета, ничто не мешает открыть новое ООО или ИП, купить за 1000 рублей в месяц виртуальный телефонный номер и запустить новый магазин на Маркете с другим доменным именем.

Так что вопрос со службой контроля качества решается, как и решается вопрос с навязчивыми производителями, пытающимися доказать вам, что нужно соблюдать их ценовую политику. На них можно просто не обращать внимания, так как антимонопольное законодательство никто еще не отменя, и не их собачье дело, по каким каналам вы приобретаете их продукцию. Яндекс.Маркет с жалобами производителей работает лишь в том случае, если есть судебные решения или возбуждено уголовное дело. То же самое касается и хостинг-центров. Так что угрозы об отключении магазина на Яндекс.Маркете или сайта на хостинге со стороны производителя – пустое сотрясение воздуха.

Лучше думать не об этом, а о другом. О том, на чем еще можно сэкономить (часть третья).

"А на чем еще можно сэкономить, – спросите вы, – кроме налогов?" Да на всем!

Например, на сотрудниках. Из приведенного выше отзыва о работе в компании-демпингере видно, что квалифицированным персоналом в подобных компаниях и не пахнет. Любой умеющий работать с компьютером и живущий неподалеку юнец сгодится на эту работу. Но нет гарантии, что подобранный им комплект оборудования будет рабочим.

Кстати, о гарантии. С ней тоже не все однозначно. Даже если у вас будет гарантия от производителя, то путь оборудования от вас до сервисного центра с учетом "кривизны" поставок может оказаться тернист и долог. Следить за ремонтом вашего оборудования тоже будет некому, так что готовьтесь к многочисленным "завтракам" и томительному ожиданию.

Демпингеру не нужен склад. По правилам того же Яндекс.Маркета, позиция, обозначенная значком "в наличии", должна быть поставлена в течение указанного продавцом срока, который может составлять даже для своего региона несколько дней, поэтому всегда есть возможность оперативно заслать курьера за товаром к поставщику. Покупатель в таком случае не сможет подобрать себе систему "на месте", "пощупать" и посмотреть ее. Отсутствие товара на собственном складе сразу увеличивает срок поставки как минимум на день, и вопрос возврата может оказаться непростым. Если купили товар у такого продавца – готовьтесь оперировать цитатами из закона о правах потребителя, если вы частное лицо, или статьями Гражданского кодекса, если оплата прошла от "юрика".

Ну что, господа демпингеры, действуйте! Советов я вам дал предостаточно. А как же производители? Что делать им?

Вредные советы. Часть третья. Отсекаем все лишнее
Если хочешь заработать: не плати совсем налоги.
Делается это просто.
Первый шаг: купи ОООшку, счет открой в некрупном банке,
Поступившие все деньги отправляй на обналичку.
Можно покупать услуги иль товар брать виртуальный
НДС свести к нулю чтоб.
Никакой зарплаты белой и, естественно, налогов.
Есть отчетность – значит, фирма существует по закону.
Как три года фирме стукнет, надо ее слить обратно.
Президент сказал не трогать бизнес первые три года.
Так что пользуйся моментом.
Есть еще одна подсказка: перейди на упрощенку,
И налог твой – с оборота.
Чтобы не светить продажи, ничего не "бей" по кассе,
"Бей" по чековой машинке. С виду чек как настоящий.
Для доставки он сгодится.
Ты представь: таким макаром шесть процентов сэкономишь.
Правда, есть один нюансик: при проверке сразу видно
Нарушение закона.
Так что будет весьма кстати завестись хорошей "крышей".

Выход есть!

Производителям оборудования для борьбы с демпингом советы я могу дать такие.

1. Разрешить официальным дилерам показывать не запредельные розничные цены, а реальные оптовые, так как времена, когда рекомендованную розницу закладывали в проекты, прошли, и начальная цена в конкурсах берется из счетов, а не из Интернета.
2. Навести порядок среди своих дилеров, вплоть до исключения нарушителей. Глядишь, и демпингеры перекинутся на более прибыльный и менее геморройный для них бренд, чем ваш. А преданные вам партнеры будут благодарны: ведь покупая у вас товар за сто рублей, они готовы продать его за сто двадцать, а не сидеть с ценником в сто пятьдесят и смотреть, как свои пять рублей зарабатывают демпингеры. ■

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

Развитие технологий безопасности службы инкассации Сбербанка

Для банков служба инкассации имеет важное значение, услуги инкассации являются востребованными. Можно иметь высокую степень безопасности банковского объекта, умело разделить уровни доступа на основе идентификации и аутентификации, использовать современные системы защиты устройств самообслуживания, однако не менее важно защитить ценности, наличные средства и документацию при перемещении из пункта А в пункт В. Эту далеко не школьную задачу и решает служба инкассации

Андрей Новиков
Управляющий директор,
заместитель директора департамента –
начальник Управления инкассации
ЦУНДО ПАО "Сбербанк"

Наличие собственной службы инкассации является необходимым условием успешной работы Сбербанка, важнейшим элементом комплексного операционно-кассового обслуживания клиентов и обусловлено масштабами бизнеса и ролью, которую Сбербанк играет в российской банковской системе. Банку необходимо обеспечивать эффективную и бесперебойную работу обширной сети отделений, банкоматов и платежных терминалов, снижать затраты на внутрисистемные перевозки и обеспечивать качественное обслуживание порядка 14 500 внутренних структурных подразделений, 75 500 устройств самообслуживания, 140 000 клиентских объектов.

Несомненно, служба инкассации Сбербанка является одной из самых технически оснащенных и передовых по внедрению инновационных решений на территории Российской Федерации.

Лучшая защита – сделать нападение на инкассаторов бессмысленным

Мир не стоит на месте, появляются новые высокотехнологичные и инновационные решения в инкассации и защите банковских ценностей. Мы исходим из правильного управления денежными потоками, которые позволят нам сократить наши расходы в обслуживании денежной наличности. Соответственно, мы меняем принципы работы подразделений инкассации, повышая производительность труда, активно применяем в этой области международный опыт, отслеживая новые технологии в сфере безопасности перевозок, оцениваем и внедряет лучшие из них.

В настоящее время служба инкассации Сбербанка нацелена на решение следующих задач:

- повышение эффективности работы без снижения уровня защищенности персонала;
- организация качественного контроля за соблюдением требований совершения операций инкассации;
- снижение операционных рисков, исключение внутреннего предательства;
- организация контроля оперативной обстановки и действий инкассаторских работников на маршруте;
- развитие интеллектуальных технологий и систем защиты банковских ценностей, делающих любые посягательства на инкассаторских работников бессмысленными.

Спецконтейнеры

Используемые в Сбербанке спецконтейнеры оснащены устройством по приведению содержимого в неплатежеспособное состояние путем окрашивания несмываемыми чернилами (краской) при несанкционированном проникновении (взломе). Возможна также установка на спецконтейнер оборудования, позволяющего дистанционно включить окрашивание его содержимого при нападении на сотрудника инкассации.

Спецконтейнеры позволяют минимизировать риски утраты/хищения денежной наличности при их транспортировке и повысить уровень обеспечения безопасности инкассаторов, а также выйти на новый уровень технического оснащения и оптимизировать деятельность подразделений инкассации.

Применение спецконтейнеров делает нападения на инкассаторов бессмысленными. Окрашенные банкноты невозможно привести в платежное состояние, предъявить к обмену или сбыть через устройства с функцией приема наличных денег (Cash-In).

В случае если окрашенные банкноты все-таки были похищены, то банк, несомненно, понесет убытки. Вместе с тем, преступник не сможет воспользоваться похищенной денежной наличностью, а следовательно, не будет планировать нападений в дальнейшем.

В настоящее время все подразделения инкассации Сбербанка оснащены подобными устройствами.

Специалистами инкассации Сбербанка совместно с производителями на постоянной основе проводится работа по совершенствованию модельного ряда спецконтейнеров и их технических характеристик.

Smart Car

Сбербанк не стоит на месте, в использовании спецконтейнеров мы идем дальше. Так в настоящее время мы приступили к обслуживанию внутренних структурных подразделений с применением спецавтомобиля Smart Car.

Smart Car – это небронированный спецавтомобиль, оснащенный электронно-механической системой хранения ценностей. Работа на маршруте осуществляется одним инкассаторским работником. Ценности перевозятся в Smart Car только в спецконтейнерах, и изъятие спецконтейнера из ячейки спецавтомобиля на маршруте возможно только при попадании в зону обслуживаемого объекта. На всем протяжении маршрута за спецавтомобилем осуществляется контроль со стороны Центра мониторинга Сбербанка. Система мониторинга позволяет производить контроль за заблокированными от несанкционированного изъятия ячейками со спецконтейнерами во время отсутствия инкассатора.

Использование в инкассации специальных автомобилей Smart Car позволило снизить численный состав бригад с двух до одного инкассаторского работника без снижения уровня безопасности совершения операций.

Доступ инкассатора к ценностям исключен. В итоге изъятие спецконтейнера из ячейки на маршруте возможно только при попадании в зону нужного объекта, вскрытие спецконтейнера во внутреннем структурном подразделении или у клиента проводится с использованием двух ключей – инкассатора и сотрудника кассы.

Применение нового технологического процесса дает следующие преимущества:

- обслуживание внутренних структурных подразделений и клиентов одним инкассаторским работником;
- эффект от снижения среднедневных остатков в кассах структурных подразделений банка;
- снижение себестоимости инкассовых операций.

Из недостатков этой системы следует отметить высокую стоимость оборудования (интеллектуальных устройств) при отсутствии недорогих отечественных аналогов.

Применение DROP SAFE

Еще более защищенными являются перевозки, осуществляемые в спецавтомобиле с DROP SAFE. В этом случае спецконтейнер используется вместе

Smart Car могут перевозить от 9 до 20 единиц спецконтейнеров

В DROP SAFE спецконтейнер используется совместно с сейфом

Центр мониторинга службы инкассации

с сейфом, а у инкассаторских работников отсутствует доступ к денежной наличности. При вложении спецконтейнера в сейф наличные деньги автоматически перемещаются в сейфовую часть.
При использовании DROP SAFE операции инкассации и перевозки наличных денег могут осуществляться как на бронированном, так и на небронированном автомобиле одним инкассаторским работником. При несанкционированном доступе наличные деньги окрашиваются в спецконтейнере либо в сейфе, установленном в спецавтомобиле.

Технологии безопасности для специализированных транспортных средств

С целью усиления защиты перевозимых банковских ценностей на спецавтомобили банка устанавливается система блокировки, которая позволяет удаленно блокировать с поста мониторинга двигатель, двери и устройство-накопитель специализированного транспортного средства и исключить возможность угона автомобиля или его отклонение от маршрута, снижает возможность завладения ценностями, в том числе при внутреннем мошенничестве. При подозрительных действиях сигнал блокировки немедленно подается оператором поста мониторинга на GSM-трекер спецавтомобиля.

Центр мониторинга службы инкассации

Созданная система мониторинга спецавтотранспорта является одним из элементов комплексной системы безопасности Сбербанка.
Посты мониторинга, развернутые в подразделениях инкассации, объединяющиеся по каналам корпоративной сети банка, позволяют обеспечивать сквозной контроль работы бригад инкассаторов и безопасность инкассаторской деятельности на всей территории России.
На экран монитора операторов выводится вся необходимая информация о местоположении и состоянии спецавтомобилей: перемещение автомобиля на карте, включение/выключение зажигания, открытие/закрытие дверей, обслуживание объектов, выезд за пределы зоны обслуживания и т.д. В случае возникновения чрезвычайной ситуации при работе на маршруте и приеме сигнала "Тревога" от бригады инкассаторов обеспечивается немедленная визуализация этого автомобиля на экране монитора и установление связи с ним. Вся информация, включая речевой радиообмен, архивируется без возможности ее корректировки оператором.
На основании статистической информации, хранящейся в базе данных системы мониторинга, готовятся управленческие решения, которые позволяют минимизировать риски, связанные с криминальной обстановкой, минимизировать потери на маршрутах, проанализировать каждый маршрут и усовершенствовать его, повысить производительность всего подразделения, а также провести другую аналитическую работу.

Внедрение персональных систем аудио- и видеофиксации

Применение мобильных и персональных систем аудио- и видеофиксации является действенной мерой для улучшения производственного контроля и повышения технологической дисциплины при проведении операций инкассации.
Комплекты системы состоят из мультимедийного терминала и персональных (носимых) видеорегистраторов.
Носимый видеорегистратор применяется:

- для синхронной аудио- и видеофиксации окружающей обстановки;
- как элемент технологического зрения инкассатора, непосредственно выполняющего операции инкассации;
- для разбирательства спорных (конфликтных) ситуаций;
- для контроля за действиями инкассаторских работников.

Носимый видеорегистратор

Интерактивный мультимедийный терминал предназначен для зарядки персональных видеорегистраторов, архивирования и хранения данных, полученных с помощью указанных устройств. Терминал имеет встроенную камеру для фиксаций действия оператора, многоуровневую систему авторизации. Имеется возможность настраивать время хранения записей и защита данных от неавторизованного копирования и удаления.

Система COGITO 4M

Другой пилотный проект службы инкассации Сбербанка заключался в апробации системы COGITO 4M. Это автоматизированная система, предназначенная для сбора и анализа психофизических признаков, которые могут влиять на принятие решения о персонале.
Система может использоваться для предварительной проверки персонала при приеме на работу и для уже работающих сотрудников в процессе их деятельности. По итогам тестирования система выдает решение – подозрительный человек или не подозрительный, а также дает рекомендации для последующих действий по данному сотруднику.
В нашем случае система помогла выявить и отсеять на ранних стадиях кандидатов, не пригодных к работе в подразделениях инкассации.
Традиционным тестированием сотрудников добиться таких результатов не представляется возможным.

Резюме

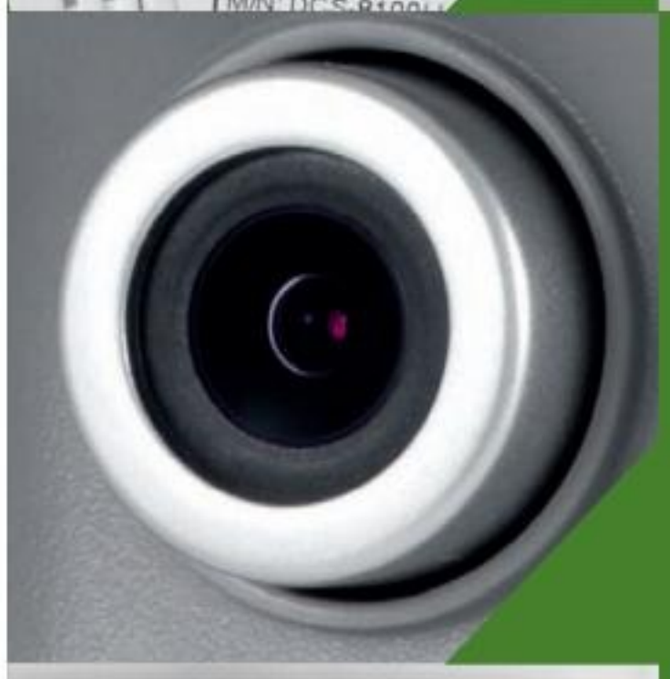
Сбербанк отслеживает новые виды оборудования и инновационные технологии, все новое, что появляется на рынке инкассации, и старается внедрять это в практическую деятельность для повышения эффективности работы и снижения рисковых событий.
Вместе с тем технологии, применяемые в Сбербанке, слабо применяются перевозчиками и банками на российском рынке из-за того, что подобные устройства дорогостоящи и в настоящее время в стране отсутствуют их аналоги.
Мы взаимодействуем с рядом российских производителей спецоборудования и ждем от них предложений по новым системам защиты наличности при транспортировке и системам поддержки деятельности инкассаторов, а также снижения стоимости спецоборудования отечественного производства по отношению к импортному. ■

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

В реалиях современного рынка безопасности необходимым требованием становится обеспечение видеонаблюдения на любом предприятии, будь то маленький магазин или огромный завод. Но зачастую требования к желаемым устройствам в этих случаях сильно разнятся. Среди профессионального видеонаблюдения встречаются задачи, которые можно решить только с применением уличных PTZ-камер с ИК-подсветкой, тепловизоров, взрывозащищенных и антивандальных камер, да и просто мультимегапиксельных моделей. А для обеспечения "бытового" видеонаблюдения, например в мелком кафе, квартире или магазине, вполне достаточно самых простых мегапиксельных камер со встроенным микрофоном. Сейчас в данной нише находятся как аналоговые, так и цифровые

ТЕСТ

IP-камеры, но оба этих решения требуют настройки видеорегистраторов, серверов. Все более распространенным и удобным в использовании становится облачное видеонаблюдение, или иначе VSaaS.



Тестирование облачных Cube IP-камер

В видеонаблюдении облачные технологии позволяют пользователю переложить все задачи обслуживания процесса приема/передачи информации на плечи представителя облачного сервиса. Такие устройства предполагают отсутствие проблем с установкой у пользователя. Клиенту требуется лишь подключить камеру к сети питания и сети Интернет, а потом пройти несложную онлайн-регистрацию. После этого доступ к архиву и трансляции с камеры становятся доступными откуда угодно (к примеру, во время отпуска), а данные будут храниться у облачного провайдера, тем самым решая проблему настройки серверов на стороне клиента.

Тестирование проведено и предоставлено независимой тестовой лабораторией CCTVLAB

Инсталлятору подобные камеры тоже могут быть интересны простотой настройки интерфейса и обучения пользователя работе с ним. В нашем тесте, чтобы еще больше подчеркнуть простоту и бюджетность облачных камер, мы решили тестировать камеры в Cube-исполнении.

Не стоит считать, что компактные камеры обладают худшими возможностями. На рынке представлены модели со встроенной ИК-подсветкой, датчиками движения, динамиками и другим функционалом. Преимуществом Cube-камер является их легкий крепеж на стену и потолок, имеется кронштейн для простой установки на горизонтальную поверхность (стол, шкаф и т.д.). На рынке представлены и модели с магнитным креплением к металлическим поверхностям. Для клиента также важно, что подобные камеры практически всегда укомплектованы встроенным микрофоном, в отличие от тех же Bullet- и Dome-камер. Помимо этого, Cube-камеры часто выбирают из-за их дизайна, что, как ни странно, оказывается довольно важным аспектом при выборе камеры видеонаблюдения в офис или тем более квартиру.

Лаборатория CCTVlab решила проверить, насколько хорошо бюджетные облачные камеры справляются со своими базовыми обязанностями.

Что тестируем

Сейчас доступно множество облачных сервисов, поддерживающих камеры видеонаблюдения любого производителя. Мы же решили повторить путь простого покупателя – рассмотреть камеры, в которые производитель сам заложил поддержку облачного сервиса и которые не требуют от потребителя дополнительного поиска и скачивания ПО после покупки. Испытывать будем те характеристики, которые являются основными для подобных бюджетных моделей: угол обзора камеры, ее разрешение и битрейт, а также работу встроенного микрофона. Если с первыми тремя пунктами все просто, то качество звука в камере мы решили оценить по ее возможности выделять человеческую речь на фоне техногенного шума, что часто наблюдается, например, в офисе.

Таким образом, критерии, которые мы ожидали увидеть от камер, следующие:

1) Cube-исполнение;
2) поддержка облачного сервиса;
3) стоимость до 15 тыс. рублей;
4) наличие встроенного микрофона.

Что нам предоставили на тест:

- **CamDrive CD310;**
- **D-Link DCS-8100LH;**
- **MICRODIGITAL MDC-N4090W-8;**
- **SpaceCam F1.**

Как измеряем?

1. Угол обзора камер измеряется по стандартной методике, по тестовым мирам.
2. Разрешение камер измеряется по специальной тестовой таблице при освещенности 500 лк ("день" на графиках) и при освещенности менее 1 лк, при работе от встроенной ИК-подсветки ("ночь" на графиках). Для камеры с сенсором 2 Мпкс проводились измерения разрешения для 1 Мпкс и 2 Мпкс ("2 Мпкс" на графиках).
3. Битрейт камер измеряется при тех же условиях, что и в предыдущем пункте. Для камер, позволяющих управлять битрейтом напрямую, дополнительно проводилось ручное уменьшение величины потока так, чтобы разрешение камеры при этом не отличалось от своего максимального значения ("снижение битрейта" на графиках).
4. Границу различимости голоса относительно уровня шума измеряли в специальной тестовой комнате. Громкость записанной речи соответствовала уровню шума в помещении, и слова были четко различимы во всех камерах. Далее для каждой камеры определялся порог, когда речь становилась неразборчивой.

CamDrive CD310

Предоставлена компанией НПП "Беверд"

Занимает лидирующую позицию по величине предельного потока (569 Кбит/с при дневной и ночной съемке), при этом базовое значение потока находится в числе лидеров (1009 и 1011 Кбит/с день и ночь соответственно). Входит в число лидеров по величине горизонтального разрешения (день – 1140 и ночь – 1122 линии) и его стабильности (различие между дневной и ночной съемкой – 2%). Входит в число лидеров по величине фактического угла обзора – 92 град., значение, самое близкое к указанному в ТТХ среди всех камер (различие составляет 2%). Камера оснащена самым чувствительным микрофоном, позволяющим различать речь на уровне шума при ослаблении до -14 дБ.

В своей камере производитель заявляет использование 1 Мпкс КМОП-сенсора со скоростью записи до 25 кадр/с при любом разрешении. Заявленная акустическая дальность встроенного микрофона составляет 10 м. В камере также есть динамик для обеспечения двусторонней связи. Заявлена поддержка мобильных устройств Android и iOS. В подсветке камеры использованы ИК-светодиоды с заявленной дальностью до 8 м. Производитель подчеркивает, что встроенный PIR- датчик позволяет добиться гарантированного срабатывания в случае обнаружения движения человека перед камерой в полной темноте (меньше ложных срабатываний). После детекции заявлена отправка сообщения пользователю по СМС или на e-mail.

В камере используется облачный сервис CamDrive, который, по словам производителя, позволяет удаленно наблюдать за происходящим в реальном времени с одной или нескольких камер, а также просматривать и управлять настройками видеоархива, используя как мобильное приложение, так и Web-браузер. В личном кабинете CamDrive можно самостоятельно выбрать размер и положение зоны детекции, а также задать порог срабатывания детектора. По словам производителя, серверы промышленного стандарта обеспечены бесперебойной работой 24 часа в сутки. Дублирование архива на нескольких носителях должно исключать случайную утерю данных. Отмечается круглосуточный мониторинг работы сервиса CamDrive, что должно позволять своевременно устранять любые возникающие проблемы. Производитель предлагает клиентам бесплатную первую неделю использования архива для записи видео. ■

D-Link DCS-8100LH

Предоставлена компанией ДЛИНК

Имеет самый большой угол обзора в тесте – 197 град. Показывает наилучшее разрешение при съемке при 500 лк среди других 1 Мпкс камер – 1199 линий, разрешение ночью находится среди лидеров – 1062 линии. При этом камера имеет наименьший базовый битрейт при дневной съемке – 948 Кбит/с и такое же значение при освещении от встроенной подсветки. Оснащена микрофоном с порогом чувствительности -12 дБ, что является вторым после лидера значением в тесте.

По словам производителя, компактная беспроводная сетевая камера предназначена для обеспечения круглосуточного видеонаблюдения

благодаря инфракрасной подсветке, с заявленной дальностью до 5 м. Отмечается, что широкоугольный объектив с углом обзора 180 град. позволяет вести съемку целой комнаты с помощью одной камеры. Встроенный микрофон и динамик обеспечивают функцию двусторонней аудиосвязи. Производитель подчеркивает, что камера спроектирована для удобной установки в любом необходимом месте. Уникальный дизайн устройства с возможностью вращения и наклона, по его словам, позволяет быстро настроить необходимый угол обзора, благодаря чему модель можно устанавливать на горизонтальных, вертикальных и потолочных поверхностях. Отмечается, что возможность беспроводного подключения позволяет установить устройство без необходимости прокладки Ethernet-кабеля.

Установка и настройка производится с помощью мобильного устройства с поддержкой Bluetooth 4.0 и бесплатного приложения Mydlink и, как подчеркивает производитель, не представляет сложности. При срабатывании функции обнаружения движения или звука должна автоматически начинаться запись, а на мобильное устройство пользователя отправляться уведомление. Камера поддерживает сервис Mydlink, который, по словам производителя, позволяет

получить доступ, настроить камеру и начать запись видео на встроенную карту памяти удаленно, вне зависимости от местонахождения. Производитель также отмечает, что в новом мобильном приложении Mydlink уже реализованы запись событий в облако (пока доступен пробный период до конца года), просмотр архива с облака, сохранение записей на смартфон, расписания для различных правил, автоматизация. ■

MDC-N4090W-8

Предоставлена компанией MICRODIGITAL

Благодаря 2 Мпкс сенсору имеет самое большое разрешение в тесте, при съемке как на разрешении 2 Мпкс (1390 линий день, 1130 линий ночь), так и при съемке на разрешении 1 Мпкс (1220 линий день, 1130 линий ночь). Значение потока при этом составляет 2190 и 2250 Кбит/с при 2 Мпкс и 1200 и 1163 Кбит/с при 1 Мпкс, днем и ночью соответственно. Имеет угол обзора 84 град. С точки зрения звука камера, обладающая микрофоном, позволяющим различить речь на -12 дБ, входит в число лидеров.

Производитель описывает свою модель как миниатюрную IP-камеру для помещений. В камере, единственной среди тестируемых, заявлен 2 Мпкс сенсор 1/2.9" Progressive SONY CMOS. Модель обеспечивает трансляцию видео с максимальным разрешением 1920x1080 пкс, со скоростью 25 кадр/с. Устройство оснащено фиксированным объективом 3,6 мм. Для организации полноценной системы безопасности в модели присутствуют входной и выходной контакты тревоги. В камере также есть микрофон и реализован аудиовыход для подключения внешнего динамика, который может быть использован для обеспечения двусторонней аудиосвязи с местом наблюдения. Присутствует ИК-подсветка. Заявляется поддержка передачи видеосигнала по сети Wi-Fi, а вместе с камерой поставляется USB Wi-Fi-модуль. Камера питается от 12 В, опционально заявлено питание по PoE.

Доступ к облачному видеонаблюдению в модели осуществляется посредством использования сервиса Veedo. По словам разработчика, хранение видеоархива в облаке гарантирует его целостность в случае возникновения форс-мажорных обстоятельств на объекте наблюдения (пожар, ограбление и т.д.). Отмечается также, что специально разработанные мобиль-

ные приложения для телефонов iOS и Android позволяют с комфортом пользоваться сервисом, используя сотовые телефоны, смартфоны, планшеты. Производитель указывает, что примененные алгоритмы обработки, сжатия и кодирования видеопотока оптимизируют и обеспечивают безопасность передачи видеопотока в зависимости от качества и скорости интернет-канала. ■

SpaceCam F1

Предоставлена компанией RVi Group

Входит в число лидеров по величине битрейта (базовое значение составляет 987 Кбит/с при дневной съемке и 878 Кбит/с при ночной). В ходе теста показала горизонтальное разрешение, равное 1083 линиям при дневной съемке и 1022 линиям при ночной. Стабильность разрешения одна из лучших в тесте – падение разрешения при освещении от встроенной подсветки составило 6%. Имеет один из лучших углов обзора в тесте – 95 град., его значение достаточно близко к заявленному, отличие составляет 5%. Камера оснащена микрофоном, позволяющим различать голос при его ослаблении до -6 дБ.

Производитель описывает свою модель как IP-камеру наблюдения для внутренней установки и работы в облачном сервисе SpaceCam. В камере присутствует поддержка Wi-Fi, что, как отмечается, исключает необходимость протягивать информационные провода. Производитель подчеркивает легкость получения видео с камеры, требующего подключения к сети Интернет и регистрации устройства в личном кабинете SpaceCam. После этих действий становится доступным просмотр.

Указывается возможность передачи прав просмотра камер родственникам, друзьям, коллегам. Производитель отмечает, что подключение к личному кабинету облачного сервиса SpaceCam осуществляется с помощью защищенного соединения https, а на сервере видео хранится в зашифрованном виде. Заявляется, что использование сервиса SpaceCam для хранения архива защищает видео от злоумышленников, обеспечивая его сохранность. Указывается возможность размещения видео с камеры на сайт простым копированием кода. Производитель заявляет, что предлагает клиентам гибкие тарифы, позволяющие выбрать оптимальное время хранения архива. Отмечается, что сервис облачного видеонаблюдения SpaceCam позволяет осуществлять видеонаблюдение через Интернет в режиме онлайн, с камеры, из любой точки планеты, выбирать интересующий отрезок времени в архиве записей и скачивать его на персональный компьютер, быстро находить нужный участок архива, воспользовавшись графиком активности.

В платных тарифах доступна запись и воспроизведение архива в облаке. Указывается, что в течение 180 дней с момента первого добавления камеры в личный кабинет в облаке SpaceCam будут храниться записи за последние 48 часов. ■

Таблица 1. Характеристики камер

Камера	CamDrive	D-Link	MICRODIGITAL	SpaceCam
Разрешение, Мпкс	1	1	2	1
Частота кадров, кадр/с	25	25	25	10
Датчик/детектор движения	Датчик и детектор	Детектор	Детектор	Детектор
Динамик	Да	Да	Вход для внешнего	Нет
Wi-Fi	Нет	Да	Внешний	Да
Питание	5 В	USB 5 В	12 В, PoE (опция)	USB 5 В
Стоимость, руб	5,9	9,5	9	6,5

Таблица 2. Возможности облачного сервиса

Сервис	CamDrive	Mydlink	Veedo	SpaceCam
Запись в облачный архив	Да	Да (пробный период)	Да	Да
Глубина архива, дней	14–56	1	0–7	0–28
Запись на карту памяти	Да	Да	Нет (есть слот)	Нет (есть слот)
Настройки камеры	Расширенные настройки	Базовые настройки	Расширенные настройки (через интерфейс камеры)	Базовые настройки
Число подключаемых камер	Не ограничено	99 (запись в облако одновременно с 3 камер)	Не ограничено (1 камера бесплатно)	Не ограничено
Просмотр с мобильных телефонов	Да	Да	Да	Да
Оплата облачного хранения в месяц за 1 камеру, руб.	175–1100 (бесплатно первые 7 дней)	Бесплатно (пробный период)	300–1000	300–500 (бесплатно первые 48 дней)

Результаты испытаний

Можно отметить, что горизонтальное разрешение камер при съемке в черно-белом режиме со включенной ИК-подсветкой уменьшается в среднем на 8% по всем камерам. Скорее всего, в реальных условиях эксплуатации этого даже не будет заметно (рис. 1).

Вместе с падением разрешения при ночной съемке закономерно уменьшается и величина потока с видеокамер в среднем на 3%. А это говорит о том, что поток с камер ночью при одинаковых условиях будет примерно таким же. Конечно, если будет присутствовать движение в кадре, результат может изменяться. Характерно также, что наличие в камере настройки величины потока позволяет снизить битрейт камер почти в два раза (рис. 2).

По результатам измерения угла обзора камер видно, что в целом реальный угол обзора достаточно близок к заявленному. Некоторые производители ТТХ-камер даже указали значение меньшее, чем то, которым реально обладает камера. В итоге среднее различие составило 6% (рис. 3).

В ходе тестирования встроенных микрофонов камер было обнаружено, что средний порог громкости звука, при котором речь различима на фоне шумов в помещении, составляет -11 дБ. А это значит, что камера услышит человека, говорящего примерно в четыре

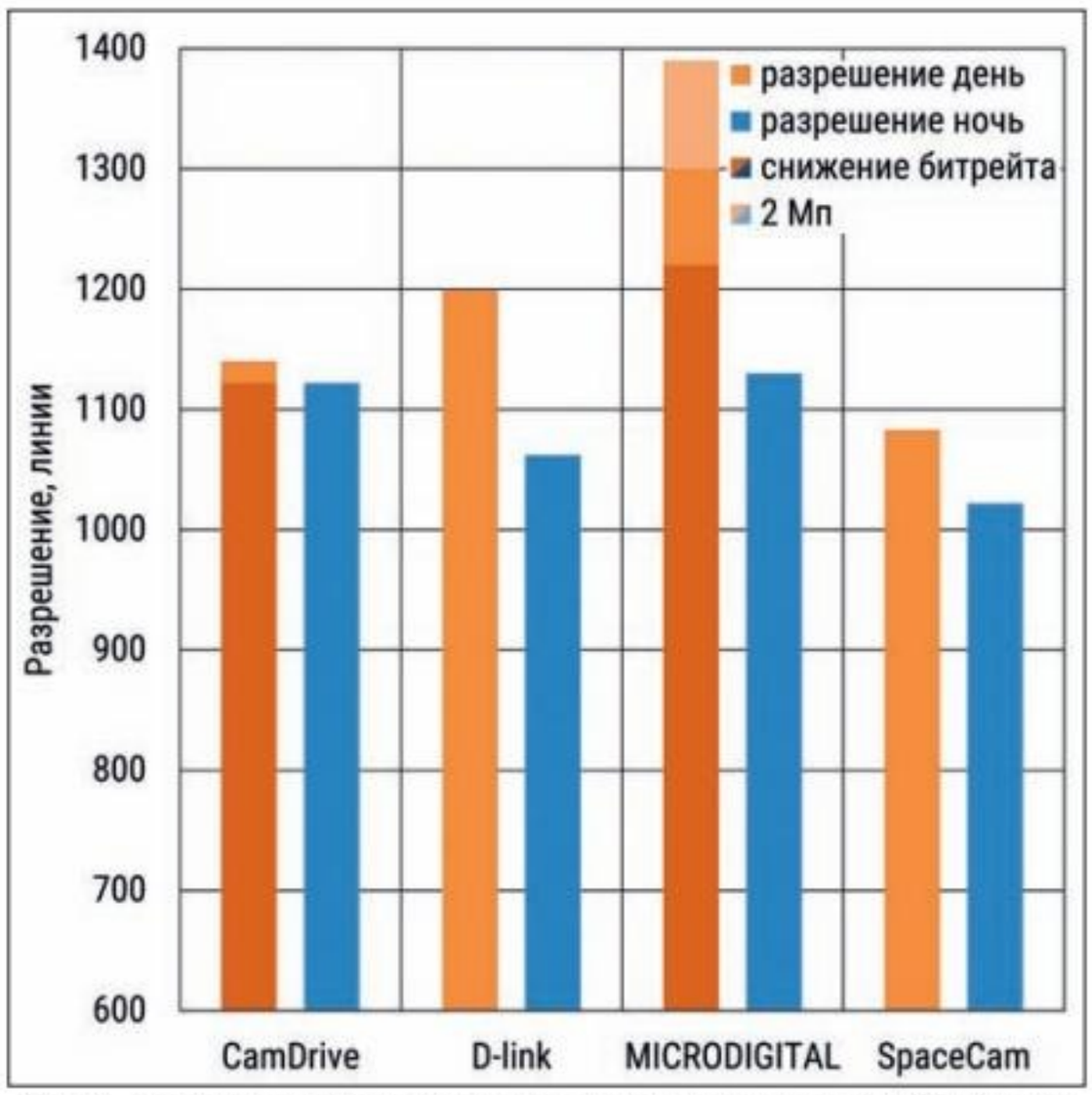


Рис. 1. Горизонтальное разрешение камер при съемке при 500 лк и при освещении только от встроенной подсветки камеры (больше – лучше)

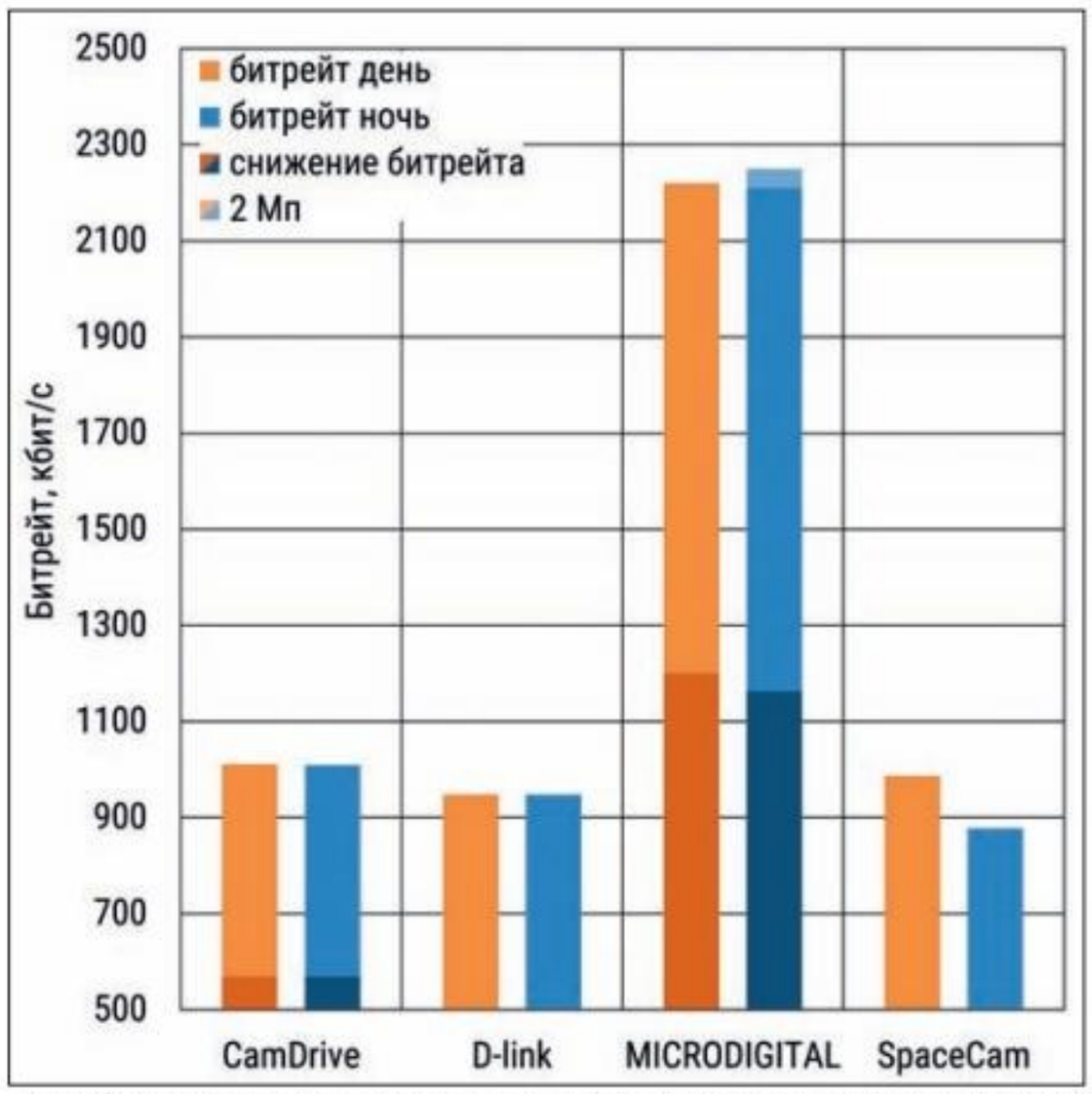


Рис. 2 Битрейт камер при съемке при 500 лк и при освещении только от встроенной подсветки камеры (меньше – лучше)

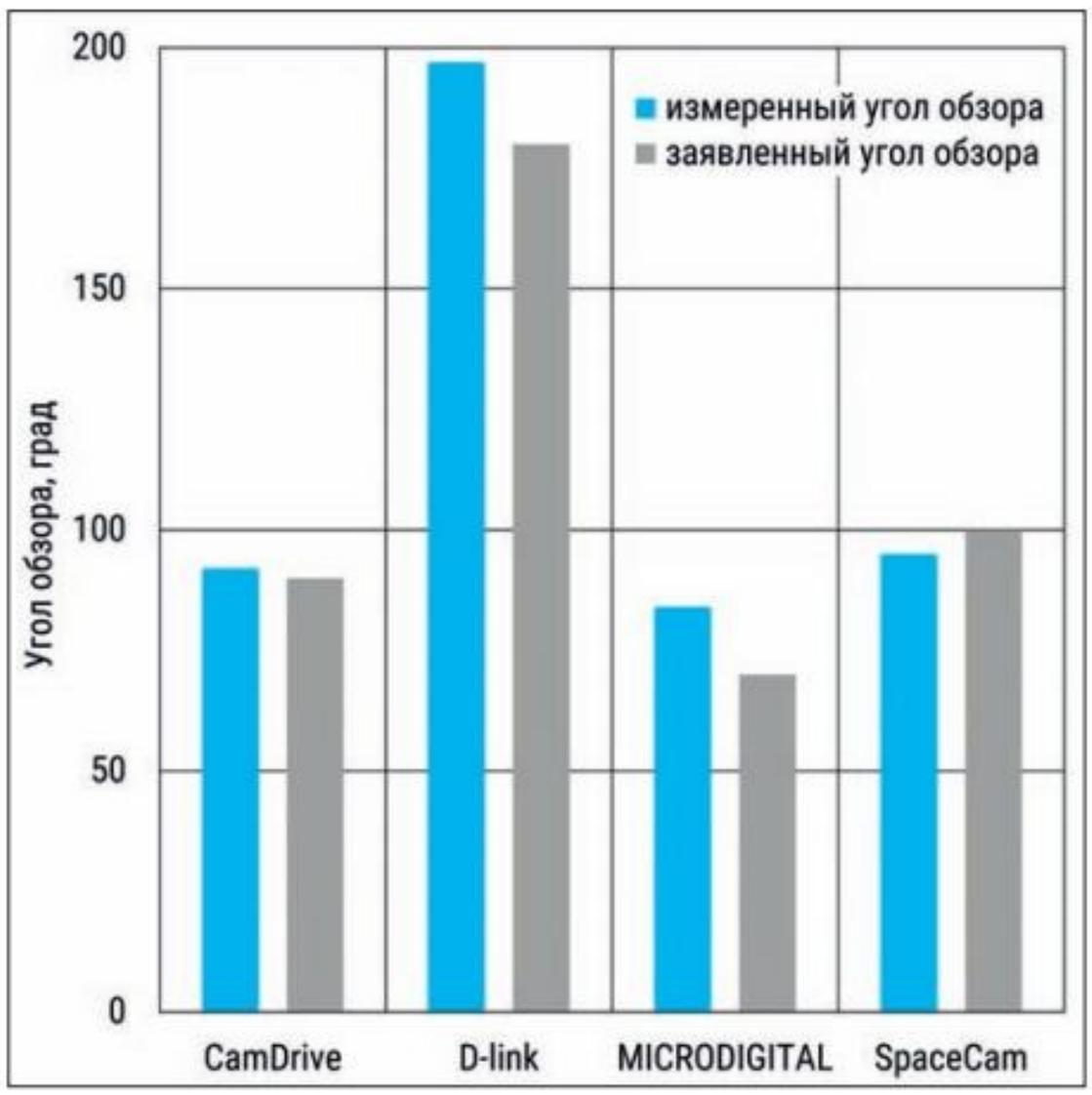


Рис. 3. Измеренный и заявленный горизонтальные углы обзора

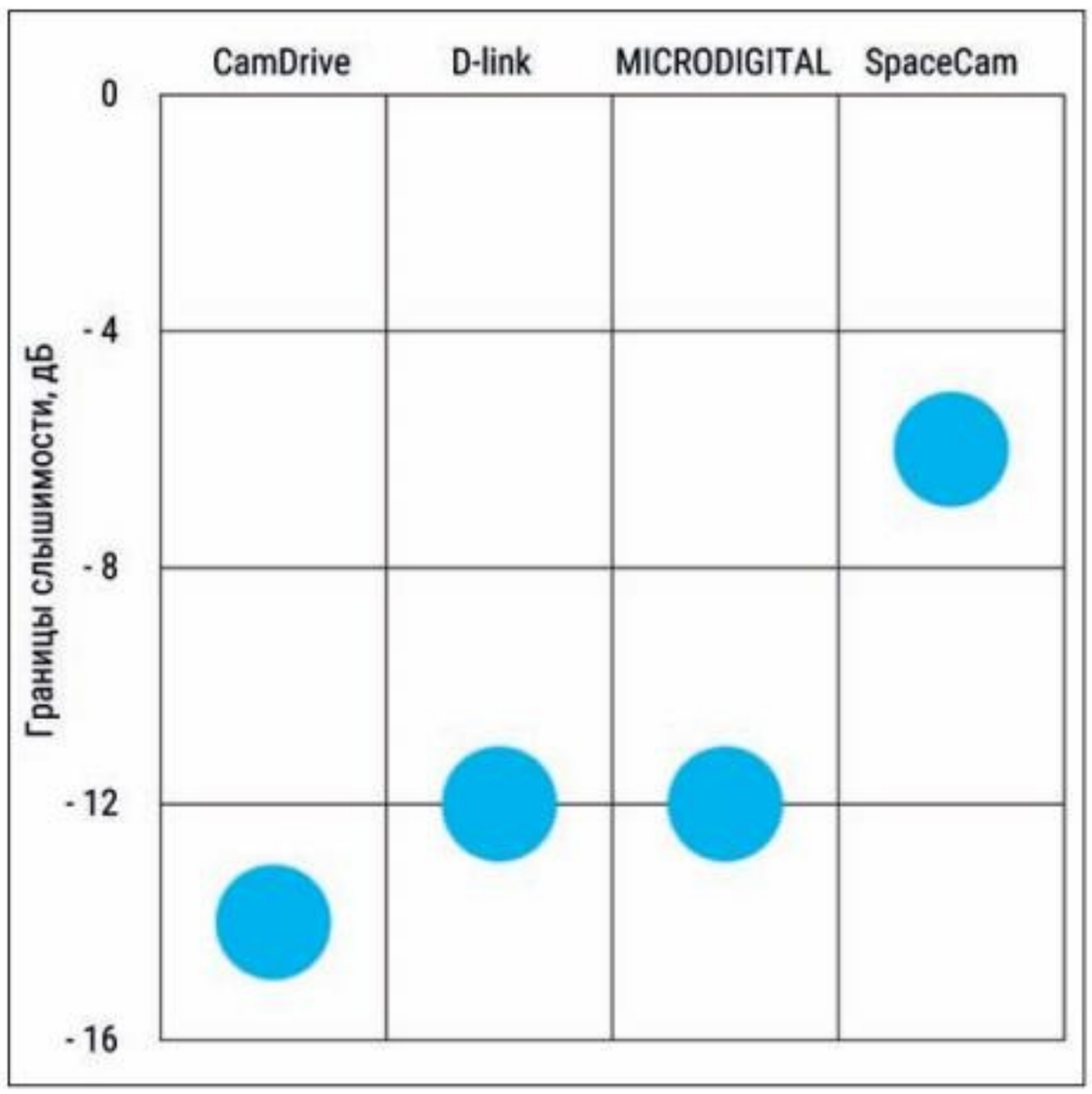


Рис. 4. Предел слышимости голоса на уровне шума (меньше – лучше)

раза тише уровня звукового шума в помещении (с точки зрения звукового давления, рис.4).

Заключение

В результате исследований было наглядно продемонстрировано, что считающиеся простыми Cube-камеры имеют достаточные характеристики для обеспечения не только видеонаблюдения, но и звукового мониторинга обстановки в помещении (включая ночной контроль, при наличии встроенной ИК-подсветки в камере).

Применение облачных технологий в подобных моделях позволяет еще больше упростить их использование и в некоторых случаях сделать эти камеры реальной альтернативой организации видеосервера на предприятии. Ведь большое число задач по обслуживанию камер перекладывается на плечи самих производителей. Все данные становятся легкодоступными для клиента из любого места и хранятся либо на самой камере, либо на удаленном сервере.

Применение в видеонаблюдении облачных технологии вкупе с Cube-камерами позволяет облегчить процесс монтажа и обслуживания камеры и добиться характеристик, близких к уровню более профессиональных моделей

Подводя итоги: можно порекомендовать облачные компактные камеры тем, кому требуется готовое решение, не требующее каких-то дополнительных действий со стороны инсталлятора или позволяющее при монтаже вообще обойтись силами своих сотрудников. Популярная и эффективная идеология Plug and Play во всей своей красоте. ■

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

DSSL
первоисточник видеонаблюдения

Российский производитель
систем видеонаблюдения

TRASSIR
ЭКОСИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

РЕШЕНИЯ* ДЛЯ РИТЕЙЛА

СОКРАЩЕНИЕ КРАЖ
на кассах магазина

БИЗНЕС АНАЛИТИКА
передвижений посетителей

РАСПОЗНАВАНИЕ
и определение лиц

Закажите бесплатную демонстрацию TRASSIR**

+7 (495) 104-20-71
www.dssl.ru/RETAIL

* Для видеонаблюдения и повышения безопасности с помощью интеллектуальных модулей: контроля кассовых операций, бизнес-аналитики (подсчёт посетителей, наполненность полок товаром, детектор очередей), распознавания лиц.
Полный список модулей Вы можете найти на сайте **www.dssl.ru/RETAIL**

** TRASSIR - одно из лучших ПО для видеонаблюдения!

ТЕСТ

Мобильные регистраторы для транспорта: в поисках идеального варианта

Вопрос обеспечения безопасности на транспорте в наши дни становится все более актуальным. Видеорегистраторы для транспорта используются прежде всего в следующих областях: инкассаторские автомобили, пассажирский и грузовой автотранспорт, сельскохозяйственный и железнодорожный транспорт, метрополитен, транспорт МВД и МО, спортивные автомобили, специальный и морской транспорт. Именно представители этих отраслей являются основными заказчиками мобильных многоканальных систем видеорегистрации.

Для чего нужна видеофиксация?

Перечислим основные цели, для которых используют мобильные регистраторы на транспорте.

Во-первых, это контроль за обстановкой снаружи и внутри транспортного средства, а также контроль за действиями водителя. Очевидно, что использование устройств видеонаблюдения повышает объективность и оперативность при расследовании происшествий и разрешении любых конфликтных ситуаций.

Во-вторых, наличие видеорегистратора на транспортном средстве помогает обеспечить безопасность перевозки пассажиров и сохранность грузов.

В третьих, видеофиксация способствует выявлению виновности/невиновности водителя при каких-либо происшествиях.

Требования к мобильным регистраторам

Автомобильная техника и мобильный регистратор для транспорта в особенности должны быть устойчивы к воздействию ударов, вибраций, низких и высоких температур, высокой влажности,

Тестирование проведено и предоставлено компанией DSSL

бросков питающего напряжения и т.д. Зачастую критически важными могут стать минимальный размер и вес устройства, а иногда одним из основных критериев выбора устройства может быть длительное время видеозаписи. Выгрузка данных из регистратора должна производиться по возможности быстро. И большим преимуществом будет, если это можно сделать бесконтактным способом (например, с помощью передачи данных по беспроводной сети).

Важно, чтобы производителем была предусмотрена и возможность удобного физического изъятия носителя информации (HDD, SD-карты и т.д.) и/или самого регистратора. Иногда требуется осуществлять удаленный онлайн-мониторинг, что влечет за собой необходимость создания некоего канала передачи данных с весьма значительной пропускной способностью.

Существенным преимуществом станет и наличие синхронизации с оборудованием автомобиля. Например, возможность начать/остановить видеозапись при запуске/выключении двигателя и т.д.

Виды мобильных регистраторов

Существуют аналоговые, IP- и гибридные модели мобильных регистраторов для транспорта. У каждого из этих типов оборудования есть свои плюсы и минусы.

Аналоговые видеорегистраторы

Безусловным преимуществом аналоговых видеорегистраторов, или DVR (Digital Video Recorder), является то, что они позволяют использовать аналоговые видеокамеры, что ведет к существенной экономии бюджета.

IP-видеорегистраторы

IP-видеорегистраторы, или NVR (Network Video Recorder), представляют собой более прогрессивные устройства, обладающие значительными преимуществами. К недостаткам этого типа оборудования стоит отнести более сложную настройку, а также тот факт, что они создают высокую нагрузку на локальную сеть. При этом поиск и устранение неисправностей в IP-оборудовании для видеонаблюдения представляет собой гораздо более сложный и ресурсоемкий процесс.

Гибридные регистраторы

Гибридные регистраторы представляют собой некий компромиссный вариант, позволяя работать одновременно как с цифровыми, так и с аналоговыми камерами. Такие решения интересны прежде всего своей гибкостью и тем, что они предоставляют возможность комбинировать различные типы оборудования между собой.

Следует обратить внимание и на тот факт, что данный тип оборудования представляет собой узкоспециализированные устройства. Получить его на тестирование оказалось непростой задачей.

Заказал – получил

В настоящий момент на российском рынке присутствует ограниченное количество моделей мобильных регистраторов, предназначенных для применения на транспорте. Это объясняется тем, что многие модели относятся производителями по тем или иным причинам к категории проектных решений. Это означает, что данное оборудование поставляется исключительно под заказ.

Именно данным обстоятельством и обусловлен тот факт, что в настоящем обзоре принимают участие лишь три модели мобильных регистраторов.

Мы надеемся, что в ближайшем будущем ситуация изменится в лучшую сторону и получить устройство и провести тестирование будет гораздо проще.

Hikvision DS-MP7508GLFWI

Оборудование предоставлено компанией DSSL

Hikvision DS-MP7508GLFWI – это абсолютно новая модель от известного производителя, и к нам в руки попал тестовый образец. Сразу отметим, что видеорегистратор от компании Hikvision – самый большой и самый тяжелый по сравнению с другими моделями, принимающими участие в нашем обзоре.

Большой алюминиевый корпус устройства надежно защищает расположенную внутри него электронику и имеет простое крепление. Корпус

Виброзащита жесткого диска в регистраторе Hikvision

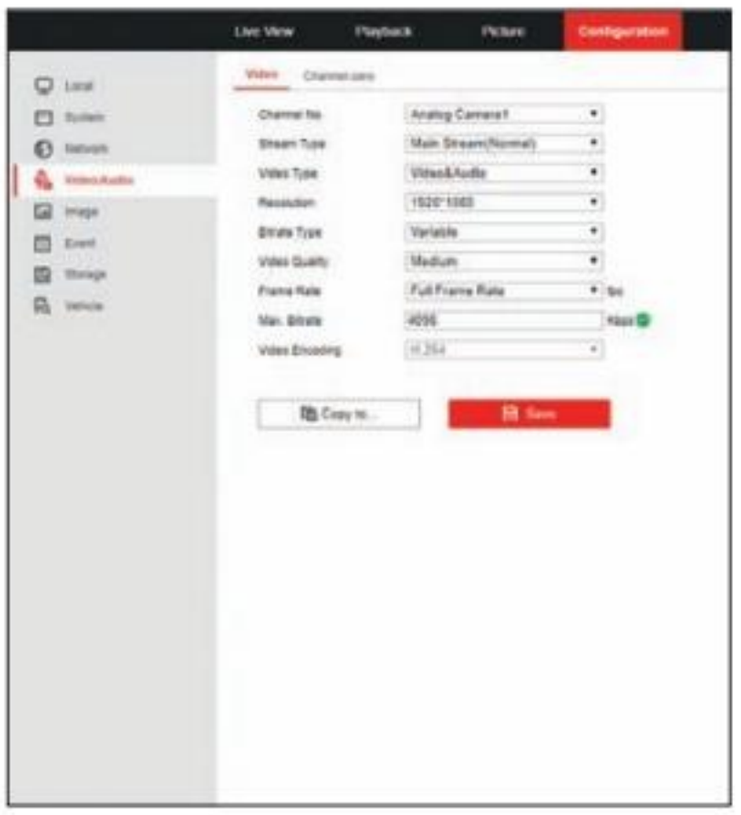
регистратора не имеет никакой виброзащиты. Однако это вовсе не означает, что в данной модели она отсутствует. Виброзащита в Hikvision DS-MP7508GLFWI присутствует именно там, где она крайне необходима – крепление жесткого диска имеет резиновые амортизаторы и позволяет гасить вибрации.

Тестируемая модель поддерживает установку двух жестких дисков (как обычных HDD, так и SSD) формата 2,5", причем контейнер с дисками является быстросъемным. Интересной особенностью устройства является то, что на задней стенке контейнера для дисков, помимо необходимых разъемов SATA и питания, имеется разъем для подключения провода USB 3.0. Таким образом, у вас есть возможность быстро подключить жесткие диски к компьютеру и сразу просмотреть все записанные данные. Для этого достаточно вынуть жесткие диски из регистратора и подключить их к ПК или ноутбуку через USB-порт. Максимальный поддерживаемый объем жесткого диска составляет 1 ТБайт. Регистратор оснащен также слотом для карты памяти формата SD. Поддерживается работа с картами объемом до 128 Гбайт.

Hikvision DS-MP7508GLFWI – это аналоговый регистратор. Он предоставляет возможность подключить до восьми камер стандарта HD-TVI либо камеры стандартного разрешения 960H. Максимальное поддерживаемое разрешение – 1080p. Особенностью этой модели является то, что подключение камер происходит через специальные разъемы, поэтому вам потребуется переходник на BNC. Питание видеорегистратора осуществляется от системы электропитания

автотранспорта. Данная модель потребляет до 20 Вт, от 8 до 36 В постоянного тока, выходное напряжение 12 В – 2 А либо 5 В – 1 А. Камеры, установленные в автотранспорте, получают питание от самого регистратора. Это является плюсом, поскольку избавляет от необходимости прокладывать лишние провода.

Как и положено современному мобильному видеорегистратору для транспорта, Hikvision DS-MP7508GLFWI имеет GPS-модуль с выносной антенной. Это позволяет привязывать видеозаписи к координатам на маршруте следования автотранспорта, что может оказаться крайне полезным при проведении расследования какой-либо ситуации. Модель от Hikvision также оснащена Wi-Fi-модулем. Съемные антенны идут в комплекте поставки. Важной особенностью является то, что регистратор может как принимать, так и раздавать Wi-Fi-сигнал. Таким образом, он может выступать в качестве точки доступа, раздавая сеть. В пути следования автотранспорта возможна передача данных по Интернету. Благодаря установленному 3G/4G-модулю имеется два слота для SIM-карт.



Интерфейс регистратора Hikvision. Настройка камер

3g-4g модуль в регистраторе Hikvision

Интерфейс регистратора Hikvision. Настройки Wi-Fi

Интерфейс регистратора Hikvision. Просмотр камер

Еще одним плюсом является то, что регистратор Hikvision интегрирован в программное обеспечение для видеонаблюдения TRASSIR. Это может существенно облегчить процедуру синхронизации архивов и предоставление доступа к ним.

Представим ситуацию, когда после рейса или смены автотранспорт возвращается в точку дислоцирования. В этом случае, как только транспортное средство приезжает на место базирования, регистратор попадает в зону действия Wi-Fi-сети и синхронизация архива регистратора и общей базы видеонаблюдения на TRASSIR происходит автоматически. Такой подход существенно экономит время и одновременно повышает надежность системы безопасности.

Помимо прочего, регистратор оборудован G-сенсором. Это датчик, позволяющий создавать тревожные события при нестандартном движении либо поведении автотранспорта или при аварии. Настройки чувствительности сенсора производятся в интерфейсе регистратора. На самом устройстве присутствуют разъемы тревожных входов-выходов.

Терминал служебной связи, подключенный к регистратору, позволит записывать переговоры водителя с пассажирами или по рации, а также синхронизировать эти данные с видеозаписями.

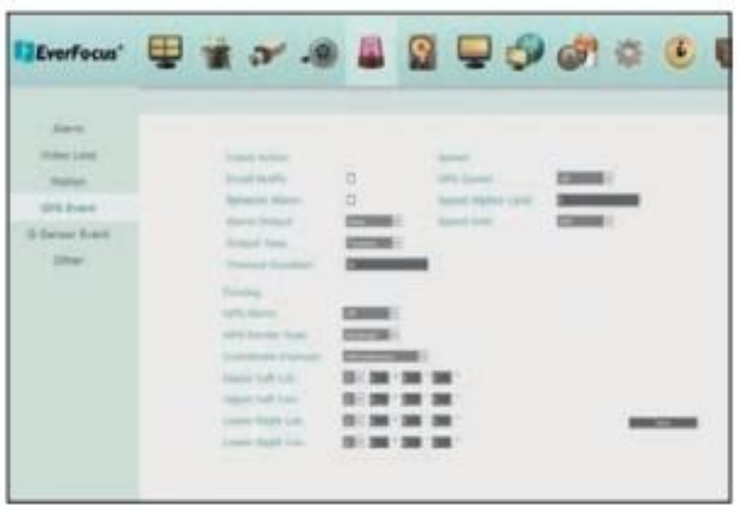
EverFocus EMV400 FHD

Предоставлен компанией ООО "Видау СБ"

Первое, что бросается в глаза, когда берешь в руки регистратор от компании EverFocus, – это специальное крепление с металлорезиновыми стойками для защиты от вибрации. Крепление жесткого диска не имеет дополнительных амортизаторов. Поддерживаются диски размером 2,5" HDD или SSD объемом до 4 Тбайт. Есть слот для SD-карты объемом до 128 Гбайт. Карта может работать и как архив, и как запись по тревогам.

К регистратору можно подключить до четырех аналоговых камер, разрешением до 1080P. Поддерживается формат AHD и стандарт PAL/NTSC 960H. Коммутация осуществляется с помощью жгута проводов типа "косичка", которая имеет стандартные BNC-разъемы и подключается к видеорегистратору через авиационный разъем M12. Суммарная скорость записи на все каналы составляет 100 кадр/с. Регистратор поддерживает два потока (main, sub). Помимо видеосигнала, регистратор позволяет подключить и четыре аудиоканала через разъемы RCA.

Интерфейс EverFocus EMVV400FHD. Настройка G-Сенсора



Интерфейс EverFocus EMVV400FHD. Настройка Тревожных событий

Интерфейс EverFocus EMVV400FHD. Основные настройки камер

Интерфейс EverFocus EMVV400FHD. Просмотр камер

Имеется функция UTC, настройка меню камер по коаксиальному кабелю.

Как и положено автомобильному регистратору, модель имеет 3-осевой G-сенсор. Он позволяет создавать тревожные события в тот момент, когда с автомобилем случается какая-то нештатная ситуация, например резкая остановка, нетипичный для транспорта крен кузова и т.д. Есть индивидуальная настройка этого сенсора.

Помимо этого модель снабжена контролем температуры – имеется два нагревателя, что позволяет регистратору работать в температурном диапазоне от -20 до +50 °C. Имеются тревожные входы и выходы (4/2). Есть также возможность подключить цифровые интерфейсы управления через порты RS 485 и RS 232.

Модель поддерживает работу модулей 3G/4G, GPS, Wi-Fi, которые поставляются опционально. Имеется поддержка модулей GPS/Глонасс, Galileo/QZSS/Beidou. Подключив модули беспроводной связи и GPS-модуль, можно настраивать тревожное событие, которое будет наступать при выходе из заданной зоны. Все настройки происходят через программный интерфейс. Допустим, транспорт курсирует по определенному маршруту и только в предопределенной зоне. Настраиваются координаты допустимых параметров, и как только автотранспорт покидает зону, обозначенную оператором, создается тревожное событие и происходит уведомление диспетчера. Как и положено, вариантов создания событий множество, делаются скриншоты, начинается запись, отправляются уведомления и т.д.

Регистратор имеет широкий диапазон бортового питания от 9 до 36 В, энергопотребление составляет 20 Вт при максимальной нагрузке 60 Вт. Помимо прочего, для питания камер, установленных в салоне, можно организовать питание от самого регистратора, что избавляет от необходимости тянуть силовые кабели к камерам от общей сети автомобиля.

Устройство имеет два видеовыхода для подключения монитора – VGA, а также и видеовыход BNC-разъем.

На передней панели регистратора имеются три порта USB, к ним можно подключить периферийные устройства – мышь, клавиатуру для настройки регистратора, а также флеш-накопитель, внешний жесткий диск для экспорта архива. Обеспечивается полный доступ по Web-интерфейсу к настройкам регистраторов и получение потока RTSP по каждому каналу.

EvefFocus ACE-DM1204AT

Предоставлен компанией ООО "Видау СБ"

Автомобильный регистратор ACE-DM1204AT принципиально отличается от моделей, о которых мы говорим в рамках нашей статьи. Прежде всего – размерами. С одной стороны, это плюс: он сопоставим с блоком автосигнализации и не занимает слишком много места. С другой стороны, платой за небольшие размеры стало отсутствие возможности установки жесткого диска. Запись происходит на карту памяти объемом до 2 Тбайт, также есть возможность подключить флеш-накопитель через порт USB.

Теперь о самом главном. К этому "малышу" можно подключить четыре IP-камеры разрешением FullHD и четыре аналоговые камеры формата TVI, AHD, PAL/NTSC 960H с максимальным разрешением 1080P, получается, что он 8-канальный. Причем записывает видеопоток со скоростью 25 кадр/с. Есть возможность управления PTZ-камерами, все как у "больших товарищей", и UTC-настройка меню камер по коаксиальному кабелю.

Несмотря на то что регистратор не имеет никакой виброзащиты, его корпус фиксируется в автомобиле саморезами или винтами, производитель гарантирует виброустойчивость: 5~500 Гц 2,7G – параметр, ничем не уступающий двум другим моделям нашего обзора. Устройство снабжено гидроустойчивыми разъемами.

Интерфейс ACE1204FT

Регистратор может похвастаться наличием GPS-модуля, поддерживаются также Глонасс, Galileo/QZSS/Beidou, антенна идет в комплекте. Записанное видео будет привязываться к GPS-точкам, что облегчит поиск видео в архиве. Помимо этого есть возможность настроить тревожное событие на превышение скорости, которая определяется также по GPS, и в случае увеличения скорости больше допустимой нормы может создаваться тревожное событие и отправляться в центр мониторинга или на базу. Причем благодаря 3G/4G-модему данные о тревожных событиях могут поступать в реальном времени. Модем подключается к USB-порту, регистратор поддерживает такие девайсы. Помимо тревожных событий, предоставляется возможность мониторить ситуацию внутри автотранспорта в реальном времени. Производитель предлагает использовать мобильные приложение для IOS- и Android-смартфонов и Mac OS. Поддерживается максимальное подключение восьми клиентов, лишь бы сетевой канал позволил. Через порт USB также может осуществляться поддержка мониторов Touch Screen. Что касается мониторов, то подключить их можно используя VGA-выход или через BNC-разъем.

Модель, помимо видеоканалов, может подключить один аудиоканал, который также может писаться в архив. Имеется два тревожных входа и один тревожный выход, к которым подключается периферийное оборудование.

Наличие G-сенсора – это норма для видеорегистраторов такого рода, и тут производитель не забыл про него, причем сенсор имеет индивидуальные настройки. Произвести все настройки регистратора и G-сенсора можно как через встроенный интерфейс, используя монитор, так и через Web-интерфейс, доступ к которому осуществляется по сети. Регистратор имеет Ethernet-разъем и способность работать в сети со скоростью 100 Мбит/с.

Интерфейс ACE1204FT. Меню настройки допустимой скорости транспорта

Интерфейс ACE1204FT. Меню настройки параметров камер

Устройство подключается на автомобильную информационную CAN-шину и может записывать показатели приборов на видео.

Устройство оборудовано нагревателем, и его рабочие температуры составляют от -15 до +50 °C. Питается прибор от сети автотранспорта от 12 или 24 В. Поддержка питания камер от регистратора тут опциональная. Зато максимальное потребление его составляет всего 10 Вт.

Сравнение характеристик камер с моторизированным объективом

	Hikvision DS-MP7508GLFWI	EverFocus EMV400 FHD	EvefFocus ACE-DM1204AT
Максимально возможное разрешение записи	FullHD	FullHD	FullHD
Поддерживаемые форматы	TVI/CVBS	AHD/CVBS	TVI/AHD/IP/CVBS
Скорость записи при максимальном разрешении	25 кадр/с	26 кадр/с	27 кадр/с
Количество каналов	8	4	4 аналоговых, 4 IP
Наличие виброзащиты	Защита жестких дисков	Есть	Нет
Количество жестких дисков	2	1	Нет
Максимальная емкость HDD	1 Тбайт	4 Тбайт	Поддержка карт памяти SD до 2 Тбайт
Количество портов USB	2 USB 2,0, 1 USB 3,0	3 USB 3,0	2 USB 2,0
3G/4G-модуль	Есть	Опционально	Поддержка USB-модели
Wi-Fi-модуль	Есть. Прием и передача	Опционально	Нет
Количество тревожных входов/выходов	4/2, RS232, RS422	4/2, RS232, RS485	2/1 RS485, RS232
Диапазон питания	9–32 В	9–32 В	12,24 В
Питание камер от регистратора	Есть 12 В	Есть 12 В	Опция
Температурный диапазон, °С	-20...+60	-20...+55	-15...+50
Дополнительные параметры	Гигабитный Ethernet Может раздавать Wi-Fi-сигнал Выходное питание камер 12 и 5 В	Гигабитный Ethernet Может раздавать Wi-Fi-сигнал Выходное питание камер 12 и 5 В	Есть мобильное приложение Маленькие размеры Есть подключение к CAN-шине автомобиля

Заключение

Все представленные в нашем обзоре модели – абсолютно разные решения. Они обладают разным функционалом и относятся к разным ценовым категориям. А самое главное – подразумевают совершенно разные сценарии использования. Поэтому сравнивать их друг с другом, что называется, "в лоб" будет не совсем корректно.

Однако некоторые выводы сделать все же можно.

Несколько лет назад мы уже делали обзор мобильных регистраторов для транспорта. В то время все участвующие в обзоре устройства были построены на базе обычного стационарного оборудования для видеонаблюдения и могли называться решением для транспорта весьма условно.

Но прогресс не стоит на месте, и мы можем наблюдать эволюцию данного типа устройств.

Сейчас представленные на рынке модели можно назвать полноценными мобильными регистраторами для транспорта. Они изначально изготавливаются для применения именно в этой области. Производители устройств подходят к их разработке более осознанно и продуманно и учитывают специфику их использования.

В оборудовании применяются качественные коннекторы, устойчивые к вибрациям. Использование таких разъемов позволяет предотвращать выпадание штекеров, ведущее к пропаданию видеосигнала. Для этих целей большинство производителей используют надежные авиационные разъемы M12.

Поддержка питания камеры непосредственно от видеорегистратора стала уже скорее нормой, чем исключением из правил, для всех серьезных производителей оборудования для видеонаблюдения на транспорте.

В ходе тестирования мы столкнулись и с одним довольно странным моментом, логическое обоснование которому нам, честно говоря, трудно подобрать.

Дело в том, что все участвующие в обзоре производители по какой-то неведомой причине до сих пор поставляют ПО для своих устройств в виде CD-диска (!), идущего в комплекте поставки. В наше время повсеместного использования Интернета и быстрых темпов устаревания программного обеспечения и внесения изменений в него такое решение выглядит несколько странным, чтобы не сказать архаичным и устаревшим. Пора уже отправить его на заслуженный отдых и использовать более современные решения, идя в ногу со временем. Это, пожалуй, единственный момент, которых вызвал у нас некоторое недоумение.

В целом прогресс в области мобильных регистраторов для транспорта налицо, что не может не радовать. И хотя мы убедились, что идеальной системы видеорегистрации для транспорта на данный момент не существует, каждый вполне может подобрать устройство под свои нужды, учитывая все плюсы и минусы, а также отталкиваясь от стоящих задач и имеющегося бюджета.

А пока будем продолжать следить за развитием рынка мобильных регистраторов для транспорта и ждать появления нового суперустройства, которое соединит в себе все лучшее и станет идеальным решением! ■

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

КОЛОНКА РЕДАКТОРА

Транспорту не хватает превентивной безопасности

Современный мир пропитан скоростью и движением: нас много, мы спешим, нам нужно везде успеть. Поэтому транспорт, общественный и личный, – обязательный атрибут общества. А для самого транспорта неотъемлемые атрибуты – это пробки, теснота, нервозность, потеря личной зоны комфорта и уязвимость.

Увы, сама природа движения предполагает немало опасностей и угроз, и вот почему системы безопасности для транспорта становятся все более актуальными и важными. Видеокамер на российском транспорте все больше – и в городских автобусах, троллейбусах, трамваях, и в пригородных электричках. И везде ситуация с безопасностью становится лучше – вандалы и хулиганы оперативно задерживаются или находятся по горячим следам, пассажиры чувствуют себя все уютнее и спокойнее. Конечно же, те пассажиры, которые оплатили проезд, ведь теперь и билетные контролеры на транспорте используют видеонаблюдение – персональные видеорегистраторы. Благодаря персональному видеонаблюдению контролеров уровень конфликтов на транспорте снижается, а уровень оплаты проезда неуклонно растет.

И вроде бы все хорошо: транспорт оснащается, пассажиры под защитой, правда торжествует. Но чего же не хватает? Превентивной безопасности!

Видеонаблюдение, которому в России уже более 20 лет, чаще всего так и остается средством "разбора полетов". А ведь множество детекторов и алгоритмов оценки происходящего в кадре уже разработано, технологии передачи видео по беспроводным каналам позволяют контролировать ситуацию на транспорте в удаленных центрах мониторинга. Операторы в таких центрах могли бы моментально реагировать на происходящее, например направлять медиков или полицейских на место чрезвычайной ситуации. И обслуживание таких центров при грамотной организации стоило бы весьма разумных денег. Но, увы, на большинстве видов транспорта такой сервис не используется. Остается лишь надеяться, что организационные методы обеспечения безопасности станут успевать за техническими возможностями. Особенно в таком важном сегменте, как транспорт.

Евгений Ерошин

Редактор раздела All-over-IP,
директор по маркетингу ООО "БайтЭрг"

Ключевые отличия Stand-alone и мобильного видеонаблюдения,

или На что обращать внимание при выборе техники

Основные задачи видеонаблюдения – собирать видеоинформацию, оперативно передавать, отображать, записывать и автоматически реагировать на нее. И для мобильного, и для стационарного видеонаблюдения эти задачи едины. Но, в области технической реализации систем появляется много отличий, ведь требований к технике мобильного видеонаблюдения гораздо больше

Михаил Жирнов

Руководитель направления
цифровых систем видеонаблюдения
ООО "БайтЭрг"

Основные требования описаны в постановлении Правительства РФ от 26 сентября 2016 г. № 969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности". В дополнение к ним мы озвучим технические требования и особенности, накопленные за два десятка лет работы в области видеонаблюдения.

Для начала опишем условия эксплуатации мобильного видеонаблюдения: ограниченное пространство размещения техники, повышенные физические нагрузки – вибрация, тряска, возможные удары, расширенный температурный диапазон, а также перепады температур, удаленность мест формирования видеоданных от мест их получения и хранения. Все это накладывает особенные требования к системам мобильного видеонаблюдения.

Определим требования по типу оборудования.

Видеокамеры

Если для объектов стационарного видеонаблюдения существует разделение на два основных класса – видеокамеры уличного исполнения и видеокамеры для применения в помещениях, то для мобильного видеонаблюдения существует совершенно отдельный класс – видеокамеры транспортного исполнения.

Исходя из особенностей применения, они должны быть близки к камерам уличного исполнения, но с дополнительными свойствами:

- исполнение должно быть вандалоустойчивым ввиду того, что часто такие камеры устанавливаются в зоне досягаемости пассажиров;

Элементы управления для мобильных регистраторов – это чаще всего мышь и ИК-пульт, ввиду того, что малые габариты не позволяют размещать кнопки на корпусах. Для мониторинга состояний регистраторов используются расположенные на корпусе индикаторы

У внешних видеокамер должна быть хорошая герметичность

- крепление камер должно обеспечивать их четкую фиксацию, и камеры не должны быть подвержены повороту из-за тряски и вибрации;
- корпуса камер внешней установки должны иметь аэродинамический дизайн, оптические окна видеокамер должны обладать повышенной устойчивостью к механическим повреждениям от песка, пыли и пр., которые могут попадать в камеры при движении на скоростях;
- такой механический элемент видеокамер, как сдвижной ИК-фильтр, должен обладать повышенным ресурсом для использования на транспорте, либо необходимо использование фиксированного ИК-фильтра с технологией IR-pass для пропуска ИК-излучения в ограниченном "окне прозрачности";
- должна обеспечиваться повышенная герметичность внешних видеокамер, так как транспортные средства моются под высоким давлением и давление воды на порядок выше, чем давление, создаваемое дождем;
- согласно постановлению № 969 видеокамеры должны быть разрешением не менее 2 Мпкс.

Все это относится и к IP-видеокамерам, и к видеокамерам Analog-HD. Последние, кстати, незаменимы в случаях, когда видео с камер используется для контроля обстановки в режиме онлайн, ведь они транслируют видео без задержек, а в случае с IP-видеокамерами могут возникать задержки до нескольких секунд, которые неприемлемы, например, для водителя, начинающего движение.

Каналы связи

Основное требование к каналам связи (кабелям) – это возможность сохранять свои рабочие качества в условиях перепада температур и вибрации, а также повышенная механическая прочность. Дополнительно необходимо использовать соединительные разъемы с надежной фиксацией, с дополнительными замками и защелками.

Условия эксплуатации мобильного видеонаблюдения: ограниченное пространство размещения техники, повышенные физические нагрузки – вибрация, тряска, возможные удары, расширенный температурный диапазон, а также перепады температур, удаленность мест формирования видеоданных от мест их получения и хранения

Видеорегистраторы

Прежде всего нужно учитывать размеры, ведь в транспортных средствах зачастую немного места, куда можно установить системы видеозаписи. Далее следует виброзащита, которая реализуется и в креплении видеорегистратора, и в креплении отсека для накопителя данных. К накопителям данных тоже есть свои требования: желательно использовать специальные серии 2,5" твердотельных дисков без вращающихся элементов, которые могут оказаться "слабым звеном" в условиях мобильного применения. Однако даже применение таких дисков не всегда гарантирует устойчивую видеозапись, поэтому для повышения надежности рекомендуется технология двойного хранения, когда кроме HDD используются SD-карты, на которые осуществляется запись в случаях неготовности, повреждения или предварительного подогрева HDD.

Отсек с накопителем желательно должен дополняться системой вентиляции для использования видеорегистратора в условиях повышенных температур, сами отсеки установки носителей должны быть защищены от несанкционированного доступа и одновременно должны быть доступны авторизованному персоналу для оперативной замены носителей.

Для удаленного просмотра и передачи данных, включая видео, желательно оснащение регистратора модулями 3G/4G, для фиксации координат – модулями GPS/GNSS. В некоторых случаях, например для настройки, полезным окажется модуль Wi-Fi. Антенны приемников и передатчиков должны быть выносными, всепогодными и с надежной системой монтирования для размещения снаружи транспортных средств, так как часто требуется интеграция с другими подсистемами транспортного средства; желательно, чтобы регистратор имел порты и тревожные входы/выходы для такой интеграции. Для архивации данных полезны порты USB и E-SATA, для отображения данных – видеовыходы CVBS/VGA/HDMI.

Элементы управления для мобильных регистраторов – это чаще всего мышь и ИК-пульт, ввиду того, что малые габариты не позволяют размещать кнопки на корпусах. Для мониторинга состояний регистраторов используются расположенные на корпусе индикаторы.

Мониторы

Зачастую мобильные системы видеонаблюдения используются в режиме черного ящика, мониторы не применяются, а в случаях их использования основными требованиями являются компактные размеры, травмобезопасный дизайн и кронштейны для установки в транспортные средства. Иногда желательно наличие на мониторе козырька для мониторинга при солнечной засветке.

Резюме

Конечно, при внедрении мобильного видеонаблюдения на транспортных средствах заказчика могут появляться дополнительные требования, например сертификаты использования мобильного видеонаблюдения для конкретных моделей техники, принадлежащей заказчику. Чтобы успешно решить все вопросы, стоит обращаться за оборудованием и поддержкой в компанию с богатым опытом в этой области, а лучше непосредственно к производителям оборудования для мобильного видеонаблюдения. ■

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

КОЛОНКА ЭКСПЕРТА

Linux неизбежен

Исторически сложилось, что ПО для систем безопасности создавалось и развивалось в основном для Windows. Это была самая популярная и зрелая десктопная операционная система девяностых и нулевых. В то время у нее отсутствовали серьезные альтернативы, поскольку Linux активно использовался только в серверных решениях.

Однако в недавнем прошлом возникла идея пересмотреть этот подход. Связано это было прежде всего с санкционными угрозами для России. Переход на платформу Linux и особенно на российские ОС, созданные на ее основе, наиболее актуален для критически важных объектов. Это позволяет защитить их от коммерческого влияния компаний и корпораций, которые могут в любой момент попасть под санкции и будут вынуждены ограничить Россию в поставках технологий.

Уже появились ГОСТы в сфере транспортной безопасности, регламентирующие применение ОС с открытым исходным кодом. Но резкий и директивный переход на Linux будет скорее вреден, поскольку в одночасье целые отрасли могут быть отрезаны от новейших разработок. Несмотря на то что построенные на ядре Linux системы за последнее десятилетие получили серьезное развитие, в большинстве своем платформы безопасности под Linux пока еще отстают по возможностям от аналогичных платформ под Windows. Поэтому переход должен быть плавным.

Тем не менее этот переход – не только противостояние угрозам, но и естественный вектор развития технологий на рынке безопасности. Устройства становятся все более умными. Видеокамеры превращаются в открытые платформы для установки приложений независимых разработчиков. Уже появились NVR с элементами искусственного интеллекта. Перенос ресурсоемких вычислений с сервера на периферийные устройства позволяет строить выгодные для пользователя решения, но только в том случае, если сами эти устройства имеют адекватную стоимость. А это означает применение мобильных платформ, операционных систем Linux и кросс-платформенного прикладного программного обеспечения.

Для нас подобные разработки уже много лет являются приоритетными, и сейчас мы имеем продукты, легко портируемые на любые типы процессоров и ОС. Уже очень скоро эта задача станет чрезвычайно актуальной для всех производителей ПО.

Мурат Алтуев

Президент компании ITV | AxxonSoft

Современные технологии повышения скорости и надежности передачи данных через глобальные сети

С 2011 по 2014 г. независимое аналитическое агентство Vanson Bourne провело опрос среди топ-менеджмента более 1500 различных крупных организаций о том, какие факторы являются наиболее важными в процессе передачи данных как внутри предприятия, так и при взаимодействии с внешними контрагентами. Среди возможных вариантов ответов были такие, как безопасность, скорость передачи, объем передаваемой информации и сложность самой передачи

Георгий Забадаев

Руководитель направления компании IBM Aspera в России и СНГ

В результате проведенного опроса с очевидным отрывом лидировал показатель безопасности, однако очевидным явился тот факт, что скорость передачи данных демонстрирует наибольший рост от года к году.

Современные тренды

Повышение безопасности и скорости передаваемой информации соответствует всем трендам, которые наблюдаются в области передачи данных.

1. Распространение Big Data:
- 90% сегодняшних данных являются наборами файлов или неструктурированными массивами, которые не имеют явной связи друг с другом;
- вариативность размеров от килобайт до терабайт;
- повсеместный рост объемов.

2. Рост и вариативность IP-сетей:
- различная ширина каналов (от Кбит/с до десятков Гбит/с);
- увеличение пропускной способности и параллельное уменьшение стоимости;
- разнообразие сетей передачи данных (наземные, спутниковые, IP-Based и беспроводные);
- вариативность условий – влияние на производительности при изменении расстояния передачи.

3. Глобализация и аутсорсинг:
- географическое распределение команд (особенно актуально для России, где часто нескольким командам из разных городов нужно ежедневно обмениваться колоссальным количеством данных между собой, чтобы завершить проект);
- при увеличении расстояния происходит деградация сети, негативно влияющая на передачу контента;
- современные решения по ускорению TCP не рассчитаны на передачу Big Data и репликацию.

4. Развитие облачных технологий:
- широкий выбор (IBM SoftLayer, AWS, Microsoft Azure, OpenStack, Google, HDS);
- переход компаний из нишевых в масс-маркет – Netflix (транскодирование), MTV (глобальная дистрибуция видео), BGI (корпорация из Китая по геномному секвенированию), Sony Media Cloud Services (производственные процессы).

Фундаментальные сложности

Вышеуказанные тренды сопряжены с определенными сложностями, с которыми можно столкнуться при передаче данных.

1. Размер и количество информации. Серьезные затруднения с надежной передачей, обменом и синхронизацией больших файлов и массивов данных по WAN.

2. Скорость. Ограничение пропускной способности, количества потоков и скорости передачи данных.

3. Расстояние. Перегруженные публичные каналы передачи данных, неизбежная деградация производительности при увеличении расстояния.

4. Контроль. Необходимость в увеличении безопасности и прозрачности контроля при передаче файлов и массивов данных как сотрудникам и бизнес-партнерам, так и конечным потребителям, оптимизация без увеличения трафика и нагрузки на сеть.

Корнем всех проблем при передаче данных является использование традиционных подходов, от которого "страдают" практически все индустрии. Большой объем данных и их размер создают проблемы во многих отраслях промышленности:
- телеком-СМИ и развлечения. Необходимо эффективно распространять большие объемы медиаданных по растущей дистрибуционной сети;

Рис. 1. Большой объем данных и их размер создают проблемы во многих отраслях промышленности

- биологические науки. Трудности при распространении и доступе к постоянно обновляющимся комплектам Big Data (например, геномная информация, цифровые снимки);
- производство. Существенные временные затраты в рамках рабочих процессов, связанные с обменом проектными CAD- и дизайн-файлами между инженерами-проектировщиками, внешними подрядчиками и непосредственным заказчиком;
- разработка ИТ-приложений. Проблемы при поддержке территориально распределенной сети разработки, тестирования и обеспечения качества;
- нефтегазовая отрасль. Необходимо передавать огромные объемы данных, полученных при геологической разведке месторождений. До сих пор зачастую для доставки данных, полученных при бурении скважин, задействуется "специально обученный" человек, который забирает жесткий диск и на вертолете летит на континент, чтобы передать эти данные на анализ, что существенно замедляет рабочий процесс;
- финансовые услуги. Требуется постоянная синхронизация большого объема данных между географически удаленными точками, ежедневная отправка отчетности в регулирующие органы со сканами документов.

Даже обычные пользователи ежедневно сталкиваются с данными трудностями, когда, например, хотят скачать файл с удаленного файлового обменника или FTP.

Недостатки TCP и традиционных технологий

Давайте разберемся, в чем проблема традиционных технологий. На рис. 1 представлена взаимозависимость скорости передачи протоколов, использующих на транспортном уровне протокол TCP, и таких параметров, как время приема-передачи (Round-Trip Time) и процент потери пакетов. Очевидно, что чем дальше друг друга расположены источник и приемник данных, тем медленнее будет передаваться информация. К сожалению, мы не можем одним проводом обернуть Землю, поэтому необходимы пограничные маршрутизаторы и другие промежуточные точки, напрямую влияющие на производительность передачи данных.

Дело в том, что протокол TCP был спроектирован в 1973 г.: перед учеными поставили задачу разработать протокол, который сможет перенести ядерный удар. Требовалось создать протокол, который смог бы безопасно передавать данные. Поэтому при создании TCP основные усилия были направлены на создание механизма именно надежной, а не скоростной передачи. В те годы не было ни мобильных, ни спутниковых сетей, а единственный трансатлантический канал из США в Европу имел скорость 64 Кбит/с, что показывает состояние технологии на тот период. TCP был разработан так, что скорость передачи обратно пропорциональна расстоянию между конечными точками. Кроме того, в случае потери пакетов TCP считает, что канал перегружен, и самостоятельно уменьшает скорость передачи. Производительность TCP снижается с ростом расстояния передачи и из-за низкого качества сети. Чем больше расстояние, тем больше задержка, и тем ниже скорость передачи. Задержку обычно измеряют величиной Round-Trip Time (RTT). Это время, которое потребуется на отправку пакета и получение подтверждения от получателя. Задержка возникает из-за законов физики, ограничивающих скорость света или электромагнитного сигнала. Например, задержка при передаче по спутниковым сетям может достигать 800 мс. Более того, при передаче на большие расстояния по глобальной сети Интернет (WAN) пакет должен пройти через большое количество маршрутизаторов, прежде чем его получит адресат. Маршрутизатору требуется время на обработку пакета, а если он настроен неправильно или перегружен, может произойти потеря пакета. Чем выше количество потерянных пакетов, тем более затратной по времени становится передача. TCP, безусловно, имеет хорошую производительность в локальных сетях (LAN) относительно доступной пропускной способности сети, но при этом чем больше RTT и потеря пакетов, тем ниже будет производительность передачи.

Производительность протокола TCP также не растет с увеличением канала. Другими словами, если у вас медленная передача на канале в 10 Мбит/с, нет никаких гарантий, что при увеличении канала до 1 Гбит/с скорость вырастет. Конечно, если необходимо передать файл на соседнюю улицу, рост производительности будет заметен, но если стоит задача передать данные на большие расстояния, то увеличение канала до 1 Гбит/с мало чем поможет.

Альтернативные технологии передачи данных

Разумеется, TCP многократно пытались улучшать. Одну из последних реализаций подобного протокола представила корпорация Google, которая переделала механизм работы с окном (изменение размеров окна каждый раз, когда передаются пакеты), но получила повышение производительности лишь на 30% по сравнению с обычными традиционными протоколами, основанными на TCP.

Самой известной альтернативой TCP стали протоколы на базе UDP. Чистый UDP сам по себе – замечательный протокол передачи, однако не до конца эффективный, а самое главное – не предоставляющий гарантии доставки передаваемой информации. Все мы сталкивались с периодическими скачками изображения и артефактами при просмотре трансляции по Интернету – это происходит при потере некоторого количества пакетов при потоковой передаче.

Другими альтернативными подходами к оптимизации передачи данных являются технологии компрессии (Data Compression) и кеширования (Data Caching). Но их нельзя назвать действительно ускоряющими передачу, они ее только оптимизируют. Кеширование можно применять далеко не всегда – когда имеется большое количество одновременных потоков и при этом передаются разные данные, кеширование становится абсолютно бесполезным. Что касается компрессии, то известно, что сейчас очень много информации передается уже в сжатом виде, и никакого явного преимущества мы не получим.

Высокоскоростные протоколы передачи данных

Современные технологии способны повысить скорость передачи, в частности модифицированные UDP-протоколы с дополнительным уровнем надежности на прикладном уровне. Самыми популярными среди них являются Aspera FASP, File Catalyst и Signiant.

Идея этих протоколов заключается в том, чтобы свести к нулю два фактора, которые сильнее всего влияют на деградацию производительно-

сти при передаче данных, а именно Round-Trip Time и Packet Loss. Это было достигнуто за счет совершенно нового подхода к тому, как передаются данные, а именно – использования механизма подтверждения. Он заключается в том, что если какой-то пакет теряется при передаче, не нужно ждать подтверждение о том, получен он или потерян, можно приступать сразу к передаче следующего пакета, а потерянный пересылается в процессе, как только появляется некое окно. За счет этого мы можем высчитать теоретическую максимальную скорость, с которой передаются пакеты.

Важнейшими параметрами таких протоколов являются:

- настраиваемая политика использования канала, когда можно подстраиваться под весь остальной трафик (чтобы не забить весь канал при передаче большого массива);
- задание лимитов вручную для каждого потока (потоки строго определенной ширины, чтобы они друг с другом не конкурировали);
- приоритизация и распределение потоков передачи "на лету".

Для таких протоколов характерны высокий уровень безопасности, двухфакторная авторизация при возможности передачи, шифрование, автоматическое восстановление передачи при сбое (при тотальном обрыве на сети), а также масштабирование, управление и мониторинг. То есть чем выше ширина канала, тем быстрее нужно передавать данные, отслеживать и мониторить каждый отдельный поток передачи и выдавать по нему детальный итог. Все это достигается благодаря программному обеспечению – наработкам по ускорению, которые ведутся на прикладном уровне. Замечательные команды разработчиков рассчитывают эти алгоритмы и методы ускорения данных или обхода стандартных ограничений, которые накладывают протоколы.

Очень важным фактором для использования таких протоколов является полная независимость от расстояния передачи и размера, количества, формата и типа файлов (шифрованные, компрессионные и др.). Это дает возможность использовать модифицированные UDP-протоколы в совершенно любой топологии (лучевая, кольцевая, точка-точка и т.д.). Фактически надо указать только на источник, откуда нужно забирать данные (файловая система или поток). Если передавать миллион файлов по 1 Мбайт или один файл весом в 1 Тбайт, скорость может меняться, но она будет относительно сравнимой за счет алгоритмов оптимизации передаваемых блоков данных, которые работают на прикладном уровне, а синхронизировать эти процессы можно с помощью приоритизации.

Полностью соответствует трендам и тот факт, что эти технологии можно использовать в локальном дата-центре, в облаке и в гибридном режиме, так как все больше и больше компаний задумываются о том, чтобы часть рабочих нагрузок переносить в облако.

Техническая реализация

Решение заключается в установке специализированного ПО или скачивании определенного набора библиотек, при работе в клиентском режиме. Для этого достаточно просто зайти на портал, на котором находится средство по ускорению данных. Оно проверяет, стоят ли на компьютере определенные библиотеки, необходимые для инициации и начала трансфера. Если он их не находит, то автоматически предлагает поставить плагин на браузер. Плагин устанавливается, браузер перезапускается и все – можно использовать новые протоколы. Многие организации в России уже успешно применяют данное решение.

Результаты меняются от случая к случаю и зависят от условий передачи: можно достичь ускорения в 2, 10, 30 и даже в тысячи раз.

Например, при тестировании видеопотока из Москвы во Владивосток ускорение составило порядка 30–40 раз.

Задержка передачи остается прежней – если Roundtrip Time был 200 мс, он таким и останется, но данные будут передаваться быстрее. Это происходит за счет программной обработки на прикладном уровне и оптимизации самой схемы передачи данных.

Распространенные сценарии использования

К распространенным сценариям применения протоколов по ускорению передачи данных относятся практически все, с которыми можно столкнуться при ежедневной работе с файлами.

- Инжестирование/транспорт. Перемещение массивов данных любого размера и количества каждый день на высокой скорости для сотрудников и партнеров, используя стандартные IP-сети вместо того, чтобы использовать жесткие диски или строить дорогостоящие аппаратные решения.
- Дистрибуция. Быстрая передача информации разным получателям, где низкая пропускная способность вызывает длительный перенос. Улучшение или замена дорогостоящих систем распределения контента, которые перемещают и хранят дублирующие файлы на пограничных серверах
- Передача и обмен файлами. Обмен и взаимодействие при помощи стандартной структуры папок, с возможностью использования как в ДЦ, так и в облаке. Безопасная отправка и получение файлов и папок любого размера пользователями где угодно, используя простой Dropbox-Like-интерфейс с ПК, ноутбука или мобильного устройства.
- Копирование и синхронизация. Передача миллионов файлов и массивов данных между разными площадками и инфраструктурами на высокой скорости, особенно актуально при репликации дата-центров.
- Потоковая передача данных. Побайтная передача контента от провайдера к конечному пользователю, при котором данные находятся на удаленном сервере с возможностью получения доступа в реальном времени к файлу прямо на лету. В условиях глобализации и увеличения объема передаваемой информации прямые трансляции, которые ведутся с другого континента, должны вестись без обрыва, а это достаточно большой челлендж при передаче потока данных.

Индустриальные примеры внедрений

Приведем примеры компаний, которые уже успешно используют протоколы по ускорению.

- Bank of America существенно оптимизирует документооборот.

Результаты: сокращение времени передачи в 42 раза, сокращение затрат на сетевую ИТ-инфраструктуру, значительное увеличение операционной эффективности.

- Universal Pictures оптимизирует и ускоряет совместную работу. Среди задач компаний такого уровня можно отметить сложные процессы постобработки (затрагивающие много участников как внутри, так и вовне студии), совместную обработку большого количества медиа контента высокого разрешения по всему миру, длительную установку и высокие требования к тренингу для каждого проекта, высокие требования к безопасности и аудиту для защиты критичных IP.

Результаты: сокращение времени ряда процессов с 2–3 недель до 2–3 часов.

- Jabil оптимизирует рабочие процессы и ускоряет обмен дизайн-файлами между инженерами, вендорами и заказчиками. Передача больших дизайн- и CAD-файлов, документации через глобальные сети существенно сказывалась на сроках производства продукта.

Результаты: ускорение процесса работы и выведения продукта на рынок.

- Leica Biosystems внедряет высокоскоростной протокол в собственное решение по передаче снимков пациентов. Это позволило решить задачу быстрой передачи оцифрованных снимков пациентов (которые могут легко превышать гигабайт памяти) как клиентам, так и медицинским специалистам для улучшения постановки диагнозов.

Результаты: быстрая загрузка существенно сокращает время обработки и постановки диагноза, что позволяет значительно улучшить диагностику и уход за пациентами.

Как определить потребность в решении?

Как понять, нужно ли в каком-либо из рабочих процессов использовать высокоскоростные протоколы передачи данных? В этом помогут ответы на шесть вопросов:

1. Передаете ли вы данные большого размера или большое количество файлов?
2. Нужно ли вам передавать данные на большие расстояния или по плохим каналам?
3. Критично ли для вас время передачи файлов? Каковы будут последствия несвоевременной передачи?
4. Нужна ли вам автоматизация передачи файлов?
5. Сталкиваетесь ли вы с ограничениями при работе с файлами и вложениями в Microsoft Outlook или MS SharePoint?
6. Есть ли у вас потребность в корпоративном или внешнем Dropbpx/FTP?

Все эти задачи можно решить с помощью современных средств программного обеспечения по ускорению и передаче передаваемых данных и файлов. ■

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

Жизнь в умном и безопасном городе

“ Как администрация городов может быстрее и эффективнее реагировать на экстренные ситуации без значительного увеличения штата полицейских? ”

На Саммите G20 в 2016 году система **Dahua Safe City Solution** автоматически обнаружила 29 823 нарушения правил дорожного движения. Это технологическое решение значительно снизило нагрузку на силы охраны правопорядка, позволив им сосредоточиться на защите ключевых зон Саммита.

Deep Learning
для улучшения существующего функционала и обнаружения рисков

Распознавание лиц
Лидер тестирования LFW. Точность 99,78%

Распознавание номерных знаков транспортных средств
Точное распознавание на скорости до 200 км/ч

Обнаружение аномального поведения
Вторжение, беспорядки, скопления людей

Детекция нарушений ПДД
Работа светофоров, нарушение скоростного режима, использование мобильного телефона за рулем, не пристёгнутый ремень безопасности и т. д

Единая платформа
для быстрого и эффективного реагирования

Унифицированная платформа Safe City
Быстрый выезд аварийных служб в зависимости от обнаруженной опасности и ее местоположения

Мобильность
Передача отчетов и видеоматериалов в центры безопасности через 3G/4G сети для комплексной обработки данных

CE FC RoHS ISO 9001:2000

ООО «ДАХУА ТЕКНОЛОДЖИ РУС»
Адрес: г. Москва, ул. Ленинская Слобода, 19, БЦ «Омега Плаза»
http://www.dahuasecurity.com/ru

Нейронные сети для задач промышленности и безопасности

Встраиваемые системы машинного зрения нового поколения

Нейронные сети в последнее время набирают все большую популярность, и интерес к их использованию растет как среди производителей, так и у заказчиков. Рассмотрим, как встраиваемые системы машинного зрения нового поколения на основе глубоких нейронных сетей могут быть применены в реальных проектах для задач промышленности и безопасности

Борис Вишняков
Начальник лаборатории анализа динамических сцен ФГУП "ГосНИИАС"

Одно из важнейших направлений внедрений, где будут особенно полезны нейронные сети – это решение задач видеоаналитики для "Безопасного города". Уже сегодня существуют алгоритмы, работающие на глубоких нейронных сетях (распознавание лица, человека и др.), которые можно вживить на чип на борту камеры.

Глубокие нейронные сети – что это?

Обычные полносвязные сети существовали с давних времен. В 1988 г. были придуманы конволюционные (сверточные) сети, а отдельно от них в 2006 г. – глубокие сети.

Революция в машинном зрении случилась в 2011 г., когда были собраны в первом виде глубокие сети для задач машинного зрения и прошла первая волна публикаций о глубоких сверточных нейронных сетях в распознавании изображений.

Ключевые плюсы таких сетей:

1. Для обучения глубокой нейронной сети нужно очень много данных, и она не страдает эффектом насыщения из-за огромного числа обучаемых параметров, проблемы Underfitting и Overfitting более-менее решаемы.
2. Глубокие конволюционные нейросети учитывают специфику изображений как объекта распознавания и, даже не зная каких-то ракурсов, могут распознать объект в совершенно неизвестной для себя обстановке.
3. Могут учиться без учителя. Для этого требуется больший объем данных и процесс обучения длится значительно дольше, но уже появились новые прорывные подходы в данной области.

У нейронных сетей есть и минусы:

1. Нужны огромные вычислительные мощности для обучения на больших объемах данных.
2. Необходимо дорогое "железо" с большим количеством видеокарт для обработки всего нескольких каналов на один сервер в режиме реального времени.

Рывок в качестве распознавания лиц

Начиная с 2015 г. на всех общедоступных базах был совершен значительный рывок в распознавании, и можно утверждать, что лучшие российские системы распознавания лиц являются и лучшими в мире – три российские компании входят в топ-5 по базе NIST. Если раньше можно было распознать лицо только во фронтальном ракурсе, то сейчас это возможно сделать практически во всех ракурсах.

Распознавание объектов вместо моделирования фона

Классические системы распознавания построены на предварительных предположениях: моделирование фона, разделение Foreground и Background (неподвижный фон и движущиеся объекты на нем). Но это противоречит восприятию человека, так как человек и без признака движения может легко определить людей, находящихся в его поле зрения. Сейчас происходит переход от предположений о сцене именно к распознаванию отдельных объектов и используются не признаки движения, а только факт наличия объекта типа "человек на сцене". Сегодня вероятность распознавания силуэта человека уже очень хорошая – ошибки 1-го и 2-го рода составляют порядка 1% на данных среднего и высокого качества.

Реидентификация с помощью нейронных сетей

Задача реидентификации может быть решена во многих спектрах.

Первый (очевидный, но редко запрашиваемый заказчиком) – это передача человека или другого объекта видеонаблюдения от одной камеры к другой, когда его нужно подхватить с тем же ID, с которым он двигался до этого. Раньше эта задача в определенной степени решалась, но если человек на одной камере был в одном ракурсе, а на следующей – уже в новом, то не все алгоритмы идентификации хорошо справлялись.

Второй – поиск человека или другого объекта в базе данных по описанию, сформированному оператором, или фотографии.

Сейчас подход к реидентификации построен на генерации Deep ID для объекта (человека, автомобиля и др.) с последующим сравнением шаблона с шаблонами других объектов (контрастные, цветовые признаки и т.д.). Более того, можно рассматривать образ человека как лицо при распознавании – то есть шаблоны внешнего вида людей загружаются в базу данных и после конкретного события, если нужно пробить образ человека по базе данных, по нему строится Deep ID, сравнивается с шаблонами, и выдаются все вхождения человека, но не по лицу, а по внешнему виду. Этот спектр задач идентификации сильно вырос и уже стал по-настоящему умным.

Контроль техники безопасности на производстве

Возросли запросы на автоматические системы промышленной безопасности в части ношения средств индивидуальной защиты. Вероятно, это связано с большими штрафами, накладываемыми на те предприятия, которые не обеспечивают ношение СИЗ на производстве. Оператору же системы видеонаблюдения отследить факт отсутствия СИЗ довольно сложно.

Глубокие нейронные сети справляются и с такой задачей – по каждому типу униформы систему придется доучить, но результаты

+	–
• Обучение без ограничений по сложности на сверхбольших объемах данных – за счет этого превосходит все методы прежних поколений по качеству • Глубокие конволюционные нейросети учитывают специфику изображений как объекта распознавания • Возможность обучения без учителя	• Для обучения требуются довольно большие объемы данных • Для обучения требуется дорогое «железо» с большим количеством видеокарт • Для работы также требуется мощные процессоры или видеокарты

Плюсы и минусы глубоких нейронных сетей

Наиболее перспективные направления для применения нейросетей

распознавания высоки даже для таких средств индивидуальной защиты, как очки, причем на сравнительно небольших разрешениях, – ошибки 1-го и 2-го рода составляют порядка 5%.

Анализ больших данных в задачах промышленности

С точки зрения применения нейросетей в промышленности наиболее перспективными направлениями являются следующие:

1. Поиск полезных ископаемых. Объем данных, генерируемый геологами, огромен, и новые методы на базе нейронных сетей позволяют выявить особенности, которые достаточно часто приводят к ответу "да" в тех случаях, где старые алгоритмы говорили "нет".
2. Транспортные и логистические задачи. Хотя они давно успешно решаются методами линейного программирования, но при огромной размерности процесс будет долгим. Обучение нейронной сети на решение транспортной задачи – действенный способ разрешения подобных ситуаций, если объем данных очень большой.
3. Предсказание неисправностей. Возможна не просто реакция на неисправность, а именно предсказание поведения системы, когда есть вероятность какого-то ЧП, например выброса химических веществ. По набору из 50–100 датчиков система должна обучаться как на успешных событиях, так и неприятных, которые имели место в прошлом. Подобные задачи уже решаются – быстро и с хорошими показателями.

Что можно добавить на борт камеры?

Когда мы говорим о том, какие алгоритмы интеллектуального видеонаблюдения можно добавить на борт камеры, то очень многое зависит от чипа (его архитектуры, процессора, памяти), который используется для обработки изображений – он получает картинку с матрицы и дальше отправляет ее в сеть. Многие производители открывают доступ к этому чипу, поскольку он практически всегда недогружен и в него можно встраивать модули видеоанализа.

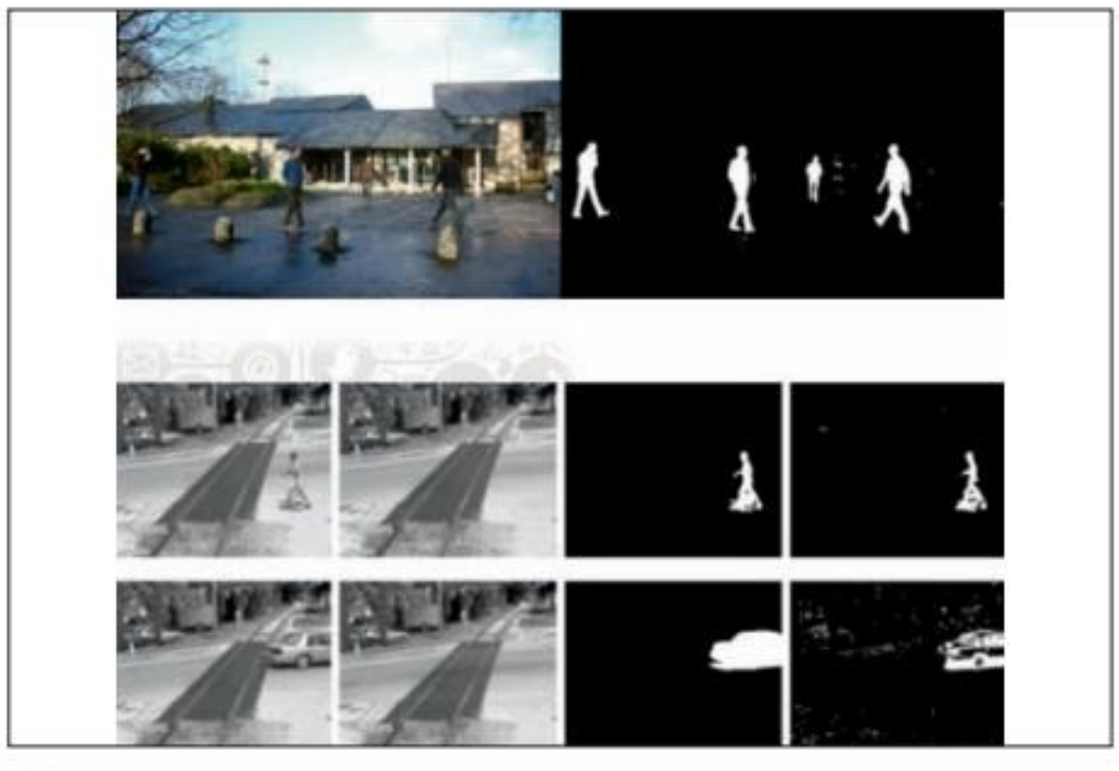
На данный момент в качестве чипа в камерах высокой ценовой категории используется в основном SoC (System on a Chip) на базе процессоров ARM, в которых есть интегрируемые Floating Point Unit или Neon.

Стоит отметить, что общие недостатки классических процессоров перевешивают их плюсы. По сути, плюс только в том, что у них достаточное количество оперативной памяти для загрузки в память нейронной сети. Но ISP в чипе практически всегда закрыт – ни один вендор не открывает ISP, хотя по умолчанию в SoC он доступен для разработчиков.

Практически все производители экономят на количестве памяти FLASH и RAM – урезают ее донельзя, пытаясь удешевить свое решение. Это приводит к катастрофе, когда начинается импорт новых алгоритмов. С алгоритмами предыдущего поколения (обнаружение лиц или движущихся объектов) нет никаких проблем, но сделать что-то на базе глубоких нейронных сетей получается очень редко.

Кроме того, до сих пор даже в достаточно дорогих камерах находится SoC с очень слабым CPU – в основном Cortex-A7, Cortex-A8, Cortex-A9. Дата выхода этих процессоров – 2012–2014 гг., новые ядра ARM в текущих SoC практически не применяются.

Архитектуры от NVIDIA и Intel (Altera) FPGA пока не используются в камерах – это дорого. Архитектуры от NVIDIA представляют больший интерес, поскольку на данный момент все фреймворки для обучения глубоких сетей реализованы с использованием NVIDIA CUDA SDK. После обучения алгоритмов практически ничего не придется делать с нейронной сетью, чтобы заставить ее работать, к примеру, на NVIDIA Jetson, в то время как для плат Intel нужно полностью переделывать и оптимизировать библиотеки работы с нейронными сетями. Тем не менее эффект хороший – в данных SoC есть достаточно места, чтобы внедрить нейронную сеть



Прошлое поколение систем видеоаналитики

Новое поколение систем видеоаналитики

(FLASH и RAM), необходимая мощность графических ядер, чтобы решать задачи в реальном времени, и поддержка процессора ARM, на который также возлагается определенная часть вычислений (начиная от декодирования картинки и заканчивая простейшими алгоритмами, которые накладываются поверх нейронных сетей или выполняют предобработку).

Реальные возможности нейронных сетей на борту камер

Какие задачи нейронные сети смогут решать, находясь на борту камер, а какие – нет?

1. Распознавание лиц. Нейросетевые детекторы лиц могут найти лицо по части лица, то есть даже по практически полностью загороженному лицу. Но можно ли их применить на камере? Нет, так как даже на обычных компьютерах, на CPU в Real-Time это практически нереально, поиск лиц работает только на видеокартах.

Зато на камере можно использовать детектор на базе старых алгоритмов, например Виолы-Джонса 2001 г.

Распознавание в реальном времени на камерах также невозможно. Биометрические шаблоны по лицу строятся на стандартных процессорах со скоростью от 250 до 2000 мс. На камерах это можно будет сделать, только когда они сменят свою архитектуру.

Однако можно проводить распознавание в близком к реальному времени – выбирать из трека лиц одно с наилучшим ракурсом и в процессе с низким приоритетом, чтобы не влиять на качество алгоритма детектирования лиц, потихоньку строить для него биометрический шаблон. Это работает хорошо, но небыстро – шаблон строится от 20 до 80 с, время зависит от глубины нейронной сети, с помощью которой распознаются лица. Однако если стоит задача сохранить список тех, кто был на объекте, а не сразу выдавать результат оператору, кто именно пришел, то такая скорость не проблема.

2. Видеоаналитика. Нейросетевой детектор людей и машин на борту камеры сделать не получится – примерная скорость работы текущих алгоритмов 3–5 кадр/с на очень хорошей видеокарте.

3. Реидентификация. Построить шаблон для распознавания человека (по силуэту, одежде и пр.) на камере можно в таких же условиях, в каких применяется построение шаблонов в распознавании лиц, поэтому решить задачу реидентификации с помощью нейронных сетей на борту камеры можно, но не в реальном времени.

4. Нейросетевой детектор оставленных предметов. Такой распознаватель можно внедрить на камеру, так как в оставленных предметах без модели фона не обойтись, а она отлично работает на камере. И далее нейронная сеть будет заниматься исключительно классификацией уже найденного моделью фона объекта.

5. Обнаружение СИЗ. Можно использовать детектор на базе моделей фона, а сверху накладывать нейросетевой классификатор СИЗ – человек в защитной одежде или обычной.

Таким образом, нейросетевые детекторы для всех задач недоступны на текущем уровне развития мобильных процессоров. Но какие-то нейросетевые классификаторы/распознаватели могут быть использованы уже сейчас на процессорах, которые производители камер внедряют в свои устройства.

Второй виток нейросетевой революции

Текущее положение дел в области нейронных сетей характеризуют четыре основных направления, которые наблюдаются в мире:

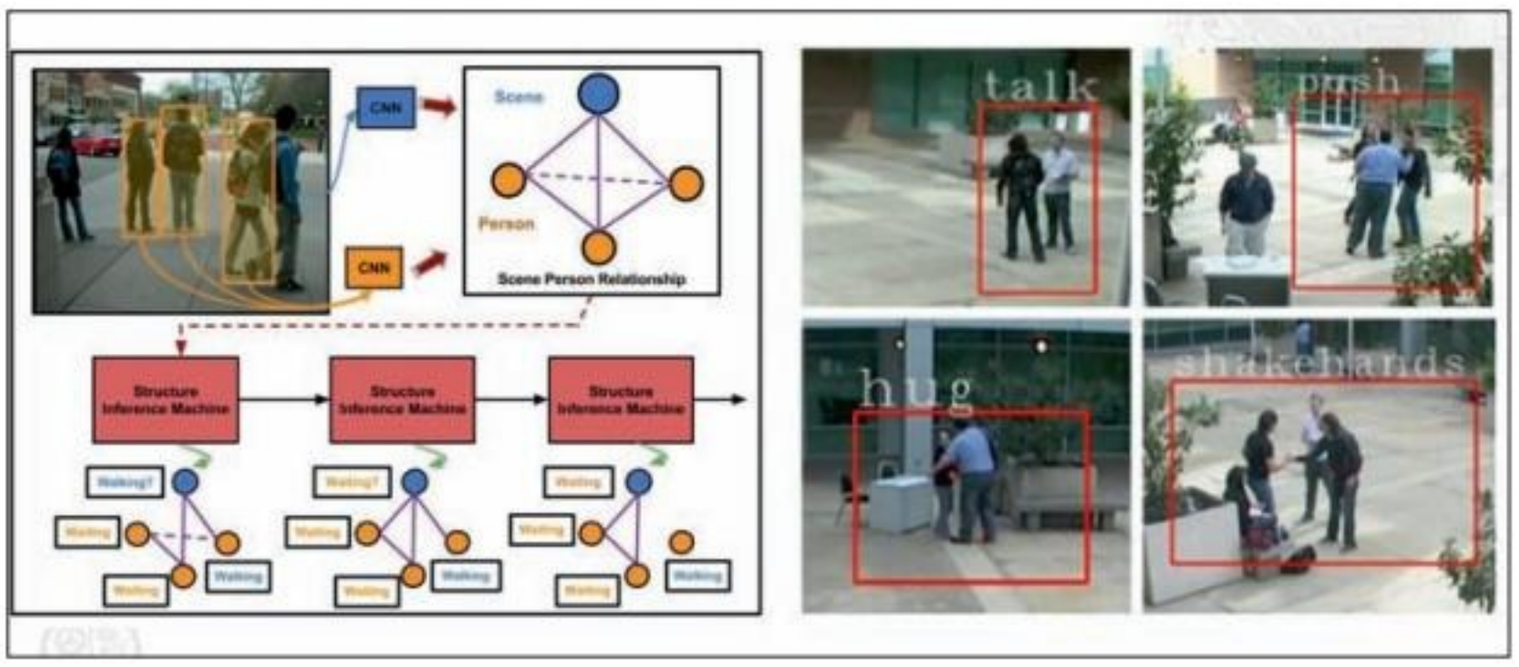
1. Глубокие соревнующиеся сети для имитации данных (GAN, Domain Transfer Learning, Zero-Shot Learning). Существенно помогают решить проблему с дополнительным созданием обучающей выборки для нейронных сетей, которые уже занимаются распознаванием.

2. Интерпретация динамической визуальной информации на естественном языке (Action Detection and Prediction, Video Annotation, Video and Language Understanding, Text-to-Video, VQA). Это то, чего все ждут, – Activity and Behavior Recognition, а именно – детекторы драк, объятий, рукопожатий, бега и др. Результаты в понимании поведения улучшились уже в два раза по сравнению с алгоритмами двухлетней давности.

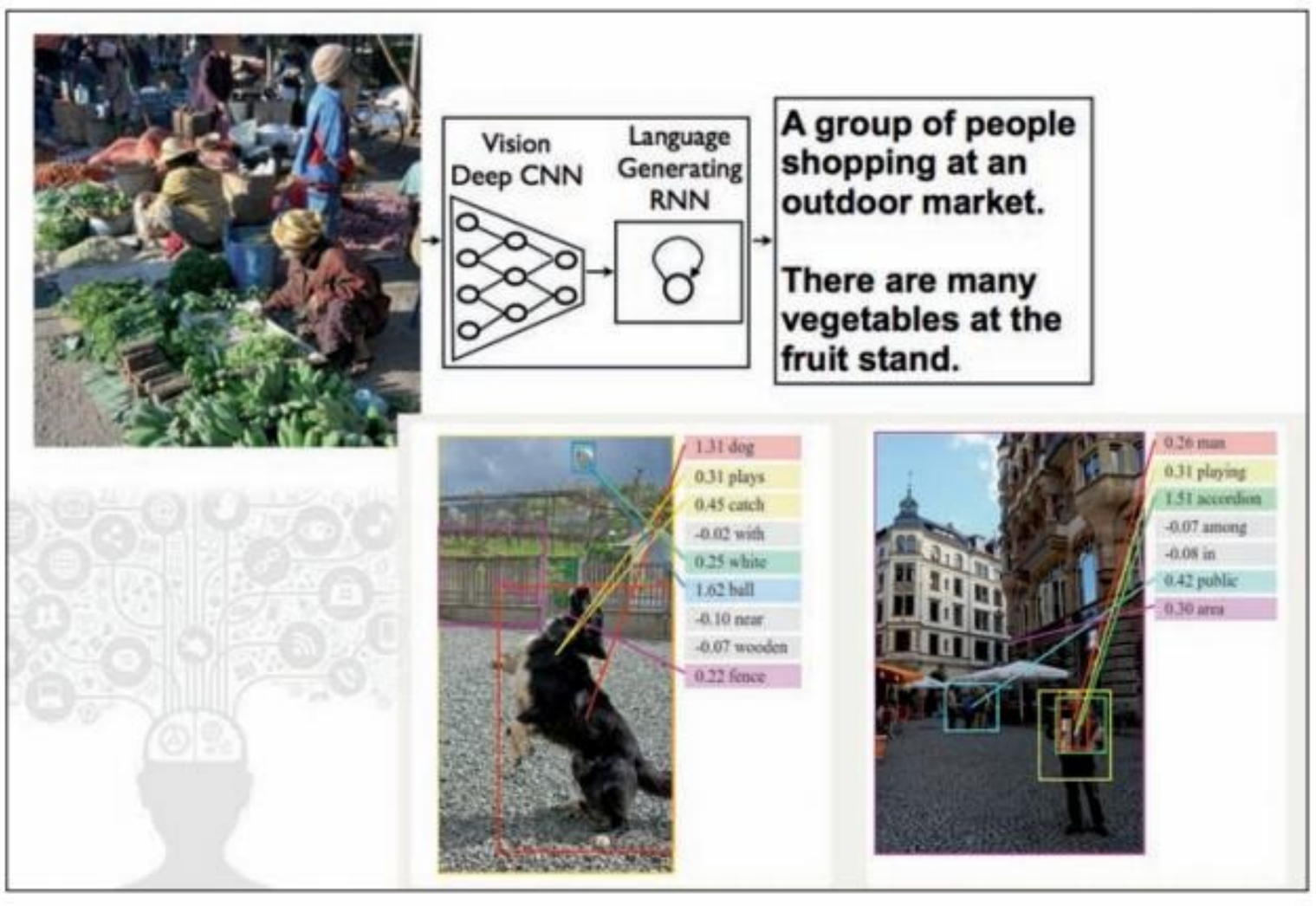
3. Обучение глубоких сетей как активных агентов (Reinforsement Learning, Lifelong Learning). Имеется в виду обучение сети без учителя.

4. Глубокое обучение с использованием структурных моделей, баз знаний и программ логического вывода (Graph Structured CNN, Deep Visual Reasoning). Был совершен большой рывок в сфере Activity and Behavior Recognition. Понимание сцены – это самое высокоинтеллектуальное, что может быть в системе видеонаблюдения. Компьютер будет описывать то, что происходит, например "человек в красной куртке прошел в здание, повернул направо и зашел в конкретную комнату". Это новый уровень взаимодействия человека с компьютером и понимания компьютером того, что происходит на сцене.

5. GANS (Generative Adversarial Networks). Это сети, которые могут сделать из чего угодно что угодно (из зимы лето и обратно, поменять местами зебр с лошадьми и т.д.) и учатся генерировать определенные объекты. ■



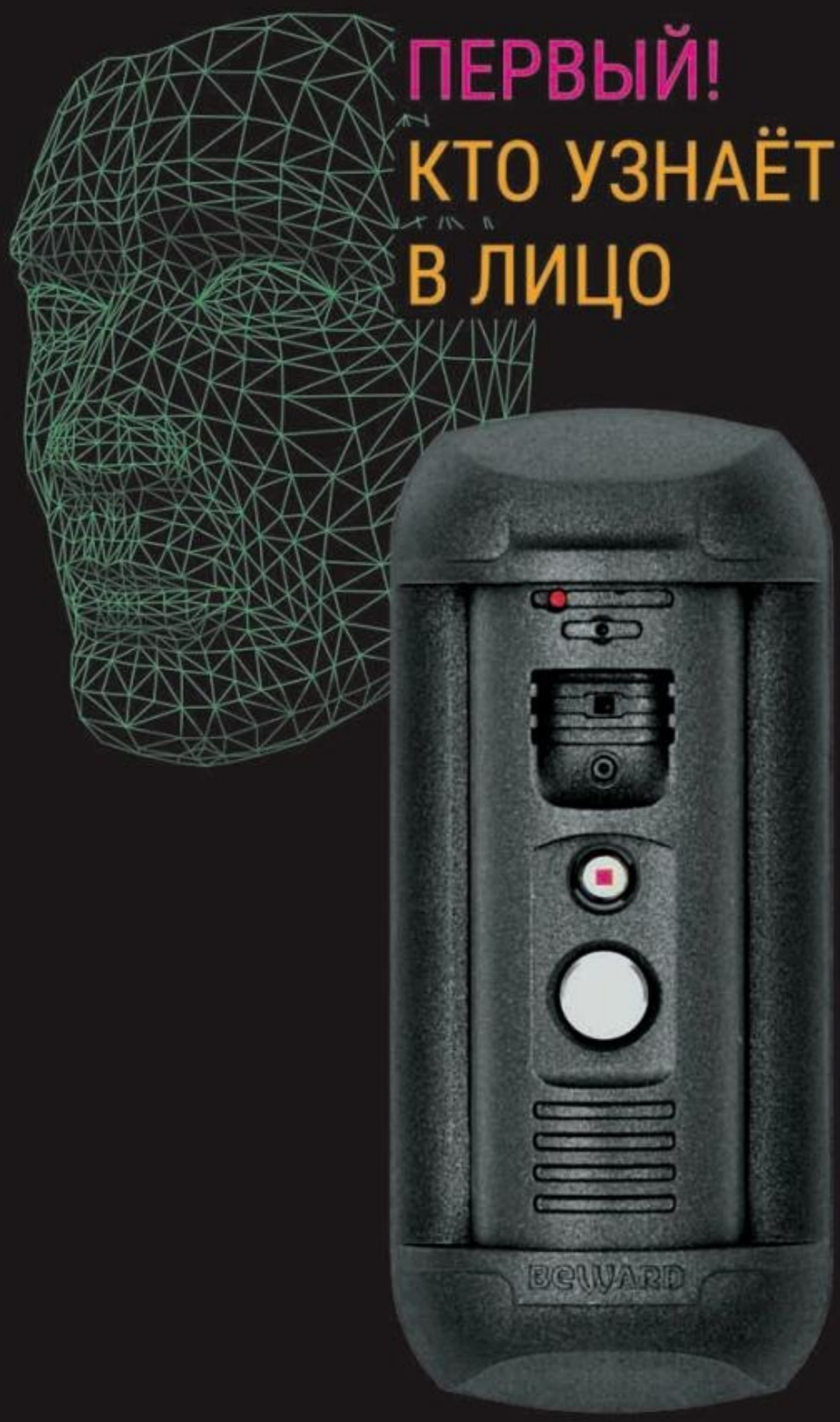
Понимание поведения



Понимание сцены

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

ПЕРВЫЙ!
КТО УЗНАЁТ
В ЛИЦО



DS06M
SIP-ДОМОФОН

Встроенное
распознавание лиц

BEWARD

www.beward.ru

Интерком будущего

Время от времени мы все задумываемся о будущем. Сегодня это повод высказаться насчет тенденций в области систем связи и оповещения

Роман Мишин
Независимый эксперт

Что такое интерком, чем он отличается от других видов связи и почему все более популярен?

Преимущества интеркома

Основные отличия этого класса систем от телефонной связи такие:

1. Наличие интеркома на объекте позволяет освободить телефон от большинства внутренних коммуникаций и оставить телефоны только там, где необходимо. Можно разделить внутреннюю связь и внешние контакты. Удобно при необходимости быстро посоветоваться с коллегами, пока внешний клиент ожидает на трубке.
2. Свободные руки и громкоговорящая связь. Общение как с глазу на глаз, хотя собеседники находятся в разных помещениях.
3. Широкий спектр переговорных устройств, специально разработанных для сложных условий. Однокнопочные панели вызова. Минимум органов управления связью.
4. Возможность работы в режиме общего вызова и как системы оповещения и управления эвакуацией.
5. Проведение совещания. Оперативная раздача команд подчиненным с подтверждением.
6. Интерком способен работать и как дискуссионная система, с той разницей, что собеседники находятся на своих местах – это экономит время!

Классификация интерком-систем

Интерком-системы можно разделить по следующим признакам:

Тип используемого сигнала: аналоговые, цифровые и IP.

Архитектура – масштабируемые и немасштабируемые, соединение звездой или использование общей проводки, а также системы без центрального сервера.

Емкость: малая (до 10 абонентов), средняя (от 10 до 100 абонентов), большая (более 100 абонентов).

Назначение (в зависимости от характера объекта и условий эксплуатации): офисные, "кассир – клиент", промышленные, диспетчерские и т.д.

Как правило, основой системы является центральный коммутационный блок (сервер). Они бывают различной конструкции, но их можно разделить на законченные моноблочные и модульные, которые комплектуются различными компонентами в зависимости от требований заказчика. Такие системы более гибкие и, как правило, имеют больше возможностей как по функционалу, так и по расширению.

Существуют также системы, в которых коммуникационный интеллект распределен по абонентам. Такие системы обходятся без центральных серверов и контроллеров, но любой интерком не может обойтись без абонентских устройств.

Абонентские устройства могут быть: офисные, промышленные, домофонные, влагозащищенные, вандалоустойчивые, для специальных условий эксплуатации, а также как с полной клавиатурой, так и только с клавишами прямого набора. Отдельная категория абонентских устройств – пульты управления или пульты диспетчера. Они, как правило, имеют наибольший функционал: оснащены и цифровой клавиатурой, и клавишами прямого набора, а также дополнительными функциональными клавишами. Имеется пульт – устройство, позволяющее оператору не только пользоваться голосовой связью, но и управлять и системой, и исполнительными механизмами, подключенными к ней. На пульт выводятся также сигналы о срабатывании датчиков или авариях системы.

Области применения и элементы интеркома

Интеркомы прежде всего используются там, где требуется оперативность, есть опасность, необходимость постоянного управления производственным или иным процессом:

- во взрывоопасной среде;
- при высоком уровне шума;
- в химически агрессивной среде;
- при прямом воздействии погодных условий;
- если требуется надежная непрерывная и безопасная работа.

Поэтому к интеркомам предъявляются повышенные требования по надежности, простоте эксплуатации и обслуживании.

Самый важный элемент системы – рабочее место диспетчера. Здесь решаются следующие задачи:

- производственная связь, управление и контроль оперативных механизмов;
- управление паркингом, кассовыми аппаратами, переговорными устройствами;
- видеонаблюдение, видеоаналитика, видеозапись;
- управление освещением, энергооптимизация;
- эвакуация людей и координация сил служб безопасности.

Требования заказчиков и их пожелания при внедрении интеркома, как правило, сводятся к следующему:

- привлекательность проектов;
- постоянный технологический и экономический контроль;
- оптимизация под конкретного клиента, минимизация издержек обслуживания;
- оптимизация для инвестиций, никаких постоянных затрат на обслуживание и ремонт.

Интеграция систем жизнеобеспечения здания

Требования к системам жизнеобеспечения здания возрастают с каждым днем. До недавнего времени отдельные системы обеспечения жизнедеятельности объекта рассматривались изолированно. Сегодня нужны комплексные автоматизированные решения. Главной идеей становится интеграция.

Основная перспектива развития – объединение всех систем. Поскольку любая техническая система обеспечения безопасности представляет собой систему связи между абонентскими устройствами, то возможно в одной системе совместить следующие сервисы: передача голоса и данных, изображение, оповещение. Управление всеми подсистемами координируется с единой пользовательской поверхности. Все логические функции (передача голоса, изображение, управление дверьми, контроль доступа) упрощаются благодаря интеграции.

Необходимое условие – унифицированные интерфейсы и соответствующее программное обеспечение. Будущее – за объединением различных устройств на основе единой интеграционной платформы.

Интеграция коснется также и рабочего места диспетчера, сведя управление всеми сервисами и контроль всех систем на один диспетчерский пульт. Отпадет необходимость во множестве пультов для разных систем, ситуация, показанная на рис. 2, уйдет в прошлое.

Прежде решения для организации внутренней связи выглядели как система с центральным устройством, к которому по лучевой топологии подключаются абоненты. Каждый тип абонента подключен к соответствующим физическим портам. Вся коммуникация реализовывалась в пределах центрального блока. Недостатком такого решения было то, что при выходе из строя интерфейсов или централи отдельный вид сервисов или вся система становятся неработоспособны. Подобным образом строились до последнего времени и системы для промышленности.

Благодаря появлению IP как универсальной среды передачи различного типа данных стало реальным унифицировать и линии связи, и тип интерфейса. Кроме того, длина линии становится фактически неограниченной при возможности оборудования поддерживать интернет-протоколы.

Благодаря IP стирается грань между телефонными системами и диспетчеризацией. IP-система может предоставить, помимо традиционной связи, еще и следующие возможности.

- Ограниченное лишь мощностью сервера количество пультов управления. Это означает, что одним сервером одновременно может обслуживаться большое число пультов управления и переговорных устройств.
- IP-системы в ряде случаев свободно конфигурируются без дополнительного ПО, через Web-интерфейс.
- Вызовы могут отображаться на дисплее оператора для определения абонента, его местоположения и т.д.
- Оператор может подключаться через IP-сеть или любую телефонную систему (например, GSM), что позволяет гибко располагать его рабочее место.
- Пульт управления может быть выполнен в виде софта на PC, Tablet или мобильном телефоне.
- Фактор ограничения количества операторов, одновременных звонков зависит от мощности сервера и сетевого оборудования.
- Применяются серверы стандартной архитектуры. Посути, различия только в ПО.
- При использовании графической поверхности возможно отображать очередь вызовов и по клику менять положение абонентов в очереди.
- Отображается длительность вызова, имя, другая служебная информация.
- Пульты управления разных систем могут объединяться для переадресации вызовов.
- Классический пример переадресации в случае переполнения очереди вызова: когда достигнуто предельные время ожидания или количество вызывающих, вызов переходит на альтернативный пульт управления.

Возможно, что с одной группы устройств вызов идет на пульт управления, а с другой группы – в полицию.

Входящий вызов можно объединять с другими системами/источниками информации, например находящейся рядом видеокамерой, планом местности (Google Maps), другими информационными данными. Оператор получает всю необходимую информацию для помощи абоненту еще до ответа на его вызов. Преимущества системы заключаются также в следующем:

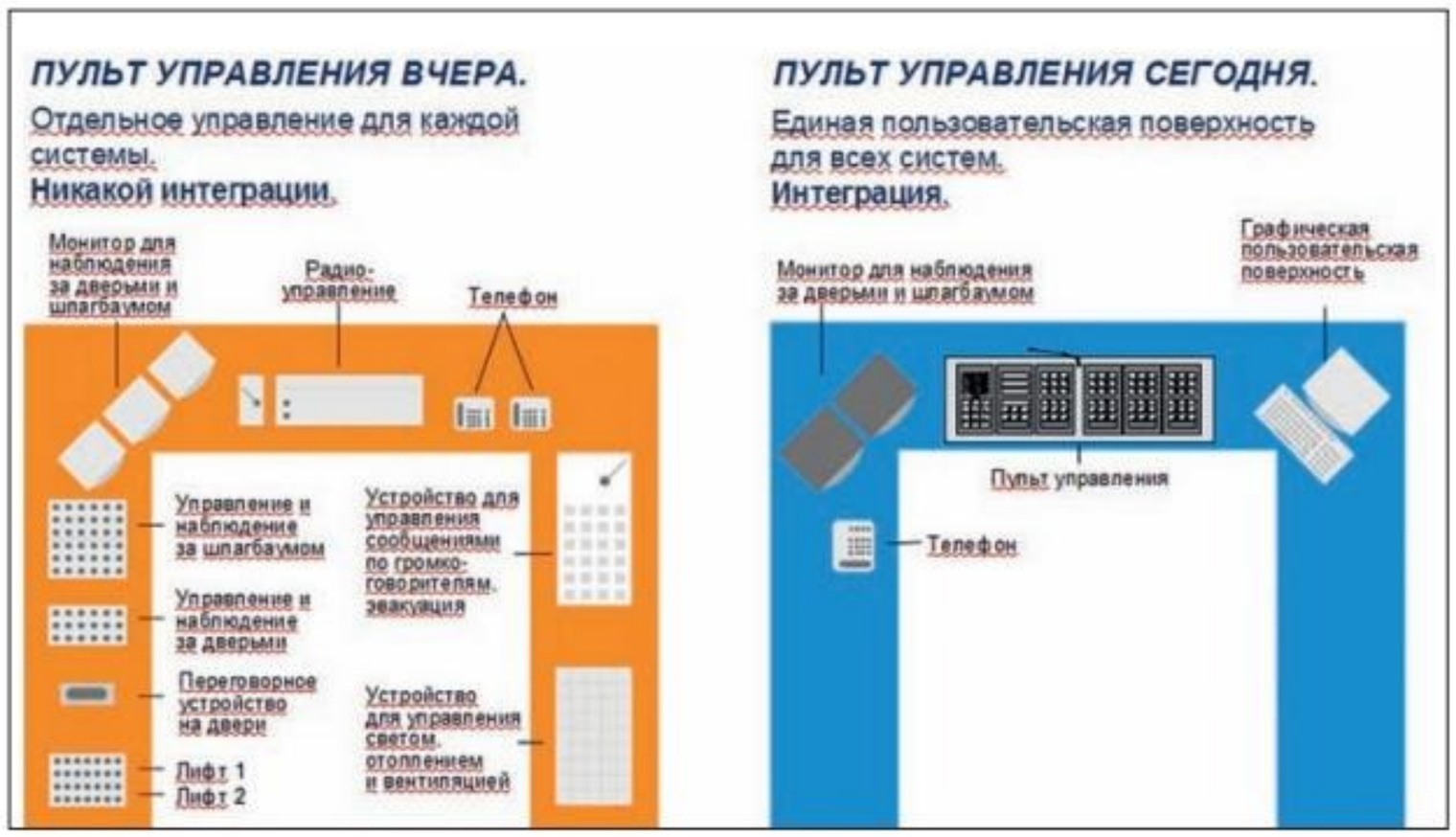


Рис. 1. Эволюция систем управления

- объединение и синхронизация информации разных IP-источников (видео-, аудиосигналы, данные);
- определение местоположения абонента для координации спасательных служб;
- протоколирование всех событий и запись переговоров (количество вызовов, время ожидания, время разговора, нагрузка операторов, количество необработанных вызовов, график загрузки и т.д.);
- протоколы выдаются в автоматическом (e-mail, СМС, принтер и т.д.) или ручном режиме – это дает возможность управления ресурсами ситуационного центра.

Интеллектуальное оповещение при эвакуации

Вычислительные мощности современных серверов и унифицированные интерфейсы позволяют перейти к качественно другому управлению эвакуацией – интеллектуальному оповещению. Такая система позволит, например, значительно уменьшить количество пострадавших от удушения дымом с помощью эффективного управления аварийными выходами.

Особенностью системы интеллектуального оповещения может быть акустическое управление аварийными выходами, которое в задымленных помещениях действует намного эффективнее, чем обычные визуальные знаки.

Пространство делится на много небольших зон оповещения, каждая из которых самостоятельна. В случае возникновения опасной ситуации на каждую зону с заранее определенным интервалом транслируется звуковой сигнал таким образом, чтобы волна последовательности сигналов вела слышащего их к выходу.

Человек реагирует в экстренных ситуациях гораздо адекватнее и быстрее на акустические сигналы. Следовательно, уменьшаются ложные эвакуации и минимизируется время эвакуации при настоящей тревоге.

Интеллектуальные системы довольно дороги, а также требуют высокой квалификации персонала, программирующего возможные сценарии. Однако правильно настроенная система позволит сберечь и материальные ценности, и жизни людей.

Использование принципов нейронных сетей

Следующий шаг в развитии IP-технологий – переход от систем с центральным сервером к распределенным системам, использующим принцип нейронной сети.

Особенности этих перспективных систем таковы:

1. Все компоненты системы автономны и обладают встроенным интеллектом. Достаточно просто соединить между собой.
2. Никаких центральных устройств. Каждый терминал одновременно является и частью распределенного сервера.
3. Настройка через Web-интерфейс. Сборка системы под силу любым пользователям.
4. Высокая живучесть. При неисправности какого-либо элемента остальные сохраняют полную работоспособность.

Основной единицей таких систем станет интеллектуальный модуль, представляющий собой микрокомпьютер с собственным адресом. Такой модуль может выступать как универсальное IP-устройство для связи, оповещения, СКУД, управления инженерными сетями и видеонаблюдения. Модуль может быть размещен как в корпусном (в том числе защищенном), так и в бескорпусном исполнении. Увеличив мощность процессора, можно нарастить возможности модуля. Можно также создавать подсистемы на базе каждого из модулей.

Модуль в состоянии обеспечить внутреннее логирование процессов, а система модулей – распределить приоритеты.

Основаная особенность нейронной сети – соединение каждого с каждым.

При увеличении количества устройств растет интеллект системы.

Развивая возможности ПО, возможно делегирование функций от одного устройства другим. По сути, мы получим "социальную сеть" интеллектуальных устройств, позволяющую при необходимости решать самые разнообразные и сложные задачи. ■

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

КОЛОНКА РЕДАКТОРА

Новая революция

За два года существования нашей рубрики много что изменилось как в технологиях, так и в бизнесе. Новая технологическая революция меняет нашу жизнь, бизнес так же кардинально, как компьютеризация 90-х и широкое распространение Интернета в нулевых годах. Пока нет общеупотребительного названия этой революции, мне нравится термин "цифровая трансформация". Эта революция стоит на двух столпах – Интернете вещей (IoT, Internet of Things) и искусственном интеллекте. Рассмотрим, что означает каждое понятие.

Wikipedia дает нам определение, что Интернет вещей – это концепция вычислительной сети физических предметов ("вещей"), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Под это определение попадают как классические технологии – системы контроля доступа, промышленной автоматизации и автоматизации зданий, так и совершенно новые, невозможные ранее – носимая электроника, каршеринг, беспилотный транспорт, розничные магазины без продавцов и т.д. То, что было автономными системами в течение десятилетий, сейчас изменяется, интегрируется на основе ИТ-технологий, при этом получая новые функции. Так, например, системы автоматизации зданий могут становиться системами контроля здоровья пожилых людей за счет интеграции с системами носимой электроники и контроля микроклимата в помещениях.

Но значительно большее влияние на нашу жизнь будут оказывать системы искусственного интеллекта, особенно основанные на системах машинного обучения. В 2014 г. произошел первый качественный скачок, когда нейронная сеть DQN, построенная на новом алгоритме глубокого машинного обучения, самостоятельно научилась играть в 50 компьютерных игр 80-х гг. ("Тетрис", "Арканоид", "Змейка" и т.д.) с результатом в десятки раз более лучшим, чем может играть человек. Программа Alpha Go компании Google, натренированная на лучших стратегиях, придуманных человеком, через полгода обыграла чемпиона мира по го, со счетом 4:1. Следующая версия этой программы, Alpha Go Zero, которая совсем не изучала человеческий опыт, а тренировалась, играя только сама с собой, выиграла у предыдущей версии программы со счетом 100:0. Но это лишь начало. Компьютеры стали понимать смысл, получать знания из данных, распознавать предметы на картинках и голос лучше самого человека. Но самое главное, что компьютеры становятся творческими. Программа Prizma может переработать ваши фотографии под рисунки известных художников. Нейронная сеть от Яндекса пишет классическую музыку и джазовые импровизации. Но самый серьезный прорыв наступит тогда, когда системы машинного обучения будут интегрированы с бизнес-системами предприятий и позволят убрать человека из производственных бизнес-процессов. При этом Интернет вещей будет выступать "руками" глобального искусственного интеллекта.

Наша рубрика начиналась как рассказ о современных тенденциях в системах автоматизации зданий, но чем дальше мы ее развивали, тем больше мы понимали, что нельзя ограничиться только этой темой и что нашим читателям будут интересны описания трендов, наиболее важные новости и различные взгляды на всю совокупность процессов, принесенных новой технологической революцией, и то, как они влияют на традиционные отрасли. Поэтому мы решили изменить название рубрики на "Цифровая трансформация: искусственный интеллект, умный город, IoT" и освещать в ней наиболее важные события, аналитику и обзоры от ведущих экспертов.

Алексей Коржебин

Редактор рубрики "Цифровая трансформация: искусственный интеллект, умный город, IoT", технический директор ООО "Эмбеддед Системс Рус"

Город в движении:

как цифровые технологии меняют будущее транспорта

На дорогах России первый автопилот появился в 1958 г., когда проехала первая электричка без машиниста. А значит, большой задел по автоматизации и созданию умного транспорта у нас есть давно. Давайте разбираться, какие могут быть варианты дальнейшего развития в этом направлении

Виталий Горбушин

Ведущий консультант по технологиям и облачным решениям Oracle в России

Урбанизация продолжается, происходит отток населения из маленьких городов и поселков в большие. По некоторым оценкам, к 2060 г. 60% населения мира будет жить в городах (сейчас 50%). Растет средний класс, и людей, которые покупают автомобили, становится все больше и больше. Следовательно, увеличивается нагрузка на городскую инфраструктуру и дороги. Высокое количество пробок ведет к негативным последствиям: задержке доставки товаров, опозданию людей на работу и т.д.

С другой стороны, несмотря на все усилия производителей, транспорт продолжает загрязнять атмосферу.

Потенциальные решения

Технологии продолжают активно развиваться, появляются новые бизнес-модели, правила ведения бизнеса на транспорте и способы его использования.

В последнее время наблюдается появление таких новшеств, как каршеринг (использование автомобилей, находящихся в свободном доступе в городе), разнообразные типы такси, которые можно вызывать с помощью мобильного телефона, совершенствование городского общественного транспорта. Кроме того, самые актуальные тенденции урбанистики – это развитие пешеходных зон в крупных городах, безмоторного транспорта, велосипедов.

Если внимательно рассмотреть проблему транспорта в больших городах, то можно увидеть факторы, которые тормозят внедрение нововведений: законы, политические вопросы, использование земли, сложившаяся структура городов, привычки потребителей и др.

В то же время многие технологические аспекты, наоборот, помогают решению транспортных проблем, как и новые способы взаиморасчетов за перевозки. Например, в области частных автомобилей интересные тренды связаны с поездками без водителя, постоянным подключением к Интернету, переходом на полностью безопасные электрические двигатели, шерингом, автономным вождением в целом (автомобили, грузовики, поезда без водителей). Это все приводит к оптимизации затрат на транспорт, уменьшению простоя, четкому выполнению графика, снижению количества аварий, пробок и т.д.

Постоянное подключение

В постоянном подключении автомобиля к Интернету важную роль играют информационные технологии: нужно в реальном времени анализировать трафик, прокладывать маршрут, обеспечить связь между автомобилями, чтобы они не столкнулись, и связь автомобиля с городом, чтобы спланировать правильный маршрут или изменить его в режиме реального времени в зависимости от ситуации.

Такие вещи уже широко распространены во всем мире, и надеемся, что они придут и во все российские города, а не только в большие.

Электрификация

Появляется все больше электрических машин. В Москве с них не берут деньги за парковку и не облагают транспортным налогом. Это примеры того, что регуляторы серьезно озабочены транспортными проблемами и делают все, чтобы каким-то образом их решить.

За каршерингом будущее

Каршеринг

Данное направление еще недостаточно развито, подобного рода машин на улицах мало, и они простаивают большую часть времени. Но видится, что за этим способом передвижения будущее. Особенно если он пойдет в комбинации с совместным использованием, когда один человек взял машину и еще подвез на работу сослуживца. Вот уже машин требуется в два раза меньше. Такие гибридные сервисы могут очень сильно изменить ситуацию на дорогах.

Автономные автомобили

Это мировой тренд с огромными перспективами. Сейчас все (и производители машин, и информационные компании Uber, Yandex и т.д.) озабочены созданием автономного способа передвижения, который очень тесно связан с приходом в будущем технологии 5G (передача по сетям связи на высоких частотах с большой плотностью радиоканала). Производители разрабатывают бортовое оборудование на машинах (правда, пока оно еще достаточно громоздкое), а операторы связи – стандарты на новые сети. В ближайшие годы эти две тенденции сольются, и уже ничего не будет удерживать от того, чтобы машины ездили без водителей. При условии качественной связи есть надежда, что это снизит аварийность на дорогах и позволит уменьшить пробки в больших городах.

Пешеходы и велосипеды

Самый кардинальный способ избавиться от машин – не ездить на них. Вводятся большие пешеходные зоны, людей призывают пользоваться велосипедами. Но тут тоже есть свои проблемы. Например, в Китае большое количество компаний сдают в аренду велосипеды, люди на них ездят, а потом попросту бросают, что ведет к захламлению города. Государство организовало стоянки на стадионах для сбора этих велосипедов, но и они уже переполнены. Брошенные велосипеды оказались никому не нужны – проще выпустить новый велосипед и поставить его опять на первую стоянку.

Таким образом, в больших городах ищут оптимальные решения для развития этой сферы.

Общественный транспорт

Чем больше людей будут ездить на общественном транспорте, тем меньше будет частных автомобилей на дорогах. Общественный транспорт вносит огромнейший вклад в снижение загрязнения и уменьшение количества пробок. Здесь в первую очередь требуются удобство и четкость расписания, слежения за транспортом: где он находится, с какой скоростью движется, когда прибудет в конкретную точку, то есть контроль в реальном времени и прогноз его движения. И это все завязано на информационных технологиях.

Мобильные сервисы

Уже обычным делом стало использование мобильных технологий, то есть использование мобильных устройств и новых приложений для заказа транспорта (информационное такси Uber, Яндекс.Такси и др.). В каждой стране существуют свои компании, которые этим занимаются, а также компании-интеграторы, собирающие всех под своим "зонтиком".

В последние годы на американском рынке инвестиции в мобильные сервисы растут, особенно их удалось привлечь компании Uber. В этой области частный капитал видит наибольшие перспективы зарабатывания денег.

Рассматриваются возможности перехода от индивидуального транспорта к использованию многомодального – когда можно пересаживаться с одного транспорта на другой очень быстро, точно зная свой маршрут, и когда много людей могут использовать одни и те же средства передвижения. Это активно применяется в корпоративном транспорте, когда заказываются небольшие автобусы, которые собирают людей и привозят их на работу. При таком подходе значительно сокращается трафик личного автотранспорта.

Общественные аспекты

Еще одно важное направление работы – это исправление ситуации с точки зрения утверждения правил оказания новых услуг и создания возможностей для их развития на муниципальном уровне.

Нововведения в технологиях в то же время вызывают и отторжение. Например, в Испании проходили забастовки и было сильное противодействие таксистов приходу Uber и других компаний – они не допустили их на свою территорию. Поэтому такси в Барселоне продолжают хорошо себя чувствовать. В других странах они вытесняются, поглощаются или меняют тактику. И здесь очень важно регулирование со стороны соответствующих служб муниципалитетов: что они хотят создать в своем городе, как они видят перспективу. Применяя новые технологии (информационные, мобильные приложения), развивая стартапы и четко определяя законы, можно легко регулировать развитие транспорта в каждом конкретном городе.

При этом нужно учитывать потребности населения, потребителей и автолюбителей – что

Самый кардинальный способ избавиться от машин – не ездить на них. Никольская улица в Москве уже давно стала пешеходной

Электронное табло делает общественный транспорт более привлекательным

им нужно? Куда они должны передвигаться, зачем они должны передвигаться? Может быть, им вообще не нужно передвигаться, а нужно перенести место работы поближе к жилью, и тем самым проблема будет решена?

Интерес со стороны инвесторов

Государство и очень крупный бизнес вкладывают большие инвестиции в развитие, например, железнодорожного транспорта: строительство высокоскоростных магистралей, запуск поездов без машинистов, автоматизацию контроля движения поездов (особенно грузового транспорта), логистику, компьютеризацию и автоматизацию системы, автоматизацию продажи билетов. В РЖД принята программа развития до 2025 г. с весьма амбициозными целями. Уже в 2018 г. начнется строительство высокоскоростной магистрали Москва – Казань.

Возможные ограничения во внедрении технологий

Серьезных ограничений в освоении технологий не наблюдается, наоборот, есть тенденция отхода от ограничений. К примеру, внедрена система "ЭРА ГЛОНАСС" экстренного реагирования при авариях. На все машины ставятся датчики, и в момент удара информация передается в экстренную службу, которая должна сразу приехать. За последние 5–7 лет труднейших переговоров удалось согласовать стандарты, по которым будут работать приборы, устанавливаемые в машины и работающие с ГЛОНАСС, кто и как их будет выпускать. Следующий этап – использовать эти технологии в коммерческих целях и передавать с их помощью дополнительную потребительскую информацию. Но на основе чего? Кто за это должен платить? По каким каналам передавать? Какие устройства ставить? Совместимы ли они с "ЭРА ГЛОНАСС"? Вот такие сейчас стоят вопросы и задачи.

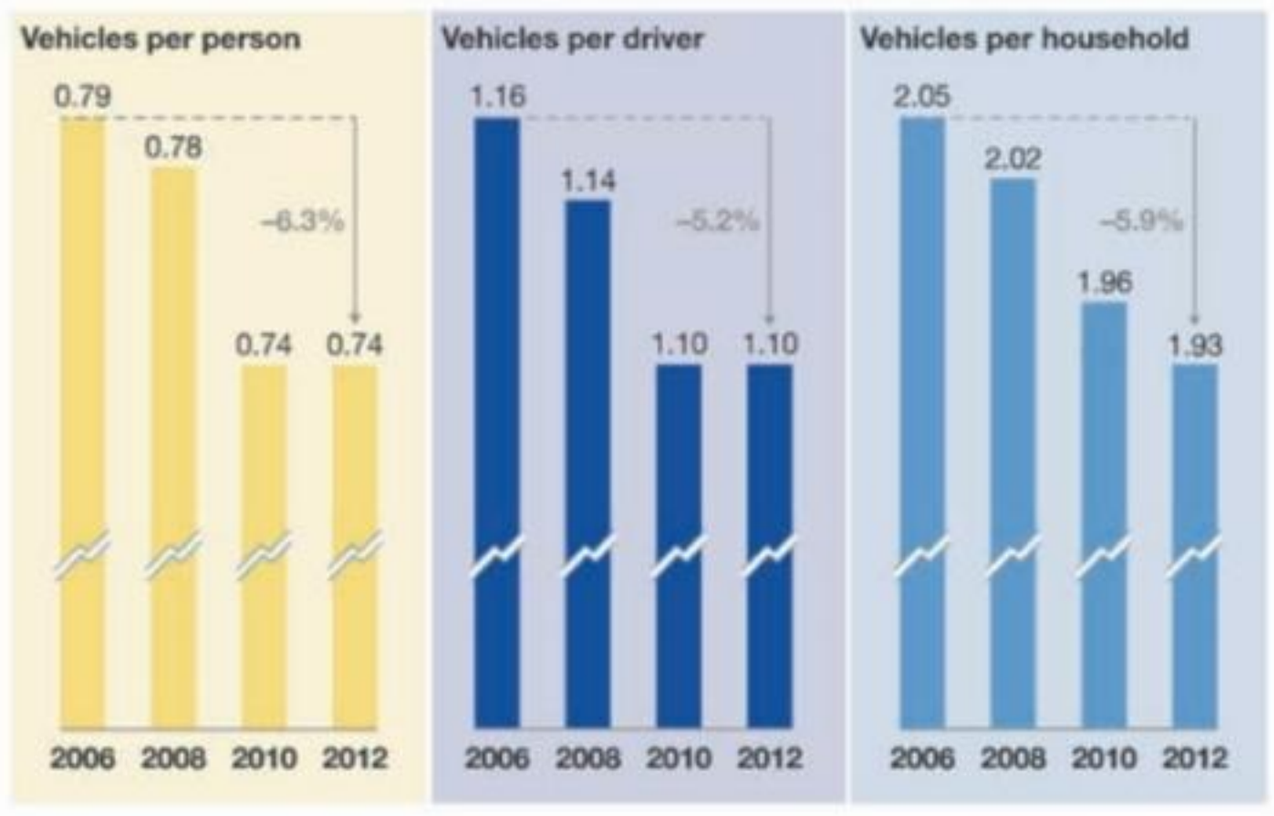


Рис.1. Снижение уровня владения авто в США

Роль облачных систем

Как показывает опыт разработки Oracle, для создания исключительно новых, ранее не применявшихся на практике услуг с использованием мощи современных информационных технологий идеально подходят облачные решения. Объяснение очень простое: заранее неизвестно, какая из услуг будет востребована большинством клиентов и потребует значительных вычислительных ресурсов. Поэтому очень важна гибкая и оперативная масштабируемость ИТ в любое время с обеспечением высокого качества, что возможно только в облаке. Постоянно покупать и продавать серверы – это лишние затраты денег, а оперативное масштабирование при высокой производительности можно получить сразу, благодаря облакам, и это самое доступное решение.

Общемировые тренды

В некоторых странах количество автомобилей уменьшается благодаря комплексу тенденций, описанных выше. Например, в США использование личного транспорта снижается как на отдельного человека, так и на домохозяйство. Но не все города одинаковы с этой точки зрения.

По исследованиям мировых агентств, их можно разбить на четыре крупных класса:

- устойчивые, старые, не очень большие (Хельсинки, Вена и др.);
- небольшие со значительным количеством личного транспорта (многие города США);
- развивающиеся – растущие большие мегаполисы, где большой приток населения, строится новое жилье и новые дороги (Москва, Шанхай, города Мексики);
- установившиеся мегаполисы – большие города, но уже стабильные (Лондон, Нью-Йорк, Токио).

Если посмотреть на эти "архетипы" городов, то можно увидеть, что все же в целом количество автотранспорта в пересчете на душу населения снижается. При этом растет использование новых технологических стартапов ("новой мобильности"), количество передвижений без автомобиля (пешеходные зоны, велосипеды) и происходит развитие общественного транспорта.

Таким образом, все рассмотренные тренды находят подтверждение практически во всех классах городов с небольшими вариациями (где-то в большей степени, где-то в меньшей), но везде – опираясь на информационные технологии.

Поиск универсального решения

В гибридной модели нового транспорта и заключается решение многих проблем. В современном мире это, прежде всего, будет зависеть от развития информационных технологий, от знания, где находится транспорт, кто на нем поехал, куда поехал, где его заправить, где находится электрическая розетка для автомобиля и т.д. Вот такое управление всем транспортом в реальном времени через информационные каналы, мне кажется, решит проблему перегруженности дорог в больших городах. ■

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

Аналитика как драйвер развития IoT и видеонаблюдения

Интернет вещей все теснее переплетается с повседневной жизнью людей. Коммерческие компании, государственные учреждения и потребители интересуются, как с его помощью можно получить новые преимущества и сделать быт намного комфортнее. По прогнозу Seagate и IDC, среднестатистический пользователь Интернета будет взаимодействовать с устройствами, соединенными с различными сетями, примерно 4800 раз в день, то есть каждые 18 секунд

Илья Яськов
Менеджер по развитию направления клиентских устройств компании Seagate Technology

Умный город Иннополис – крупномасштабный научно-технический проект федерального значения

Данные, которые активизируют деятельность мощных соединенных устройств нового поколения, уже начали кардинально менять наш мир. В России в 2015 г. появился новый умный город – Иннополис, крупномасштабный научно-технический проект федерального значения со специализацией в области высоких технологий. Здесь все элементы городской инфраструктуры, включая инженерные системы зданий, транспорт и коммунальные службы, подключены к единой интеллектуальной сети, на базе которой реализована общественная сеть Wi-Fi, система видеонаблюдения, средства управления городской средой, а также не загрязняющая воздух транспортная система, оснащенная комплексом датчиков, средствами мониторинга транспортных потоков и управляемыми светофорами.

Интернет вещей – неизведанная территория

Внедрение Интернета вещей окажется успешным, когда технологии будут "вплетены" в ткань повседневной жизни и для конечного пользователя он сможет оставаться невидимым. В результате возрастет количество как применяемых повсеместно цифровых гаджетов, так и автоматизированных источников данных – конечных устройств, генерирующих и передающих информацию. Неизбежность этих перемен является серьезным поводом для беспокойства, поскольку на первый план выходят следующие факторы:

- обеспечение безопасности и приватности создания, сбора и обработки данных;
- планирование начальных и последующих денежных затрат на инфраструктуру Интернета вещей, позволяющую извлекать пользу из данных;
- удовлетворение растущей потребности в построении экономики, основанной на интеллектуальной собственности, в рамках которой доход приносят творчество, инженерное проектирование и анализ данных.

Предприятия ждут от Интернета вещей в первую очередь возможности улучшения операционной эффективности и качества обслуживания клиентов. Например, компания Mastercard, меняясь по мере вхождения Интернета вещей в повседневную жизнь, адаптирует бизнес-модель, постепенно отказываясь от сделок "покупатель – продавец" и все больше ориентируясь на транзакции "продавец – устройство" и "устройство –устройство".

При этом инвестиции направляются на то, чтобы обеспечить бесперебойную связь вещей в рамках бизнес-процессов и взаимодействий с клиентами. Стремясь избавить своих клиентов от многократного ввода данных проверки подлинности, Mastercard разрабатывает систему единовременного входа и аутентификации, которая позволит соединяться с помощью устройств для защищенного обмена данными и совершения платежей.

Главное в Интернете вещей – аналитика

Эффективность Интернета вещей во многом зависит от доступности средств аналитики, ведь именно они помогают правительствам и коммерческим предприятиям извлекать пользу из собираемых данных.

К примеру, данные реального времени активно используются для картографических сервисов. Так, автомобильные навигаторы передают информацию о пробках, а информационная служба предоставляет водителям рекомендации по изменению маршрутов для объезда заторов. Обширные возможности открываются благодаря все более широкому использованию Интернета внутри транспортных средств с помощью смартфонов и бортовых компьютеров. Со временем технологии связи "автомобиль – автомобиль" и "автомобиль – инфраструктура" можно будет использовать для снижения количества ДТП.

Стремительно развивается и рынок сетевых регистраторов с системой видеоаналитики. В обозримом будущем нас ждет повсеместное применение систем искусственного интеллекта, в частности программ глубинного обучения, предназначенных для распознавания лиц, анализа аномалий поведения и других задач. Параллельно получат широкое распространение системы оперативного анализа видеозаписей, создающие повышенную нагрузку на хранилища сетевых видеорегистраторов. Это обусловливает необходимость в накопителях с высокой производительностью и улучшенными механизмами кеширования, мгновенным откликом и предвосходной скоростью произвольного чтения для быстрого поиска и анализа видеозаписей.

Где хранить все данные, которые мы создаем?

В технологической отрасли о взрывном росте данных заговорили еще несколько лет тому назад, но тогда он был обусловлен массовым распространением мобильных устройств, благодаря которому начал формироваться большой объем контента, создаваемого потребителями. Сегодня главной движущей силой этого роста становятся оконечные устройства Интернета вещей: емкость их хранилищ обычно ограниченна, поэтому генерируемую ими информацию нужно куда-то переносить для накопления и анализа.

Не всю информацию, сохраненную пользователями и устройствами, нужно анализировать, но правительства и коммерческие компании выдвигают жесткие требования в отношении безопасности, контроля затрат и соблюдения географических ограничений на размещение данных, поэтому операторам ЦОД и облачных сервисов нужны передовые решения для их хранения. Учитывая эту острую необходимость, мы продолжаем разрабатывать решения, ориентированные на помощь специалистам дата-центров, обеспечивая гарантированную производительность, безупречную надежность и максимальную безопасность. ■

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

КОЛОНКА РЕДАКТОРА

Дорожные штрафы как двигатель видеоаналитики

Говоря о транспорте, хочу затронуть тему придорожных камер ГИБДД. Именно они были и являются драйвером многих инноваций в видеонаблюдении. Основой системы является распознавание государственных регистрационных знаков. Современная камера распознавания номеров совмещена с импульсной системой инфракрасной (ИК) подсветки. ИК-диоды включаются только на время открытия электронного затвора камеры, что позволяет существенно увеличить их рабочий ток, а следовательно и дальность освещения. Программные модули распознавания автомобильных номеров всем известны и являются пионерами видеоаналитики.

На изображение "накладывается" информация с радара о скорости и иные необходимые данные. Далее в автоматическом режиме формируется то самое, ненавистное автомобилисту, "письмо счастья". Государство получает дополнительный доход и, что называется, входит во вкус.

Помимо превышения скорости есть еще масса нарушений, которые можно фиксировать с помощью автоматизированной системы видеонаблюдения. Возьмем, к примеру, остановку за стоп-линией. Нарушение довольно легко определяется системой. Доказательством остановки могут быть два стоп-кадра, разнесенные по времени на несколько секунд. Нарушение разметки и выезд на встречную полосу тоже можно зафиксировать. Проезд на красный свет светофора должен быть подтвержден кадром, в котором автомобиль будет запечатлен на перекрестке одновременно с горящим запретительным сигналом светофора. Ну и самое простое – идентифицировать в потоке автомобили с отсутствующими в базе данных страховыми полисами ОСАГО.

Теоретически любое нарушение правил дорожного движения можно определить с помощью системы видеонаблюдения в автоматическом режиме. К примеру, опасную езду можно распознать по частым перестроениям. Но встает другой вопрос: как составить квитанцию о штрафе? С последовательностью стоп-кадров? Это не слишком убедительно. Выходом может стать перевод квитанций в электронную форму. Тогда к ним вполне можно прицепить любой видеоролик. Весьма вероятно, что в будущем бумажные извещения о штрафах вообще уйдут в прошлое.

Михаил Арсентьев
Редактор раздела "Видеонаблюдение", коммерческий директор ООО "Артсек"

Привет из аналогового прошлого

Кибербезопасность и видеонаблюдение

Всеобъемлющий Интернет, или "Интернет всего", становится реальностью. Будучи его предтечей, видеонаблюдение стремительно развивалось последние 10 лет. Первое поколение аналоговых систем сменили цифровые, затем сетевые, наступает эра умных видеосистем. Технические достижения улучшают повседневную жизнь, но и создают вызовы для общества. Так, широкое распространение Интернета принесло новый уровень комфорта, но с комфортом пришли угрозы кибербезопасности. Аналогично с Интернетом вещей (IoT): улучшения, которые появились благодаря ему в жизни и бизнесе, сопровождаются новыми задачами. Одна из них – кибербезопасность

Ху Янгжонг
Президент компании Hangzhou Hikvision Digital Technology

Вне всякого сомнения, рынок видеонаблюдения должен двигаться вперед в соответствии с трендами цифровизации, сетевых и умных технологий. Открытые сети позволили связать между собой системы безопасности, которые прежде существовали обособленно и были полностью изолированными, а широкий доступ к данным и обмен информацией радикально влияют на управление бизнесом и быт. Однако кибербезопасность для видеонаблюдения стала абсолютно новой областью.

Процесс трансформации систем видеонаблюдения от аналоговых и изолированных, роль которых сводилась к получению данных, к цифровым, сетевым и умным выявил преимущества цифровой и сетевой революции. Но вместе с интернет-технологиями в видеонаблюдение пришли кибератаки. Более того, зачастую дефекты безопасности возникают в сетевой среде по причине того, что современные системы безопасности уходят корнями в традиционные системы.

Кибербезопасность не является проблемой конкретных стран или компаний. Все государства и организации должны понимать, что вопросы кибербезопасности равно важны для всех и требуют международного сотрудничества:

- по развитию стандартов кибербезопасности и применению лучших практик;
- по проведению научно-исследовательских работ для совершенствования защиты информационных систем;
- по анализу опыта потребителей с целью улучшения методик и технологий защиты.

Риски Интернета вещей

Угрозы и риски безопасности для Интернета вещей можно разделить на три уровня: устройства, сети и приложения.

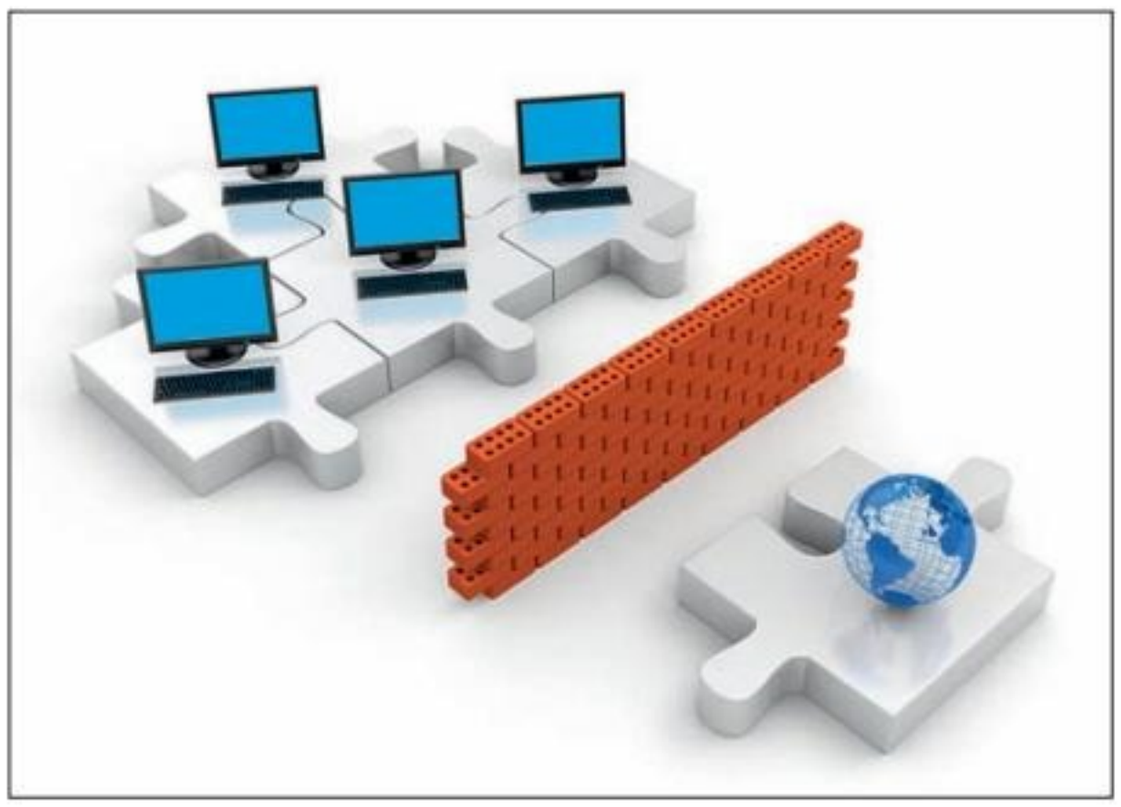
Угрозы уровня устройств

- Кража (или потеря) устройства в отсутствие физической защиты при удаленном размещении.
- Вмешательство в работу устройств, например уличных терминалов и распределенных систем.
- Атаки через известные уязвимости, такие как истекшая версия ОС или ПО.

Видеонаблюдение позже ИТ-рынка вступило в цифровую эру, поэтому специалисты в области видео, включая разработчиков оборудования и систем видеонаблюдения, в целом довольно слабо подкованы в вопросах кибербезопасности. Индустрия видеонаблюдения должна объединить усилия перед лицом киберугроз, которые несет Интернет вещей. Однако ответственность за безопасность в киберпространстве лежит не только на производителях технических средств. Каждый участник проекта по видеонаблюдению, в том числе конечный заказчик, системный интегратор, оператор связи, проектно-монтажная организация и другие поставщики услуг, отвечает за применение адекватных мер по кибербезопасности. Задача защиты от кибератак на 30% технологическая и на 70% управленческая; для борьбы с киберугрозами все организации и люди, вовлеченные в проект, должны работать сообща.

Истоки уязвимости видеонаблюдения

Последние пять лет были отмечены активной цифровизацией систем видеонаблюдения. Индустрия умного видео воплощала в реальность мечту об Интернете вещей и теперь находится в авангарде внедрения концепции IoT.



- Обход механизма аутентификации. Чревато в случае применения ненадежного пароля или пароля, установленного производителем по умолчанию.
- Кража конфиденциальной информации, хранящейся непосредственно на устройстве.
- Удаленное управление устройствами через Test- и Debug-порт. Debug-порт не имеет ограничений по пошаговой отладке кода, поэтому злоумышленники могут взять устройство под полный контроль посредством этого системного ресурса.
- Утечка персональных данных при их сборе, передаче или обработке с помощью устройств Интернета вещей.

Кибербезопасность не является проблемой конкретных стран или компаний. Все государства и организации должны понимать, что вопросы кибербезопасности равно важны для всех и требуют международного сотрудничества

Угрозы уровня сети

- Вторжения в беспроводную сеть. Дефекты беспроводных протоколов, например отсутствие эффективного метода аутентификации, могут привести к неавторизованному доступу к персональным данным.
- Атака, направленная на нешифрованный сетевой трафик, передающийся между устройствами, облаком и мобильными терминалами.
- Атаки на IP-системы из сети Интернет.
- DDoS-атаки.

Угрозы уровня приложений

- Трудности апгрейда и обеспечения безопасности различных устройств, управляемых на уровне платформы.
- Риски конфиденциальности и безопасности, вызываемые несанкционированным доступом.
- Отсутствие обновления или проверки настроек безопасности в течение продолжительного периода времени.

Если оценить множество скрытых рисков безопасности аппаратных и программных средств IoT, а также сетевого окружения, становится очевидно, что будущее за системами видеонаблюдения, построенными на основе концепции Интернета вещей и многомерной защите оконечных устройств, данных, приложений и сетей.

Пять постулатов цифрового мира

Аналоговые системы видеонаблюдения строились на закрытых сетях, и производители сосредотачивали свои усилия на создании простой в применении продукции с высокими эксплуатационными характеристиками и приемлемой ценой. Защищенность от кибератак не была критичным условием. Но в процессе стремительного перехода на сетевые технологии недостаток внимания вопросам кибербезопасности привел к тому, что главные достоинства аналоговых систем – удобство и простота использования – начали затмевать несоответствие требованиям защиты от информационных угроз в цифровую эпоху.

Индустрия видеонаблюдения не так давно столкнулась с проблемами кибербезопасности, причина того кроется в особенностях эволюционного развития технических средств. Однако это не означает, что рынок настолько уязвим, как считают некоторые эксперты. Ведущие вендоры ведут скоординированную работу по борьбе с потенциальными рисками безопасности и уже довольно эффективно защищают свои решения.

Объективно говоря, проблема кибербезопасности не является специфичной для видеонаблюдения. Это проблема общества в целом. На рынке ИТ задачи кибербезопасности наблюдаются повсеместно. Можно выделить пять базовых постулатов.

1. Уязвимости широко распространены

Нет таких ИТ-систем или технических средств, которые бы не имели уязвимости. Более того, уязвимости весьма распространены. Каждый ИТ-продукт содержит в себе миллион строк кода, достаточно одной ошибки, чтобы создать угрозу всей системе. Не существует универсального автоматического или ручного способа обнаружить все потенциальные проблемы кибербезопасности ни в автоматическом, ни в ручном режиме.

Защищать следует систему целиком

Чтобы защитить систему видеонаблюдения, камеры, регистраторы, серверы, ПО, сетевое оборудование и инфраструктура должны взаимно дополнять друг друга, чтобы обеспечить всестороннюю безопасность решения. Проблема защищенности любого элемента может отразиться на всей системе.

Безопасность открытых библиотек под вопросом

Во многих системах видеонаблюдения используются инструменты популярных открытых библиотек. Они общедоступны и бесплатны, но зачастую таят в себе огромные риски безопасности. За последние годы в разных криптографических библиотеках, таких как Struts2 и OpenSSL, были обнаружены несколько серьезных уязвимостей. Многие инструменты открытых библиотек применяются в различных информационных системах нижнего уровня. Поэтому любые уязвимости создают угрозу для целых отраслей, а не систем или продуктов.

Безопасность находится в подвижном равновесии

Нет такого понятия, как "абсолютная безопасность". Безопасность всегда относительна. Технические решения и приемы, которые сегодня считаются безопасными, завтра могут оказаться ненадежными. Иначе говоря, в безопасности нельзя достичь конечной цели. Каждое техническое средство будет сталкиваться с проблемами защищенности на протяжении своего жизненного цикла.

Управление системой должно быть адекватным

Важнейшим элементом системы безопасности является человек. Если пользователь не способен адекватно управлять даже хорошо защищенной системой, ее безопасность находится под вопросом. Многие инциденты безопасности в системах видеонаблюдения связаны именно с неадекватной эксплуатацией и управлением, например со слабыми паролями, отсутствием файрволов или аппаратных средств защиты. Кибербезопасность должна войти в привычку пользователей: следует регулярно знакомиться с уведомлениями от производителей, обновлять ПО до новейшей версии и своевременно устанавливать патчи. ■

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

Евгений Озеров
Ведущий инженер
ЗАО НВП "Болид"

Как автоматизировать проектирование систем видеонаблюдения?
В поисках волшебного рецепта

Будущее наступило: роботы заменяют труд людей, ведутся работы над прикладными аспектами создания искусственного интеллекта; многие профессии становятся неактуальными. Аналогичные процессы идут и в сфере проектирования. И не стоит этого бояться – эффективность труда возрастает, мы можем решать все более сложные и творческие задачи. А повторяющиеся рутинные операции можно и нужно упрощать для человека, автоматизируя их с помощью современных программных продуктов, облачных сервисов, CAD- и BIM-систем

В данной статье мы рассмотрим те аспекты автоматизации проектирования системы видеонаблюдения, которые можно внедрить в своей работе уже сегодня, чтобы оставаться конкурентоспособным на рынке труда в новое время.

Шаги проектировщика: от постановки задачи до оформления результатов проектирования

Проектирование – это сложная, комплексная задача, состоящая из принятия основных технических решений (ОТР) и оформления данных решений в соответствии с требованиями нормативно-правовых актов (НПА), постановлений и распоряжений Правительства РФ – прежде всего проектной и рабочей документации. Часть задач можно и нужно автоматизировать. Рассмотрим подробней шаги проектировщика на пути к оформленному проекту и возможности автоматизации решаемых задач.

Шаг 1. Определение проблемы

"Если лестница приставлена не к той стене, то сколько бы ступенек вы ни одолели, все равно придете не туда" (Стивен Кови). Это действительно так. Поэтому прежде чем приступить к проектированию, необходимо определить проблему или задачу, которую мы собираемся решить в процессе проектирования. Подробно данный шаг описан в британских рекомендациях полиции CCTV Operational Requirements Manual. В данной статье не будем углубляться в эту тему. Стоит лишь заметить, что данный шаг нельзя автоматизировать: сбор информации и ситуационный анализ требует квалифицированного труда проектировщика.

Шаг 2. Определение цели наблюдения

На втором этапе мы должны определить цели наблюдения. Цели должны быть логически связаны с задачами, определенными на первом шаге. Существуют рекомендации, позволяющие перевести язык эксплуатационных требований в количественные характеристики изображения, получаемого на экране монитора охраны. Руководствоваться можно как российскими рекомендациями МВД Р 78.36.008–99, так и европейскими EN 50 132–7 или британскими Home Office Scientific Development Branch 2009. После этого имеет смысл зафиксировать полученные данные в виде задания на проектирование (ТЗ). В ряде случаев задание на проектирование должно быть оформлено согласно требованиям ГОСТ Р 57839–2017 "Производственные услуги. Системы безопасности технические. Задание на проектирование. Общие требования" (вступают в силу 1 июня 2018 г.). Данный шаг также невозможно автоматизировать. Как правило, его выполняет техническая служба заказчика либо сам проектировщик по поручению заказчика для последующего согласования.

Шаг 3. Определение параметров зон обзора

После второго шага мы знаем конкретно, что хотим получить на экране монитора охранника. Теперь нам необходимо собрать данные по параметрам зон обзора, чтобы на следующем этапе путем простых вычислений получить необходимые характеристики камеры: фокусное расстояние и разрешение матрицы. То есть на шаге 3 мы собираем исходные данные для следующего шага, на котором уже можно выбрать конкретную модель камеры.

Существует не так много параметров, которые полностью определяют положение камеры относительно объекта съемки:

- высота установки камеры;
- высота верхней границы зоны обзора;
- расстояние до верхней границы зоны обзора.

Для каждой цели наблюдения мы определяем возможные места установки камеры и, исходя из этого, перечисленные выше параметры. Автоматизация – стандартными средствами CAD-систем, такими как AutoCAD, NanoCAD, ZWCAD и др.

Шаг 4. Основные решения по камере: место расположения, фокусное расстояние, разрешение матрицы

Итак, мы уже примерно выбрали место расположения нашей камеры и знаем основные параметры зоны обзора. На четвертом шаге нужно рассчитать фокусное расстояние и разрешение матрицы. Это можно сделать и с помощью обычного калькулятора по формулам, приведенным в Р 78.36.008–99:

Углы зрения объектива по горизонтали (аг) и вертикали (ав) определяют по формулам:

$$\alpha_в = 2 \cdot arctg\left(\frac{V}{D}\right),\ \alpha_г = 2 \cdot arctg\left(\frac{H}{D}\right),$$

где V, H – поле зрения объектива соответственно по горизонтали и вертикали, м;

D – расстояние до объекта контроля, м.

Затем определяют фокусное расстояние объектива (f):

$$f_1 = \frac{H}{2} \cdot tg\left(\frac{\alpha_г}{2}\right),\ f_2 = \frac{V}{2} \cdot tg\left(\frac{\alpha_в}{2}\right),$$

где V и H – размер ПЗС-матрицы по горизонтали и вертикали, мм;

f_1, f_2 – фокусные расстояния объектива, мм.

Далее определяют минимальную деталь объекта контроля, которая может различаться с помощью выбранных камеры и объектива:

$$S_H = \frac{2000 \cdot D}{R} \cdot tg\frac{\alpha_г}{2},\ S_V = \frac{2000 \cdot D}{625} \cdot tg\frac{\alpha_в}{2},$$

где R – разрешение телевизионной камеры (в данной формуле имеется в виду разрешение в ТВЛ);

D – расстояние до объекта контроля, м;

S_H, S_V – размеры минимально различимой детали (МРД) по горизонтали и вертикали, мм.

После этого рассчитанное значение размера МРД сравнивают с показателями для решаемой данной камерой задачи (как правило, это идентификация, различение или обнаружение по классификации Р 78.36.008–99 либо аналогичные критерии иностранных рекомендаций, приведенные в рекомендациях МВД Р 78.36.008–99, EN 50 132–7 либо Home Office Scientific Development Branch 2009). Выбор документа – в зависимости от требований заказчика, прописанных в задании на проектирование.

Данные расчеты позволяют примерно очертить круг подходящих камер, а также оптимизиро-

вать расположение камеры на объекте по сравнению с шагом 3. Данный шаг – крайне трудозатратный для проектировщика. Безусловно, его можно и нужно автоматизировать. Есть два основных способа автоматизировать данную задачу без покупки дополнительного программного обеспечения: использовать бесплатные утилиты или онлайн-сервисы производителей оборудования (существует бесплатное программное обеспечение – калькуляторы от производителей ПО для проектирования видеонаблюдения) либо создать/использовать готовую инструментальную палитру динамических блоков для CAD-систем, содержащих углы обзора с учетом мертвой зоны и распределение пространственного разрешения от камеры видеонаблюдения до потенциального объекта съемки.

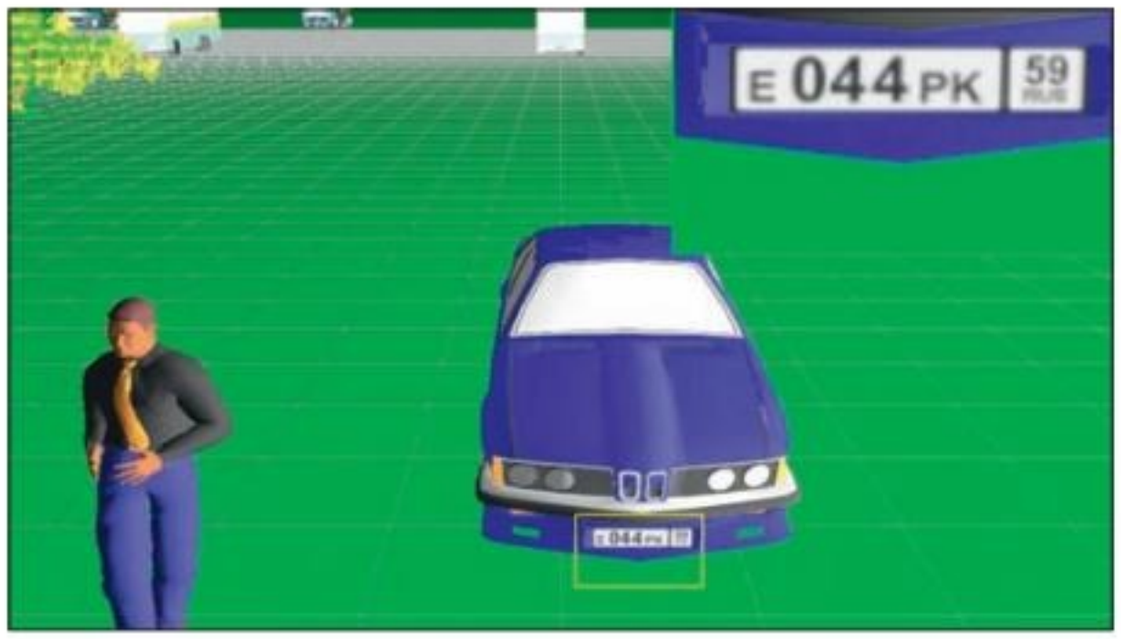
Шаг 5. Учет неочевидных моментов: освещенность, контраст и скорость цели наблюдения, глубина резкости

Для того чтобы окончательно определиться с выбором конкретной модели, нужно учесть дополнительные факторы, которые важны для решения именно этой задачи. В зависимости от места установки камеры, условий съемки, объекта съемки бывает необходимо учесть параметры:

- чувствительности;
- глубины резкости;
- настройки диафрагмы и затвора;
- дисторсию объектива и др.

Кроме того, часто требуется учесть затенение зоны обзора препятствиями (при этом нужно помнить о высоте препятствия и о высоте установки камеры). Многие из приведенных условий на практике посчитать без использования специализированного программного обеспечения просто невозможно.

Автоматизация для данного шага не просто необходима, она еще и увеличивает скорость работы проектировщика, поднимает степень проработанности принимаемых решений на совершенно другой уровень.



Моделирование изображения с камеры видеонаблюдения

Шаг 6. Выбор структуры и компонентов ЛВС. Расчет архива

Следующий шаг после выбора расположения и параметров камер – построение локальной вычислительной сети (ЛВС) и при необходимости – структурированной кабельной системы (СКС). На этом же шаге мы рассчитываем потребности в архиве видеонаблюдения. Возможная структура сети и подходы к построению известны и многократно описаны в специализированной литературе. Тем не менее без понимания специфики объекта грамотно построить ЛВС невозможно, поэтому данный этап слабо поддается автоматизации. Другое дело – подсчет архива и проектирование СКС.

Расчет архива можно и нужно автоматизировать, хотя и тут существует доля субъективности и опыта проектировщика – современные межкадровые кодеки сжатия видеосигнала дают слишком большой разброс требуемой "ширины" канала Ethernet, к тому же битрейт, как правило, переменный (VBR – Variable Bit Rate). Поэтому возможны "всплески" трафика, что заставляет проектировщика закладывать при проектировании существенный запас производительности ЛВС.

Таблица. Основные направления и возможности автоматизации проектирования системы видеонаблюдения

№ пп	Задача проектировщика	Можно ли автоматизировать?	Что автоматизируем?	Чем автоматизируем?
1.	Определение проблемы	Нет	–	–
2.	Определение цели наблюдения	Нет	–	–
3.	Определение параметров зон обзора	Да	Расчеты: высота установки камеры высота верхней границы зоны обзора расстояние до верхней зоны обзора	Стандартные средства CAD-систем Специализированное ПО
4.	Основные решения по камерам	Да	Расчеты: фокусное расстояние разрешение матрицы Выбор: расположение камеры	Бесплатные утилиты или онлайн-сервисы производителей оборудования Создать/использовать готовую инструментальную палитру динамических блоков для CAD-систем Специализированное ПО
5.	Учет неочевидных моментов: освещенность, контраст и скорость цели наблюдения, глубина резкости	Да	Выбор: светочувствительность камеры F-число объектива глубина резкости время экспозиции расположение прожекторов	Специализированное ПО
6.	Выбор структуры и компонентов ЛВС. Расчет архива	Да	Расчеты: битрейт с камер емкость архива	Бесплатные утилиты или онлайн-сервисы производителей оборудования
7.	Выбор ПО, сервера, проектирование поста наблюдения	Да	Определение требуемых характеристик видеосервера	Бесплатные утилиты или онлайн-сервисы производителей оборудования
8.	Выполнение кабельного журнала, спецификации	Да	Расчеты: подсчет длин кабельных линий подсчет количества используемого оборудования	Стандартные средства CAD-систем
9.	Оформление документации	Да	Автоматизация: оформление штампов простановка номеров страниц другое	Стандартные средства CAD-систем

Проектирование системы распознавания автомобильных номеров

Автоматизация процесса проектирования СКС – это, прежде всего, заполнение кабельного журнала; маркировка оборудования; расчет коробов, лотков; учет в спецификации оборудования из баз данных производителей СКС, шкафов и кабеленесущих систем.

Резюмируем: автоматизировать проектирование архива и ЛВС можно и нужно, но без опыта проектировщика эти инструменты могут давать огромные погрешности вычислений.

Расчет ЛВС и архива

Основным способом является использование бесплатных утилит или онлайн-сервисов производителей оборудования.

Шаг 7. Выбор ПО, сервера, проектирование поста наблюдения

Выбор программного обеспечения (ПО) напрямую связан с первым шагом – постановкой задачи. Именно задача, решаемая системой видеонаблюдения, определяет то, какие функциональные модули программного обеспечения будут востребованы в конкретном проекте. Кроме того, на выбор ПО влияют размеры системы, выбор вендора камер и многие другие нюансы. Определение требуемых характеристик видеосервера – задача более формализуемая. Минимальные требования к характеристикам видеосервера, как правило, известны из рекомендаций производителя. Для выбора конкретного сервера требуется учитывать количество каналов на запись и отображение, параметры видеопотоков, необходимость использования ресурсов процессора и видеокарты на дополнительные видеоаналитические функции и т.п. Основным способом автоматизации процедуры выбора сервера является использование бесплатных утилит или онлайн-сервисов производителей оборудования.

Более специфическая задача – это проектирование поста наблюдения. Без ручного труда проектировщика тут, увы, не обойтись. Требуется учесть особенности построения интерфейсов "человек – машина", эргономику рабочего места, алгоритм работы оператора видеонаблюдения и многое другое. Автоматизировать данную работу можно лишь частично, например можно смоделировать подробность изображений от камер в полиэкране, возможность вывести изображения с разных камер в разном размере, выбрать оптимальное количество и размеры мониторов, а также оптимальное расстояние наблюдения за этими мониторами с учетом особенностей проектируемой системы видеонаблюдения.

Шаг 8. Выполнение кабельного журнала, спецификации

После того как мы приняли все основные технические решения (ОТР), наступает этап подсчета количества требуемого оборудования, кабельной продукции, расходных материалов. Требуется заполнить кабельный журнал, подготовить спецификацию оборудования и материалов. Данный шаг идеально подходит для автоматизации ручного труда проектировщика, что может серьезно повысить производительность работы.

Расчет кабельного журнала

Основным способом является использование встроенных в CAD-системы функций учета длин линий (простой способ) либо написание небольших программ на языках типа LISP (более сложный вариант).

Расчет спецификации

CAD-системы, как правило, позволяют извлекать из чертежей количество и атрибуты блоков, что позволяет достаточно быстро подготовить спецификацию. Более сложный вариант – полностью автоматизировать данный процесс за счет написания программы на языках типа LISP.

Шаг 9. Оформление документации

Работа проектировщика не ограничивается принятием ОТР. Кроме этого, данные решения должны быть грамотно оформлены в виде проектной или рабочей документации. Работы по оформлению рабочей документации также могут и должны быть автоматизированы.

Автоматизация оформления документации

CAD-системы, как правило, имеют развитый инструментарий для оформления итоговой документации. Необходимо только уметь грамотно пользоваться функционалом "Модель" и "Лист(ы)", "Видовые экраны", "Внешняя ссылка", "Поле", "Подшивки" и др.

Повышаем качество проектных решений

Несмотря на наличие большого числа различных бесплатных инструментов для проектирования видеонаблюдения, специализированное программное обеспечение пользуется спросом. Дело в том, что платные инструменты проектирования имеют функционал, значительно повышающий возможности проектировщика по оптимизации и обоснованию основных технических решений. Ну и, конечно, автоматизация рутины – также важный вектор усилий тех компаний, которые производят данное ПО.

Модель объекта, а не просто подложка

Одним из главных отличий современных специализированных CAD-систем проектирования видеонаблюдения является наличие простых и эффективных инструментов получения 3D-модели объекта из двухмерной подложки. Это позволяет учитывать высоту установки камер, влияние затенений от препятствий на зону обзора камеры, визуально оценивать правильность установки камер с учетом особенности объекта.

Визуализация расчетов: попытка понять друг друга

Вторым важным фактором, играющим на популярность CAD-систем проектирования видеонаблюдения, является возможность моделировать изображение с проектируемой камеры в окружении 3D-модели объекта и дополнительных 3D-моделей людей, автотранспорта, турникетов, шлагбаумов, элементов мебели для офиса и т.п. Это позволяет согласовать расположение и характеристики камер с заказчиком на понятным ему языке без углубления в специализированные термины.

Учет неучитываемого: расчет и обоснование выбора неочевидных параметров камер

Кроме вышеперечисленного, некоторые платные программные продукты для проектирования систем видеонаблюдения позволяют рассчитать и учесть в проекте совсем не очевидные моменты, которые без такого софта просто не учитывались бы при проектировании либо учет данных факторов носил бы эмпирический характер, основанный на опыте проектировщика. Основные факторы, которые позволяет учесть CAD-система проектирования:

- освещенность на объекте;
- светочувствительность камеры, степени раскрытия диафрагмы объектива (F-число);
- влияние движения объекта (смаз из-за движения) при заданном времени экспозиции;
- влияние дисторсии объектива на распределение пространственного разрешения;
- затенение препятствиями зоны обзора с учетом высоты установки камер и высоты препятствий и др.

Безусловно, наличие такого инструментария позволяет повысить точность принятия проектных решений на несколько порядков и, что немаловажно, – обосновывать принятые решения. ■

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

TRASSIR®

ЭКОСИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

5 В 1

ЗАКАЖИТЕ ПО ТЕЛЕФОНУ ИЛИ ЧЕРЕЗ САЙТ
бесплатную удаленную демонстрацию возможностей TRASSIR

+7 (495) 104-20-71

www.dssl.ru/DEMO

Расширение линейки видеонаблюдения компании BOLID: что нового?

Линейка оборудования для видеонаблюдения компании "Болид" была выпущена в продажу в апреле 2017 г. и насчитывала 69 позиций. Для рынка этого оказалось недостаточно, возникла необходимость в расширении ассортимента. Давайте рассмотрим, какие новинки были добавлены

Значительное расширение получили линейки видеокамер и регистраторов – как сетевых, так и аналоговых, а также была проведена определенная работа по модернизации существующих моделей.

Сетевые видеокамеры

Основное расширение линейки пришлось на позиции в 2 Мпкс. Три камеры с вариофокальным объективом в разрешении 2 Мпкс были самыми ожидаемыми новинками:

- цилиндрические VCI-120 и VCI-120-01;
- купольная VCI-220.

Камеры получили матрицу размером 1/2,8" и увеличенный диапазон изменения фокусных расстояний f = 2,7–13,5 мм. Традиционно практически все камеры компании оснащаются модулями PoE и ИК-подсветкой, но эти модели дополнительно получили возможность использования самого современного кодека H.265, что делает их по-настоящему универсальными для решения большинства задач видеонаблюдения. Дополнительно камера VCI-120-01 имеет моторизированный объектив, что позволяет настраивать ее изображение удаленно по сети.

Бюджетные цилиндрические камеры пополнились моделью VCI-122, которая обладает объективом с коротким фокусным расстоянием f = 2,8. Это дает ей горизонтальный угол обзора 110 град. Ее назначение – широкий обзор с близкого расстояния, например для наблюдения придомовой территории дач и коттеджей, площадки перед входом в здание.

Появились две внутренние поворотные камеры, но в классическом купольном корпусе. Это модели VCI-627-00 с 4-кратным оптическим увеличением и VCI-628-00 с 20-кратным оптическим увеличением. С помощью этих камер можно решать задачи детализации изображения для наблюдения больших залов в банках, офисах, гостиницах, магазинах, складах и цехах.

В новой линейке не смогли обойти вниманием мировой тренд развития камер с разрешением 4K (Ultra HD). Это отразилось в разработке следующих моделей:

- цилиндрическая VCI-180-01;
- купольная VCI-280-01.

Сводная таблица характеристик сетевых видеокамер

Форм-фактор	Корпусные	Кубические	Цилиндрические			Купольные, EyeBall			Мини-купольные	Купольные FishEye	Поворотные	Высокоскоростные поворотные		
														
Объектив / Разрешение, Мпкс	-	Фиксированный	Фиксированный	Вариофокальный	Вариофокальный моторизированный	Фиксированный	Вариофокальный	Вариофокальный моторизированный	Фиксированный	Фиксированный	Вариофокальный	Вариофокальный		
до 1,3		VCI-412 f = 2,8	VCI-113 f = 3,6 TCI-111 f = 9; 13; 25; 35			VCI-212 f = 2,8								
2	VCI-320		VCI-122 f = 2,8 VCI-123 f = 3,6	VCI-120 f = 2,7–13,5	VCI-120-01 f = 2,7–13,5 VCI-121-01 f = 4,7–47	VCI-222 f = 2,8	VCI-220 f = 2,7–13,5	VCI-220-01 f = 2,8–12	VCI-722 f = 2,8		VCI-627 f = 2,7–11 VCI-627-00 f = 2,7–11 VCI-628-00 f = 5,3–64	VCI-528-00 f = 4,8–120	VCI-528 f = 4,8–120	VCI-529 f = 6180 VCI-529-06 f = 6–180
3		VCI-432 f = 2,8		VCI-130 f = 2,8–12			VCI-230 f = 2,8–12	VCI-830-01 f = 2,8–12						
4			VCI-143 f = 3,6		VCI-140-01 f = 2,8–12	VCI-242 f = 2,8		VCI-240-01 f = 2,8–12	VCI-742 f = 2,8					
5										VCI-252-05 f = 1,44				
8			VCI-184 f = 4,0	VCI-180-01 f = 2,7–12		VCI-884 f = 4,0	VCI-180-01 f = 2,7–12							

Сводная таблица характеристик сетевых видеорегистраторов

Каналы видео	Диски						
	1		2		4		8
	Без PoE	С PoE	Без PoE	С PoE	Без PoE	С PoE	Без PoE
4	RGI-0412	RGI-0412P04					
8	RGI-0812	RGI-0812P08		RGI-0822P08	RGI-0848		
16	RGI-1612		RGI-1622	RGI-1622P16	RGI-1648	RGI-1648P16	RGI-1688
32			RGI-3228		RGI-3248		RGI-3288
64					RGI-6448		RGI-6488

Сводная таблица характеристик аналоговых видеокамер

Форм-фактор	Корпус-ные	Цилиндрические			Купольные, EyeBall		Мини-купольные	Высокоскоростные поворотные	
									
Объ-ектив / Разре-шение, Мпкс		Фикси-рован-ный	Вario-фокаль-ный	Вario-фокальный моторизи-рованный	Фикси-рован-ный	Вario-фокаль-ный	Фикси-рован-ный	Вario-фокаль-ный	Вario-фокаль-ный
До 1,3	VCG-310	VCG-113 f = 3,6			VCG-812 f=2,8				
2	VCG-320	VCG-122 f = 2,8 VCG-123 f = 3,6	VCG-120 f = 2,8–12	VCG-120-01 f = 2,8–12	VCG-222, VCG-822 f = 2,8	VCG-220 f = 2,8–12	VCG-722 f = 2,8 VCG-726 f = 6	VCG-528 f = 4,8–120	VCG-528-00 f = 4,8–120

Сводная таблица характеристик аналоговых регистраторов

Каналы видео	Диски			
	1		2	
	Запись 720p	Запись 1080p	Запись 720p	Запись 1080p
4	RGG-0411	RGG-0412		
8	RGG-0811	RGG-0812		RGG-0822
16	RGG-1611			RGG-1622

Обе модели имеют вариофокальный моторизированный объектив.

Высокоскоростные поворотные камеры компании "Болид" расширили свой список за счет проектной модели с 30-кратным увеличением, которая оснащена дворником.

Еще одна новинка – тепловизор BOLID TCI-111. Выпускается с пятью вариантами фиксированных фокусных расстояний: 9, 13, 19, 25 и 35 мм. Тепловизор имеет два интерфейса: сетевой для подключения к локальной вычислительной сети (ЛВС) и аналоговый для подключения к старым системам с существующей коаксиальной кабельной инфраструктурой (поддерживаются форматы PAL, NTSC и HD-CVI).

Это позволяет подключать BOLID TCI-111 ко всем видеорегистраторам "Болид" – как к сетевым, так и к гибридным.

Сводная таблица характеристик взрывозащищенных кожухов

Наличие ИК-подсветки	1 – ИК-подсветки нет			2 – ИК-подсветка есть		
Полезный внутренний объем / Материал корпуса	А – алюминиевый сплав	М – оцинкованная сталь	Н – нержавеющая сталь	А – алюминиевый сплав	М – оцинкованная сталь	Н – нержавеющая сталь
1 – ø56x60 мм	-	-	-	ТК-Ex-1A2	-	ТК-Ex-1H2
2 – ø90x110 мм	-	-	-	ТК-Ex-2A2	-	ТК-Ex-2H2
3 – 65x65x210 мм	ТК-Ex-3A1	-	-	-	-	-
4 – 70x70x190 мм	-	ТК-Ex-4M1	ТК-Ex-4H1	-	-	-
5 – 85x85x210 мм	-	ТК-Ex-5M1	ТК-Ex-5M2	-	ТК-Ex-5H1	ТК-Ex-5H2

Сетевые видеорегистраторы

Появился новый класс сетевых регистраторов – 8-дисковые RGI-1688, RGI-3288, RGI-6488 на 16, 32 и 64 камеры соответственно и с пропускной способностью 320 Мбит/с каждый. Эти три модели пока единственные во всей линейке будут поддерживать технологии RAID 0, RAID 1, RAID 6, RAID 10.

4-дисковые регистраторы без поддержки PoE получили расширение в сторону младших моделей на 8, 16 и 32 камеры соответственно. Как и ранее существовавшая модель в классе 4-дисковых регистратров RGI-6448, новые модели RGI-0848, RGI-1648 и RGI-3248 при пропускной способности 320 Мбит/с каждая имеют функционал поддержки по HDMI двух мониторов и "сухие" контакты.

Две новинки у регистраторов с PoE. Это 8-канальная двухдисковая модель RGI-0822P08 и 16-канальная 4-дисковая модель RGI-1648P16.

Аналоговые видеокамеры

В линейку аналоговых камер были добавлены три модели, оснащенные моторизированными вариофокальными объективами:

- цилиндрическая VCG-120-01;
- купольная VCG-220-01;
- VCG-820-01 в корпусе EyeBall.

Все три камеры имеют разрешение 2 Мпкс. Управление объективом осуществляется по коаксиальному кабелю, через меню регистратора.

Ассортимент камер с ручным вариофокальным объективом гармонично дополнился моделью VCG-820 в корпусе EyeBall.

Внутренние аналоговые камеры также получают новый класс корпусов в свою линейку – это мини-купольные камеры с фиксированными объективами VCG-722 (f = 2,8) и VCG-726 (f = 6). Узкий горизонтальный угол в 53 град. дает камере VCG-726 возможность использования ее в узких коридорах – в этом ее преимущество перед VCG-722. Корпусные камеры дополнены моделью VCG-320 с большим разрешением 2 Мпкс.

Бюджетные аналоговые цилиндрические камеры пополнились новой моделью – VCG-122, которая имеет объектив с коротким фокусным расстоянием f = 2,8. Это дает ей горизонтальный угол обзора 106 град. и широкий обзор на близком расстоянии.

Аналоговые видеорегистраторы

В линейку аналоговых видеорегистраторов добавлена одна модель RGG-0822 – 2-дисковый регистратор на восемь камер. В отличие от предыдущих моделей линейки, RGG-0822 позволяет записывать изображение со звуком – этот функционал имеется в аналоговой камере VCG-822. В течение последующих двух лет все модели аналоговых регистраторов также будут модернизированы и получат функцию работы со звуком. ■

Видеть сквозь препятствия

Что могут технические системы охраны?

Современные тепловизоры обладают широкими возможностями. В темное время суток и в сложных атмосферных условиях они показывают самую высокую эффективность в охранном видеонаблюдении. Там, где требуется действительно ночное видение, тепловизор зачастую оказывается лучшим решением с технической точки зрения. А совмещение его с видеокамерой делает ТВМ практически незаменимым средством наблюдения и охраны

Владимир Попов
Генеральный директор
АО "ОКБ "АСТРОН"

Константин Аношин
Начальник отдела германиевой оптики
АО "ОКБ "АСТРОН"

Новые достижения науки и техники привели к появлению в составе технических средств охраны (ТСО) камер, способных работать в режиме прибора ночного видения (ПНВ). Все ПНВ (кроме тепловизионных) используют один и тот же принцип – фокусировку и усиление света до уровня, различимого человеческим глазом. Основным недостатком таких систем является то, что они не способны эффективно работать в условиях полной темноты. В этом случае ПНВ использует дополнительный источник освещения – инфракрасный или лазерный прожектор (ИК-подсветка). ИК-подсветка позволяет расширить диапазон применения камер видеонаблюдения в ночном режиме. Но любые классические приборы ночного видения будут практически бесполезными в туман, сильный дождь, при снегопаде. К тому же они не помогут рассмотреть объект, скажем человека, который скрыт за препятствием, например в кустах. Опять же, в классических камерах с возможностью ПНВ максимальная дальность наблюдения составляет не более нескольких сотен метров. Для случаев, когда охраняемая зона имеет большую дальность, разработаны тепловизионные камеры наблюдения, называемые тепловизионными модулями (ТВМ).

Важнейшие элементы тепловизоров

Современные модели ТВМ обладают высокой точностью и замечают изменения в поле зрения в пределах сотых долей °С. Они могут осуществлять эффективное видеонаблюдение в условиях тумана и дождя, а также способны засечь объект, двигающийся в густых зарослях или кустах.

Современные модели ТВМ обладают высокой точностью и замечают изменения в поле зрения в пределах сотых долей °С. Они могут осуществлять эффективное видеонаблюдение в условиях тумана и дождя, а также способны засечь объект, двигающийся в густых зарослях или кустах

Общая схема любого тепловизора выглядит достаточно просто (рис. 1). Для фокусировки ИК-излучения используют линзы из оптического германия (рис. 2), прозрачного в области 2–15 мкм.

Вторым важнейшим элементом тепловизора является детектор, который может быть охлаждаемым и неохлаждаемым. Системы на детекторах первого типа обычно применяются в составе специализированных систем наблюдения, например на боевых кораблях и вертолетах, в аэропортах и т.д. Неохлаждаемые детекторы используются гораздо чаще, в этой роли, как правило, выступает микроболометр (болометрический сенсор). Основным его элементом является высокочувствительная полупроводниковая пластинка, изменяющая свои характеристики электрического сопротивления при колебаниях собственной температуры, которая, в свою очередь, зависит от количества ИК-излучения, попадающего на поверхность сенсора.

Максимальное разрешение современных серийных ИК-камер, как правило, не превышает 640x512 пкс. Далее сигналы микроболометра необходимо преобразовывать в понятный человеку вид. Этим занимается электронно-вычислительный блок (рис. 3). Затем результаты обработки сигналов детектора подаются на видеовыход и могут отображаться на мониторе в цветном или монохромном виде. Для охранного видеонаблюдения в большинстве случаев используется второй вариант, поскольку он более контрастный и несет меньшую нагрузку на оператора (наблюдателя).

Известно, что в ряде случаев эффективность тепловизоров снижается. Они, например, не помогут увидеть что бы то ни было расположенное за стеклом, которое поглощает значительную часть ИК-излучения. Решение нашлось в создании мультиспектральных систем наблюдения. Благодаря наличию двух каналов существенно увеличилась обнаружительная способность в дневное и ночное время. Отдельный анализ видеоизображения дополняет тепловизионный.

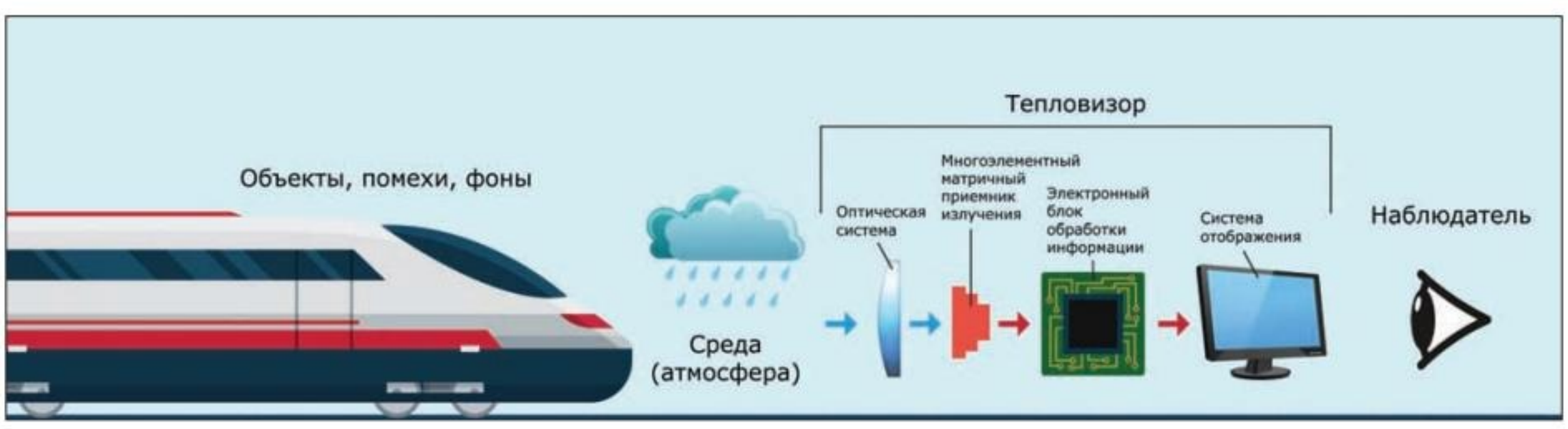


Рис. 1. Схема работы тепловизора

Рис. 2. Линза из оптического германия

Рис. 3. Отечественный тепловизионный модуль

Основные производители тепловизоров

Сегодня существует большое число различных серийных ТВМ – они есть у многих мировых производителей. Характеристики всех упомянутых видов ТВМ сведены в сравнительную таблицу.

FLIR Systems

Одним из лидеров данного сегмента является американская компания FLIR Systems. Тепловизоры для различных применений – ее основная специализация. Что же касается охранного видеонаблюдения, то в этом направлении у компании имеется более двадцати различных моделей. Есть тепловые камеры с разрешением 640x480 пкс, а наиболее дорогие системы представляют собой роботизированную PTZ-систему с двумя камерами – тепловизионной и оптической. Это позволяет вести эффективное наблюдение круглые сутки. Примером такого решения являются устройства серии PT. Отдельная серия устройств FC-3xx T предназначена для контроля транспортных потоков. Это камеры внешней установки для всепогодного наблюдения с разрешением 320x240 пкс и фокусным расстоянием 9, 13 или 19 мм, для контроля дорожной обстановки в условиях нулевой освещенности.

Axis Communication

Компания Axis Communication имеет около десятка разновидностей тепловизионных камер – это модели серий Q1941-E/1942-E, Q2901-E, роботизированные Q8631-E/8632-E и Q8721-E/8722-E (последние совмещены в одном корпусе с оптической камерой). Особенностью Q2901-E является функция температурной сигнализации с возможностью точного дистанционного измерения в диапазоне от -40 °C до 550 °C. В качестве сенсора здесь используется неохлаждаемый микроболометр с разрешающей способностью 336x256 пкс.

Bosch Security Systems

Несколько интересных тепловизионных камер есть у компании Bosch Security Systems. Так, модель Dinion IP thermal 8000 обладает разрешением 640x480 пкс и способна обнаруживать автомобили на расстоянии до 6 км. Она защищена в соответствии с IP66 и оснащена фирменным программным обеспечением (ПО) для видеоаналитики (Intelligent Video Analytics), может выдавать тревожные сообщения по событию (обнаружение объекта в кадре, пересечение им условной линии, вход в запретную зону и т.д.). Для обеспечения локальной записи поддерживаются карты памяти microSDHC емкостью до 32 Гбайт или microSDXC – до 2 Тбайт.

Mobotix

Имеются тепловизионные камеры и в предложениях немецкой компании Mobotix – это модели M15/M16 Thermal и S15 Thermal. Первая совмещает в одном фиксированном корпусе оптическую и тепловую камеру.

Dahua

Несколько десятков моделей тепловизоров для охранного видеонаблюдения предлагает китайская компания Dahua. Все изделия разделены на две группы – Pro (фиксированные и поворотные тепловизоры) и Ultra (системы, оснащенные двумя камерами – оптической и тепловой). Модель TPC-BF5300-T представляет собой типичную фиксированную камеру уличной установки. Камера оснащена сенсором с разрешением 336x256 пкс, может работать в трех режимах и передавать видео по IP, в формате HDCVI или аналоговом виде, питается по PoE. Корпус камеры отвечает степени защиты IP66. Здесь также имеется слот для SD-карты объемом до 128 Мбайт. Модель может оснащаться объективами с фокусным расстоянием 7,5, 13 или 19 мм. Камера роботизированная, оснащена функцией патрулирования и слежения за объектами, попадающими в кадр. Тепловизор может оснащаться различными объективами,

Таблица. Характеристики тепловизионных модулей

Производитель	Модель*	Детектор движения	Разрешение, пикс	Детекция человека (О/Р/И)**, м max (в идеальных условиях)	Детекция автомобиля (О/Р/И)*, м max (в идеальных условиях)	Наличие видеоканала	Наличие интеллектуальной встроенной аналитики
FLIR	LC -X	-	336x256	О: 570	О:1550	-	-
	PT-602 CZ	-	640x480	9200/2900/1200	15000/6000/3300	+	-
Dahua	TPC-BF5300-T (f объектива 19 мм)	-	336x256	600/150/70	1500/400/200	-	-
	TPC-PT8620C (f объектива 150 мм)	-	640x512	4000/1100/500	12000/3300/1700	+	-
Bosch	Dinion IP thermal 8000	+	640x480	О:3900	О: 5850	-	-
	VOT-320		320x240	н/д	н/д	-	-
Hikvision	DS-2TD2136-25	+	384x288	735/184/92	2255/564/282	-	-
	DS-2TD6160-75/KM	+	640x512	2200/750/275	6765/1700/850	+	-
Axis	Q1942-E (f объектива 60 мм)	-	640x480	2000/500/250	6200/1500/770	-	-
Mobotix	S15 Dual Thermal	-	336x252	н/д	н/д	-	-
АСТРОН	АСТРОН-3А	+	640x480	3000/1000/400 ***	9000/2000/1000 ***	+	+
	АСТРОН-IQ640 (f объектива 50 мм)	+	640x480	1470/500/350 ***	5000/1300/600 ***	-	+

* *Во всех случаях в качестве датчика изображения используется неохлаждаемый микроболометр.*

** *Обнаружение/Распознавание/Идентификация.*

*** *Параметры, указанные в таблице, представлены на основе опыта эксплуатации на главном ходу железной дороги и отличаются от критерия Джонсона.*

Рис. 4. Пример изображения с тепловизионного модуля. Условия: ночь, отсутствие освещения и легкий снег. Изображение "позитивное". Дальность до человека – 400 м. Дальность зоны наблюдения (выделено красным) – 1100 м

самый "дальнобойный" (с фокусным расстоянием 150 мм), по данным производителя, способен заметить движение крупного объекта (2,3x2,3 м) в полной темноте на расстоянии 12 км.

Hikvision

Еще один китайский бренд на рынке систем видеонаблюдения (СВН) – компания Hikvision – предлагает около двадцати различных моделей тепловизоров, также разделенных на две группы по принципу разрешения теплового сенсора – 640x512 и 384x288 пкс. Оба семейства включают в себя как фиксированные, так и роботизированные камеры. Фиксированная модель DS-2TD2136-25, благодаря своему чувствительному сенсору с разрешением 384x288 пкс, может обнаружить неподвижный или движущийся транспорт (с габаритами 4x1,4 м) на расстоянии свыше 2 км при угле обзора 11x15 град. Камера питается по PoE, имеет слот для установки SD-карты (128 МБайт) и оснащена встроенным ПО для видеоаналитики, которое позволяет ей определять возгорание, нахождение посторонних на объекте, пересечение условных "красных линий" и т.д. Кроме того, встроенная система безопасности подаст звуковой сигнал.

ОКБ "АСТРОН"

Среди российских производителей необходимо упомянуть компанию ОКБ "АСТРОН", которая с 2007 г. занимается разработкой и производством ТВМ в системах ТСО. Мультиспектральный модуль АСТРОН-3А работает в двух диапазонах излучения: видимом и дальнем ИК (7–14 мкм). В модуле, кроме тепловизионного, предусмотрен видеоканал с возможной дальностью видения и распознавания до 1000 м (в зависимости от применяемых объективов). Углы обзора видео- и тепловизионного канала идентичны, применение в камерах видимого диапазона низкоуровневых сенсоров позволяет использовать оптический канал при низких освещениях (до 0,001 Лкс). Разрешение видеоканала составляет 1280x960, 720x576, разрешение ИК-сенсора (болометр FPA) – 384x288, фокусное расстояние – 120, 100, 75, 60, 40 мм. Размер точки ИК-матрицы – 25 мкм. Модули различных моделей позволяют обнаруживать человека на разных расстояниях. Так, для модели АСТРОН-3А30/08 с фокусным расстоянием 30 мм и апертурой 0,8 это расстояние составляет 500 м, а для модели АСТРОН-3А100/14 с фокусным расстоянием 100 мм и апертурой 1,4 – 2,5 км. Интеллектуальная аналитика видео- и термоизображения способна распознавать тип объекта (человек, собака, предмет, поезд и т.д.) и определяет его размеры и скорость движения (рис. 4). Алгоритмы, применяемые в оптико-электронных системах охраны и наблюдения "АСТРОН", позволяют строить объемную 3D-модель тепловизионной сцены с учетом горизонта и проекции и осуществлять классификацию и селекцию наблюдаемых событий по широкому набору различных факторов. Стандарт передачи видео – PAL, NTS. ■

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

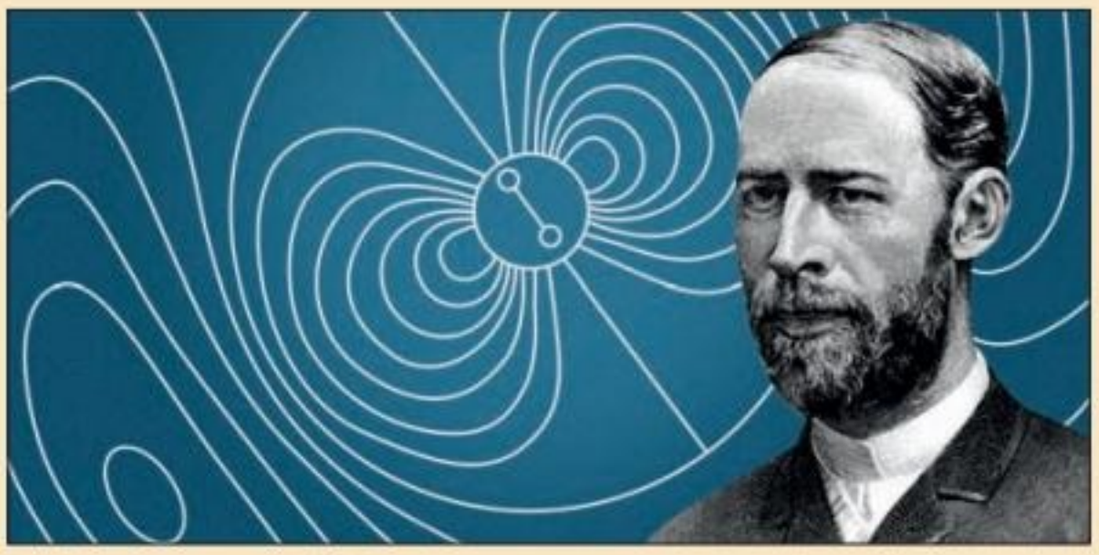
Явление внешнего фотоэффекта – основа первой ТСО

Первое упоминание о создании устройства технических средств охраны (ТСО) относится к 1928 г., когда для развития звукового кино концерны Siemens & Halske и AEG организовали компанию Klangfilm GmbH. Тогда же, в 1928 г., старейший банк Германии – Berenberg Bank (Joh. Berenberg, Gossler & Co. KG) – обратился в компанию Siemens с просьбой оборудовать все его филиалы охранной сигнализацией.

В основе первой ТСО лежало явление внешнего фотоэффекта, открытое Г. Герцем и описанное А. Столетовым. В своих опытах Столетов использовал наполненный газом стеклянный баллон с расположенными в нем двумя электродами, который позже стал называться газонаполненным фотоэлементом. Электроны, вылетающие из катода, сталкиваясь с атомами газа, могут ионизировать их. В результате таких столкновений возрастает число электронов, попадающих на анод, и сила тока увеличивается. Когда на катод фотоэлемента падают световые лучи, через прибор идет ток. Фотоэлемент может приводить в действие реле – автоматический выключатель тока. Данный газонаполненный фотоэлемент с внешним фотоэффектом нашел достаточно широкое применение и производился с начала 20-х гг. прошлого века фирмой Radiovisor и компаниями Westinghouse Electric Company и General Electric.

В середине 20-х гг. британская компания Radiovisor и германская Siemens & Halske практически одновременно предложили серийный образец охранной сигнализации на основе инфракрасных лучевых систем, предназначенной для контроля помещений. Принципиальная схема работы данной сигнализации базировалась на размещении в охраняемом помещении лампы с фильтром, испускающей инфракрасные (940 мкм) лучи. На противоположном конце пучка света устанавливался фотоэлектрический приемник – цезиевый элемент. При прерывании луча нарушителем, зашедшим в помещение, прекращается подача тока на фотоэлемент, в результате чего срабатывает звуковая сигнализация. Данная система охранной сигнализации нашла широкое применение в Западной Европе, Великобритании и США с начала 30-х гг. прошлого века – например, компания из ЮАР De Beers уже в 1932 г. начала применять на своих складах оптические лучевые инфракрасные сигнализаторы британской компании Radiovisor. Примечательно, что аналогичная система ТСО была впоследствии установлена в здании личной резиденции А. Гитлера "Бергхоф".

Первые оптические лучевые инфракрасные сигнализаторы, кроме очевидных преимуществ, имели и большие недостатки: например, давали ложные срабатывания при сильном снегопаде, тумане, дожде и ветре.



В основе первой ТСО лежало явление внешнего фотоэффекта. Открыл это явление Генрих Герц

EVIDENCE®

СПЕЦИАЛИЗИРОВАННЫЕ РЕШЕНИЯ ДЛЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ НА ТРАНСПОРТЕ

НАБЛЮДЕНИЕ В САЛОНЕ ТРАНСПОРТНОГО СРЕДСТВА,
В ЗОНАХ СКОПЛЕНИЯ ЛЮДЕЙ
И НА ОБЪЕКТАХ ИНФРАСТРУКТУРЫ

ГОТОВАЯ СИСТЕМА ОТ ОДНОГО ПРОИЗВОДИТЕЛЯ, ПОЛНАЯ ИНТЕГРАЦИЯ ВСЕХ КОМПОНЕНТОВ И КВАЛИФИЦИРОВАННАЯ ПОДДЕРЖКА

МЕГАПИКСЕЛЬНЫЕ ПАНОРАМНЫЕ
FISHEYE-КАМЕРЫ ДЛЯ ВРЕЗНОГО МОНТАЖА

МЕГАПИКСЕЛЬНЫЕ КАМЕРЫ
УГЛОВОГО КРЕПЛЕНИЯ

ПРОМЫШЛЕННЫЕ КОММУТАТОРЫ
С ЗАЩИЩЕННЫМИ РАЗЪЕМАМИ

МОБИЛЬНЫЕ ВИБРОУСТОЙЧИВЫЕ
СЕРВЕРЫ ВИДЕОЗАПИСИ

Комплексные решения для посторения IP-системы видеонаблюдения

EVIDENCE — это мегапиксельные видеокамеры различного исполнения, устройства записи и архивирования, коммутационное оборудование, а также рабочие станции, мониторы и программные средства управления системой.

Оборудование EVIDENCE позволяет создать профессиональную и легко управляемую систему видеонаблюдения на крупных территориально распределенных объектах любого масштаба.

ОФИЦИАЛЬНЫЙ ПРЕДСТАВИТЕЛЬ EVIDENCE
В РОССИИ – КОМПАНИЯ «СТА ПЛЮС»

Москва, 1-й Электрозаводский пер., д. 2
тел: +7 495 221-0821, e-mail: info@sta.ru

WWW.STA.RU

WWW.EVIDENCE.RU

Распознавание автомобильных номеров на борту камеры

Технологии в системах видеонаблюдения стремительно развиваются. Аналитика на видеосервере и с помощью вычислительных средств камеры, распознавание лиц и номеров являются неотъемлемой частью многих систем. Как следствие, видеонаблюдение используется не только в обеспечении безопасности, но и для решения бизнес-задач: анализа поведения посетителей в торговом зале, подсчета посетителей на входе/выходе из магазина, организациии систем доступа по алгоритмам распознавания лиц, автоматизации паркинга и др. Одним из наиболее востребованных решений для бизнес-аналитики является распознавание автомобильных номеров

Максим Савельев
Продакт-менеджер компании Hikvision

Внедрение системы видеонаблюдения с распознаванием автомобильных номеров снижает затраты на организацию бизнес-процессов, уменьшает риски и потери различного рода, а также сокращает потребность в дополнительном штате сотрудников. Современные автоматизированные системы не требуют вмешательства оператора – исключительно контроль и реагирование в случае возникновения нештатных ситуаций.

Традиционный подход

Рассмотрим классический вариант работы системы распознавания автомобильных номеров на въезде/выезде с территории: устанавливаются камеры, которые передают информацию непосредственно на видеосервер, а специализированный программный модуль на сервере осуществляет поиск и распознавание номера в кадре. Далее номер проходит проверку в базе данных, и система выдает сигнал о допуске на территорию. На въезде/выезде могут быть задействованы разные датчики, управление светофорами и шлагбаумами. Работа с системой возможна из интерфейса видеосервера, а также с помощью интеграции со СКУД.

Необходимость осуществлять анализ изображения, поиск и выделение информации номера автомобиля в изображении накладывают дополнительные требования на вычислительную мощность сервера и, следовательно, на его стоимость. Нужно также учитывать цену специализированного программного модуля распознавания. Эти факторы влияют на конечную стоимость системы.

Эффективная альтернатива

Существует и альтернативный, экономически более эффективный вариант. Речь идет о системах, в которых распознавание номеров автомобилей осуществляется непосредственно самой камерой (на профессиональном сленге это называется "распознавание на борту камеры"), без использования дорогостоящего сервера.

В такой системе видеокамера сама распознает номер и высылает информацию о нем (время фиксации, страна, тип транспортного средства и цвет) в текстовом виде совместно с изображением автомобиля, подтверждающим факт фиксации номера. Данные могут отправляться на FTP-сервер, электронную почту, систему наблюдения и записи, а также сохраняться на SD-карту. Видеокамера имеет возможность настройки и работы с данными посредством Web-интерфейса или программного обеспечения. При настройке камеры можно создать базу данных номеров (до 2 тыс. номеров), а также белые и черные списки, позволяющие ограничивать доступ транспортного средства или выявлять нарушителей. Работа с полученными от камеры данными включает набор соответствующих фильтров. Видеокамера обычно имеет встроенный коммутируемый выход (реле), который может быть использован для автоматического управления шлагбаумом. Таким образом, камера с распознаванием на борту может быть самодостаточным решением для небольшого объекта.

Впрочем, такие видеокамеры могут также использоваться в условиях города и контролировать более одной полосы. Существуют модели, способные фиксировать номера при скорости движения транспортного средства до 160 км/ч.

В настоящее время точность камер с распознаванием автомобильных номеров на борту достигает 98%, что является очень высоким показателем. При этом камеры могут быть интегрированы в любые программные решения.

Критерии выбора камеры с распознаванием на борту

При выборе камеры с встроенной функцией распознавания номеров необходимо четко понимать отличия ее параметров от параметров обычной обзорной камеры, а также условия работы и установки.

Разрешение

Разумеется, важным пунктом является разрешение камеры. Низкое разрешение может вызвать ошибки и неточное распознавание, а высокое увеличит нагрузку на сеть передачи данных. Еще одна проблема высокого разрешения – это низкая светочувствительность из-за высокой плотности пикселей и их малого размера, что может сделать номер нечитаемым в темное время суток или потребовать энергозатратного дополнительного освещения. Как следствие, видеокамеры с распознаванием номеров на борту имеют разрешение 2 Мпкс и используют технологии повышения чувствительности, а также CMOS-сенсоры большого формата.

Объектив

Объектив камеры должен обеспечивать большую глубину резкости и пропускать необходимое количество света на матрицу в любое время суток. Существуют модели камер с встроенными вариофокальными объективами в широком диапазоне фокусных расстояний и модели, требующие установку объектива.

Фокусное расстояние выбирается исходя из необходимости обеспечения требуемого угла обзора и расстояния от места установки камеры до пункта, где необходимо распознавать номера. Вариофокальный объектив позволяет отрегулировать угол обзора по месту установки камеры, но у него есть свои недостатки, такие как меньшая светосила по сравнению с фиксированным, высокая стоимость, расфокусировка во время эксплуатации. Объектив с фиксированным фокусным расстоянием подойдет в том случае, если известны точные данные о месте установки камеры.

Относительно применения объективов с автоматической диафрагмой существуют разные мнения, однако предпочтительным вариантом является возможность настройки оптимального значения диафрагмы и электронной экспозиции.

Освещение

Обеспечение дополнительного освещения также немаловажно во избежание низкой точности распознавания. Некоторые модели камер производятся с встроенной ИК-подсветкой, однако в реальных условиях может потребоваться иное или дополнительное освещение.

Углы съемки

Наконец, еще одним важным параметром являются горизонтальный и вертикальный углы съемки, которые также влияют на точность распознавания.

Таким образом, решение задачи распознавания не ограничивается только выбором модели камеры, но требует внимательного выбора места установки и настройки.

Перспективы очевидны!

В заключение стоит отметить, что перспективность использования видеокамер с функцией распознавания номеров, учитывая уровень развития данной технологии и точность, не вызывает сомнения. Можно с уверенностью заявлять о скором доминировании таких видеокамер на рынке систем видеонаблюдения. ■

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

Модель видеорегистратора	ACE-DM1204AT	TRASSIR PVR-211/32G	EMV-400FHD
			
Производитель (страна), Web-сайт производителя	ACE, www.vidau-cctv.ru	DSSL, www.dssl.ru	EverFocus el. Co., www.everfocus.com.tw
Компания, предоставившая информацию, сайт	Vidau Systems, www.vidau-cctv.ru	DSSL, www.dssl.ru	Vidau Systems, www.everfocus.ru
Режим работы	Пентаплекс	Дуплекс	Триплекс
Операционная система	Embbedded Linux 3.0	Linux	Embedded Linux 3.0
Алгоритм сжатия (компрессии)	H.264	H.264	H.264
Количество видеоканалов	4 x (AHD 1080P/720P/960H) + 4 x IP (1080P, TVI)	1	4 AHD
Макс. кол-во изображений в 1 с на каждый канал при просмотре/записи, размер изображения при этом	100 кадр/с, 1080P (1920x1080 пкс)/720P/960H	30 кадр/с, 1920x1080 пкс	100 кадр/с, 1080P/720P/960H
Макс. размер изображения на каждый канал при просмотре/записи, кол-во изображений в 1 с при этом	1920x1080 пкс, 100 кадр/с	1920×1080 пкс, 30 кадр/с	1920x1080 пкс, 100 кадр/с
Входы	BNC, Ethernet, RS232, RS-485	Встроенная камера	BNC, Ethernet, RS-485, RS-232
Видеовыходы	VGA 1080P + BNC (CVBS)	Нет	VGA (1080P) + BNC (CVBS)
Тревожные входы/выходы; журнал событий	2 входа, 1 выход; да	Нет	4/2; да
Аналоговые аудиовходы/аудиовыходы	1 аудиовход/1 аудиовыход	Нет	4/1
Датчик удара (G-sensor)	Да	Нет	Да
Максимальная скорость передачи информации в сеть	20 Мбит/с	Нет данных	20 Мбит/с
Модуль Wi-Fi	Нет	Да	Опция
Модуль GSM/CDMA	Нет	Нет	Опция
Подключение к блоку управления автомобиля для регистрации данных о скорости, торможении и др.	Да	Нет	Да
HDD/Flash-карты	SD/SDXC до 2 Тбайт	SDHC 32 Гбайт в комплекте (до 128 Гбайт опц.)	HDD/SSD 4 Тбайт, 2,5"
Конвертирование записей в AVI	Да	Да	Нет
Резервирование	USB, Web	USB	USB, Web, Hot Swap HDD, FTP
Кнопка аппаратного сброса Reset	Нет	Да	Нет
Модуль GPS/ГЛОНАСС	Да	Нет	Да
Встроенный источник питания для камер	Нет	Нет данных	Да
Органы управления	Да	Кнопки на панели	Да
Режимы записи	Обычный, по событию, по расписанию	Непрерывный	Обычный, по событию, расписанию
Возможности детектора движения	22x16	Нет	22x16
"Водяные знаки" для защиты записей	Да	Нет	Нет
Язык(и) интерфейса и ПО	Русский	Русский	Русский
Материал корпуса, цвет	Металл, серебристый	Пластик, черный	Металл, черный
Диапазон рабочих температур, °C	-15...+50	-5...+55	-20...+55
Допустимая вибрация	5–500 Гц	Нет данных	5–500 Гц
Допустимые удары	8G, 11 мс	Нет данных	8G, 11 мс
Напряжение питания, потребляемый ток (или мощность); адаптер питания	9–35 В DC, номинал 12 В DC, до 10 Вт; БП в комплекте нет	1,8 Вт	9–36 В DC, номинал 12 В DC, до 60 Вт подогрев + питание камер; БП в комплекте нет
Габариты, масса	118,5x128x43,5 мм, 0,4 кг	84x58x28 мм, 0,3 кг	178x199x50 мм, 2,15 кг (с кронш.)
Розничная цена	20 490 руб.	29 990 руб.	47 453 руб.

Модель видеорегистратора	EMV-400S FHD	EMV-400SSD	EMV-800FHD
			
Производитель (страна), Web-сайт производителя	EverFocus el. Co, www.everfocus.com.tw	EverFocus el. Co, www.everfocus.com.tw	EverFocus el. Co, www.everfocus.com.tw
Компания, предоставившая информацию, сайт	Vidau Systems, www.everfocus.ru	Vidau Systems, www.everfocus.ru	Vidau Systems, www.everfocus.ru
Режим работы	Триплекс	Триплекс	Триплекс
Операционная система	Embedded Linux 3.0	Embedded Linux 3.0	Embedded Linux 3.0
Алгоритм сжатия (компрессии)	H.264	H.264	H.264
Количество видеоканалов	4 AHD	4 AHD	8 AHD
Макс. кол-во изображений в 1 с на каждый канал при просмотре/записи, размер изображения при этом	100 кадр/с, 1080P(1920x1080 пкс)/720P/960H	100 кадр/с, 1080P (1920x1080 пкс)/720P/960H	200 кадр/с, 1080P (1920x1080 пкс)/720P/960H
Макс. размер изображения на каждый канал при просмотре/записи, кол-во изображений в 1 с при этом	1920x1080 пкс, 100 кадр/с	1920x1080 пкс, 100 кадр/с	1920x1080 пкс, 200 кадр/с
Входы	BNC, Ethernet, RS-232, RS-485	BNC, Ethernet, RS-232	BNC, Ethernet, RS-485, RS-232
Видеовыходы	VGA, 1080P (основной) + BNC (CVBS, тревожный)	VGA (1080P, основной) + BNC (CVBS, тревожный)	VGA1080P+BNC(CVBS) + RCA
Тревожные входы/выходы; журнал событий	1/1; да	1/1; да	8/2; да
Аналоговые аудиовходы/аудиовыходы	4/1	4/1	8/1
Датчик удара (G-sensor)	Да	Да	Да
Максимальная скорость передачи информации в сеть	20 Мбит/с	20 Мбит/с	20 Мбит/с
Модуль Wi-Fi	Опция	Опция	Опция
Модуль GSM/CDMA	Опция	Опция	Опция
Подключение к блоку управления автомобиля для регистрации данных о скорости, торможении и др.	Да	Да	Да
HDD/Flash-карты	SDHS/SDXC, 128 Гбайт	SSD 2 Тбайт, SD/SDHD 128 Гбайт	HDD/SSD 4 Тбайт, SD/SDHD 128 Гбайт
Конвертирование записей в AVI	Нет	Нет	Нет
Резервирование	USB, Web, Hot Swap SDHC, FTP	USB, Web, Hot Swap SSD/SDHC, FTP	USB, Web, Hot Swap HDD, FTP
Кнопка аппаратного сброса Reset	Нет	Нет	Нет
Модуль GPS/ГЛОНАСС	Да	Да	Да/да
Встроенный источник питания для камер	Да	Да	Да
Органы управления	Да	Да	Да
Режимы записи	Обычный, по событию	Обычный, по событию	Обычный, по событию, расписанию
Возможности детектора движения	22x16	22x16	22x16
"Водяные знаки" для защиты записей	Нет	Нет	Нет
Язык(и) интерфейса и ПО	Русский	Русский	Русский
Материал корпуса, цвет	Металл, черный	Металл, черный	Металл, черный
Диапазон рабочих температур, °С	-40...+55	-40...+55	-40...+50
Допустимая вибрация	5–500 Гц	5–500 Гц	5–500 Гц
Допустимые удары	8G, 11 мс	8G, 11 мс	8G, 11 мс
Напряжение питания, потребляемый ток (или мощность); адаптер питания	8–35 В DC, номинал 12 В DC, до 10 Вт; БП в комплекте нет	8–35 В DC, номинал 12 В DC, до 10 Вт; БП в комплекте нет	9–36 В DC, номинал 12 В DC, до 60 Вт подогрев + питание камер; БП в комплекте нет
Габариты, масса	131x171x38,4 мм, 0,69 кг	131x167x50 мм, 0,87 кг	178x209x63 мм, 2,15 кг
Розничная цена	26 682 руб.	41 936 руб.	63 045 руб.

Модель видеорегистратора	MNVR 40/PoE	WISENET TRM-1610S	DS-M5504HM-T
			
Производитель (страна), Web-сайт производителя	EVIDENCE, www.e-vidence.ru	Hanwha Techwin, www.hanwha-security.eu	Hikvision, www.hikvision.ru
Компания, предоставившая информацию, сайт	"СТА плюс", www.sta.ru	"АРМО-Системы", www.armosystems.ru	Hikvision, www.hikvision.ru
Режим работы	Пентаплекс	Дуплекс	Пентаплекс
Операционная система	Windows	Linux	Linux
Алгоритм сжатия (компрессии)	H.264/H.265	H.265, H.264, MJPEG; WiseStream (H.265, H.264)	H.264, H.264+
Количество видеоканалов	4 x IP	Подключение 16 IP-камер	4 (аналог), 4 (IP), 1 (двухстор. аудио)
Макс. кол-во изображений в 1 с на каждый канал при просмотре/записи, размер изображения при этом	25 кадр/с	30 кадр/с при просмотре (1920x1080 пкс) и при записи (4000x3000 пкс)	25 кадр/с, 1280x720 пкс
Макс. размер изображения на каждый канал при просмотре/записи, кол-во изображений в 1 с при этом	8 Мпкс	12 Мпкс (4000x3000 пкс) при просмотре (2 кадр/с) и при записи (30 кадр/с)	Нет данных
Входы	Ethernet	USB/GPS/Gigabit Ethernet x 2 RJ-45 (M12 у модели TRM-1610M)	Аналоговые BNC/HD, Ethernet, RS-232, RS-422, USB, тревожные
Видеовыходы	VGA, HDMI	HDMI/VGA	2 канала: 1-канальный основной выход (встроен в интерфейс EXT.DEV), 1-канальный видеовыход VGA; 1 аудиовыход
Тревожные входы/выходы; журнал событий	4/4	16/6	4/2
Аналоговые аудиовходы/аудиовыходы	1/1	Нет	Нет данных
Датчик удара (G-sensor)	Да	Нет	Нет
Максимальная скорость передачи информации в сеть	1 Гбит/с	256 Мбит/с	Нет данных
Модуль Wi-Fi	Опция	Да	2 x 5.8G, Wi-Fi-антенна
Модуль GSM/CDMA	Опция	Нет	Опция
Подключение к блоку управления автомобиля для регистрации данных о скорости, торможении и др.	Нет	Нет	Да
HDD/Flash-карты	SATA	2, "горячая" замена; макс. 2 Тбайт каждый (HDD, без RAID); макс. 4 Тбайт (SSD, без RAID); RAID 1	1 x 2,5" жесткий диск/SSD. До 2 Тбайт для каждого HDD/SSD. 1 x SD-карта (хранит данные при повреждении HDD/SSD)
Конвертирование записей в AVI	Да	Да	Нет данных
Резервирование	USB, сеть	Да, по сети	Передняя панель – 1 x USB 2.0, задняя панель – 1 x USB 2.0
Кнопка аппаратного сброса Reset	Да	Нет	Нет
Модуль GPS/ГЛОНАСС	Опция	GPS	1 x позиционная антенна для GPS
Встроенный источник питания для камер	Да	4 порта PoE/PoE+, поддержка Plug & Play	Нет данных
Органы управления	Мышь	Опционально	Мышь, ИК-пульт, Web-упр., сенсор. экран
Режимы записи	Да	Непрерывный, по детектору движения, по расписанию и др.	Непрерывный, по детектору движения, по расписанию
Возможности детектора движения	Да	Нет	Нет данных
"Водяные знаки" для защиты записей	Нет	Нет	Да
Язык(и) интерфейса и ПО	Русский	Рус., англ., франц., нем., итал. и др.	Английский
Материал корпуса, цвет	Черный, металл	Алюминий, черный	Алюминий, черный
Диапазон рабочих температур, °C	-20...+60	–25...+55 (с HDD), –40...+70 (с промышленными дисками SSD)	-10...+55 (уст-во с обогревом корзины HDD); -20...+60 (другие устройства)
Допустимая вибрация	Нет данных	EN-50155 (удары/вибрация на ж/д транспорте), EN-50121-4 (ЭМС на ж/д транспорте); MIL STD-810F	Нет данных
Допустимые удары	Нет данных	EN-50155 (удары/вибрация на ж/д транспорте), EN-50121-4 (ЭМС на ж/д транспорте); MIL STD-810F	Нет данных
Напряжение питания, потребляемый ток (или мощность); адаптер питания	9–38 В DC	Макс. 93 Вт (низкая темп.), макс. 67 Вт (комнатная темп.), макс. 32 Вт (суммарная мощность PoE)	9–32 В DC, режим ожидания ⩽ 0,5 Вт, полностью загружен ⩽ 20 Вт (без дисплея, камеры, жесткого диска/SSD)
Габариты, масса	235x268x101 мм	250x99x303 мм, 7,35 кг	236x210x73 мм, 1,6 кг
Розничная цена	По запросу	3336 долл.	По запросу

Модель видеорегистратора	KEDACOM KDM2410M-V21	DH-NVR0804MF	PRO-MDVR0400H
			
Производитель (страна), Web-сайт производителя	Suzhou KEDA Technology Co., Ltd, www.kedacom.com	ZheJiang Dahua Vision Technology CO., LTD, www.ru.dahuasecurity.com/ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru
Компания, предоставившая информацию, сайт	ООО "Видеоконтроль", www.video-control.pro	ООО "ДАХУА ТЕКНОЛОДЖИ РУС", www.ru.dahuasecurity.com/ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru
Режим работы	Пентаплекс	Пентаплекс	Пентаплекс
Операционная система	ОС Linux	Embedded LINUX	Linux
Алгоритм сжатия (компрессии)	H.265/H.264	H.264/G.711/PCM	H.264
Количество видеоканалов	4+4	8 IP	4 аналоговых HD-канала
Макс. кол-во изображений в 1 с на каждый канал при просмотре/записи, размер изображения при этом	25 кадр/с	25 кадр/с, 1080P	25 кадр/с, 1280x720 пкс
Макс. размер изображения на каждый канал при просмотре/записи, кол-во изображений в 1 с при этом	4 Мпкс, 30 кадр/с	1080P, 25 кадр/с	1920x1080 пкс, 12 кадр/с
Входы	4 аналоговых входа, 4 x RG-45	8 PoE-портов (IEEE802.3af/at)	BNC, Ethernet
Видеовыходы	1 x VGA, 1 x RG-45 Ethernet	1 x HDMI, 1 x VGA, 2 x TV	Да, BNC основной
Тревожные входы/выходы; журнал событий	4/1; журнал событий	8/2	8/2; да
Аналоговые аудиовходы/аудиовыходы	1 вход/1 выход, двусторонняя связь	1/1 RCA	4/1
Датчик удара (G-sensor)	Да	Да	Да
Максимальная скорость передачи информации в сеть	4 Мбит/с	48–8192 Кбит/с	100
Модуль Wi-Fi	Да	Опция	Опция
Модуль GSM/CDMA	2 SIM-карты	Опция	Опция
Подключение к блоку управления автомобиля для регистрации данных о скорости, торможении и др.	Нет данных	Нет данных	Да
HDD/Flash-карты	Да	2 x HDD до 4 Тбайт, 1 x SD-карта до 128 Гбайт	HDD 2,5" до 2 Тбайт (1 шт. опционально), SDHC до 256 Гбайт (1 шт. опционально)
Конвертирование записей в AVI	Нет данных	Да	Да
Резервирование	Да, USB	USB, по сети	USB, Ethernet
Кнопка аппаратного сброса Reset	Да	Нет	Нет
Модуль GPS/ГЛОНАСС	Да	Опция	Опция
Встроенный источник питания для камер	Да	Да	Да
Органы управления	Да	Мышь	Опционально мышь USB, Ethernet
Режимы записи	Да	Непрерывный, по детектору движения, по расписанию	Непрерывный, по детектору движения, по расписанию, по тревоге
Возможности детектора движения	Да	396 зон (22×18)	Более 10 зон
"Водяные знаки" для защиты записей	Да	Да	Нет
Язык(и) интерфейса и ПО	Русский, английский, китайский	Русский, английский	Русский
Материал корпуса, цвет	Металл/пластик, черный	Металл	Металл, серебристый
Диапазон рабочих температур, °С	-40...+70	-30...+60 (-30 с обогревателем)	-40...+70
Допустимая вибрация	Нет данных	В соответствии со стандартом CE EN50155	Нет данных
Допустимые удары	Нет данных	В соответствии со стандартом CE EN50155	Нет данных
Напряжение питания, потребляемый ток (или мощность); адаптер питания	9–36 В DC, до 15 Вт (без диска)	6–36 В DC, до 15 Вт (без HDD)	8–36 В, макс. 43 Вт; адаптера питания нет
Габариты, масса	252x188,4x60 мм, 2,6 кг	180×208×100 мм, 3 кг (без HDD)	182,3x168x67 мм
Розничная цена	По запросу	По запросу	27 000 руб.

PRO-MDVR0401	PRO-MDVR0401HG-AHD2.0	PRO-MDVR0800H	PRO-MDVR8844G-AHD
			
ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru
ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru	ООО "БИК-Информ", www.mobiledvr.bic-video.ru
Пентаплекс	Пентаплекс	Пентаплекс	Пентаплекс
Linux	Linux	Linux	Linux
H.264	H.264	H.264	H.264
4 аналоговых HD-канала, 1 канал IP	4 аналоговых HD-канала, 1 канал IP	8 аналоговых HD-каналов	8 аналоговых HD-каналов, 4 канала IP
25 кадр/с, 960x576 пкс	25 кадр/с, 1280x720 пкс	25 кадр/с, 1280x720 пкс	25 кадр/с, 1280x720 пкс
1280x720 пкс, 12 кадр/с	1920x1080 пкс, 12 кадр/с	1920x1080 пкс, 12 кадр/с	1920x1080 пкс, 12 кадр/с
BNC, Ethernet	BNC, Ethernet	BNC, Ethernet	BNC, Ethernet
Да, BNC основной	Да, BNC основной	BNC основной	BNC основной
8/2; да	8/2; да	8/2; да	8/2; да
4/1	4/1	8/1	8/1
Да	Да	Да	Да
100	100	100	1000
Опция	Опция	Опция	Опция
Опция	Опция	Опция	Опция
Опция	Опция	Опция	Опция
Да	Да	Да	Да
SDHC до 256 Гбайт (2 шт. опционально)	HDD 2,5" до 2 Тбайт (1 шт. опционально), SDHC до 256 Гбайт (1 шт. опционально)	HDD 2,5" до 2 Тбайт (1 шт. опционально); SDHC до 256 Гбайт (1 шт. опционально)	HDD 2,5" до 2 Тбайт (1 шт. опционально), SDHC до 256 Гбайт (1 шт. опционально)
Да	Да	Да	Да
USB, Ethernet	USB, Ethernet	USB, Ethernet	USB, Ethernet
Нет	Нет	Нет	Нет
Опция	Да	Опция	Да
Да	Да	Да	Да
Пульт ДУ, опционально мышь USB, Ethernet	Опциональное мышь USB, Ethernet и др.	Опционально мышь USB, Ethernet	Пульт ДУ, опц. мышь USB, Ethernet и др.
Непрерывный, по детектору движения, по расписанию, по тревоге	Непрерывный, по детектору движения, по расписанию, по тревоге	Непрерывный, по детектору движения, по расписанию, по тревоге	Непрерывный, по детектору движения, по расписанию, по тревоге
Более 10 зон	Более 10 зон	Более 10 зон	Более 10 зон
Нет	Нет	Нет	Нет
Русский	Русский	Русский	Русский
Металл, пластик, черный	Металл, пластик, черный	Металл, серебристый	Металл, пластик, черный
-40...+70	-40...+70	-40...+70	-40...+70
Нет данных	Нет данных	Нет данных	Нет данных
Нет данных	Нет данных	Нет данных	Нет данных
8–36 В, макс. 29 Вт; адаптера питания нет в комплекте	8–36 В, макс. 29 Вт; адаптера питания нет в комплекте	8–36 В, макс. 52 Вт; адаптера питания нет в комплекте	8–36 В, макс. 60 Вт; адаптера питания нет в комплекте
255,3x150x89,1 мм, 0,83 кг	255,3x150x89,1 мм, 2 кг	182,3x168x67 мм	295x222x89 мм, 2,6 кг
18 700 руб.	51 100 руб.	27 000 руб.	67 200 руб.

Век эмоджи,
или Как используется машинное зрение на традиционных и новых рынках

Сегодня машинное зрение серьезно влияет как на традиционные системы безопасности (СКУД, видеоаналитика и др.), так и на многие другие области, облегчая решение задач для пользователей, но в то же время и вторгается в нашу жизнь, когда мы этого не просим...

Андрей Жуков
Руководитель направления разработки продуктов на базе машинного обучения центра компетенций больших данных компании "Техносерв"

Внедрение систем машинного зрения наблюдается уже в самых различных сферах, начиная с применения на Земле и заканчивая космосом. Рассмотрим, какие функции оно может выполнять и к каким результатам это приводит.

Видеонаблюдение

В области видеонаблюдения базовые задачи, решаемые с помощью машинного зрения, – это распознавание лиц и отслеживание людей. Причем с распознаванием лиц большинство алгоритмов и систем справляются достаточно успешно, в то время как отслеживание людей (кто куда пошел, зачем и почему) проходит немного сложнее: происходит сегментация людей, попытка выделить каждую персону и то, как она двигается внутри кадра в видеопотоке. Для этого требуется выделить характерные части человека (например, одежда), автоматически их определить и отследить, чтобы затем наблюдать за движением в кадре.

С помощью машинного зрения Greenpeace следит за незаконными вырубками, ведется наблюдение за возникновением лесных пожаров. Сегментировать зелень и замерить изменения площади на спутниковом снимке несложно – подобные решения находятся уже в зрелой стадии

От ритейла все чаще приходят запросы по выделению горячих зон, когда по видеопотоку можно обозначить наиболее посещаемые места в магазине. Кроме того, в ритейле пытаются по многим параметрам (как по видеоаналитике, так и частично по съемке со спутников и малой летательной техники – коптеров) определить, что происходит внутри магазинов и снаружи больших моллов (выделение посетителей на парковках, поток людей), понять по количеству машин проходимость и доходность торгового центра и т.д.

Более сложные задачи – анализ дорожной обстановки с точки зрения как видеонаблюдения, так и с беспилотной техники (создается много летающих и ездящих дронов, которые должны сами ориентироваться в пространстве).

Медицина

Машины в медицине могут выполнять аналитику фотографий и не только, так как видят во многих спектрах (как видимом, так и в инфракрасном и радио) с возможностью определения визуальных характеристик. Наиболее перспективные задачи в данной области:

- получение данных по кровотоку и блуждающим опухолевым клеткам (по изображению и по видео);
- сегментация МРТ (анализ тканей внутри органа для определения размерности каких-либо частей, выявления аномалий и др.);
- определение текстур (текстуры раковых клеток специалист определяет лучше, чем машина, но с поддержкой машины количество ошибок снижается на 10%);
- определение возраста костных тканей по рентгеновским снимкам (установление возраста пациента по сегментированию и размеру кости).

Развлекательные сайты

На некоторых видеосайтах при постановке на паузу можно просмотреть не только стандартную информацию о фильмах, но и даже разметку киноактеров – кто находится в кадре.

Многие сайты с потоковыми сервисами пробуют определить, какие стили картин интересны зрителям с точки зрения как характерных актеров и лиц, так и картинки (цветность и др.), сделать сегментацию и автоматическое определение жанра.

Спутниковые снимки

В последнее время появилось огромное количество конкурсов, посвященных сегментации определенных объектов на снимках, определению адресов, где они находятся. Например, министерство обороны Великобритании провело конкурс по поиску на снимках автомобилей, дорог и домов.

Интересные проекты на базе машинного зрения реализует Massachusetts Institute of Technology (MIT), когда на панорамах Google выделяются наиболее безопасные участки в городах США. Другой их проект – определение площади зелени на панораме и конкретном участке (индекс зелени).

Археология

В археологических сообществах горят идеей определять возраст того или иного объекта по изображению и характерным признакам, а по текстуре – к какому периоду относится вещь или окаменелость.

Сельское хозяйство

Хотя многим сельскохозяйственным предприятиям машинное зрение экономически невыгодно, но технологии и разработки есть, например для определения степени зрелости пшеницы.

Лесное хозяйство

По спутниковым снимкам и автоматической идентификации изображения можно получить информацию об изменении лесного покрова. С помощью машинного зрения Greenpeace следит за незаконными вырубками, ведется наблюдение за возникновением лесных пожаров. Сегментировать зелень и замерить изменения площади на спутниковом снимке несложно – подобные решения находятся уже в зрелой стадии.

Что теперь?

Хотя сегодня очень многие проекты находятся еще на зачаточной стадии, но уже настает век анимированных разговаривающих эмоджи.

Технологии съемки с высоким разрешением и в широком видимом диапазоне становятся все доступнее. Возрастающие вычислительные мощности позволяют все эффективнее обрабатывать эти данные.

Машины помогают нам видеть. Помогают нам узнать больше об окружающем мире. Спутниковая съемка, съемки с беспилотников, панорамы с наземной техники – весь этот бесконечный массив информации мы уже готовы обработать и проанализировать.

Машины помогают нам узнать больше о себе. Искусственный интеллект становится надежным помощником врачей, подмечая мелочи на рентгеновских снимках, МРТ.

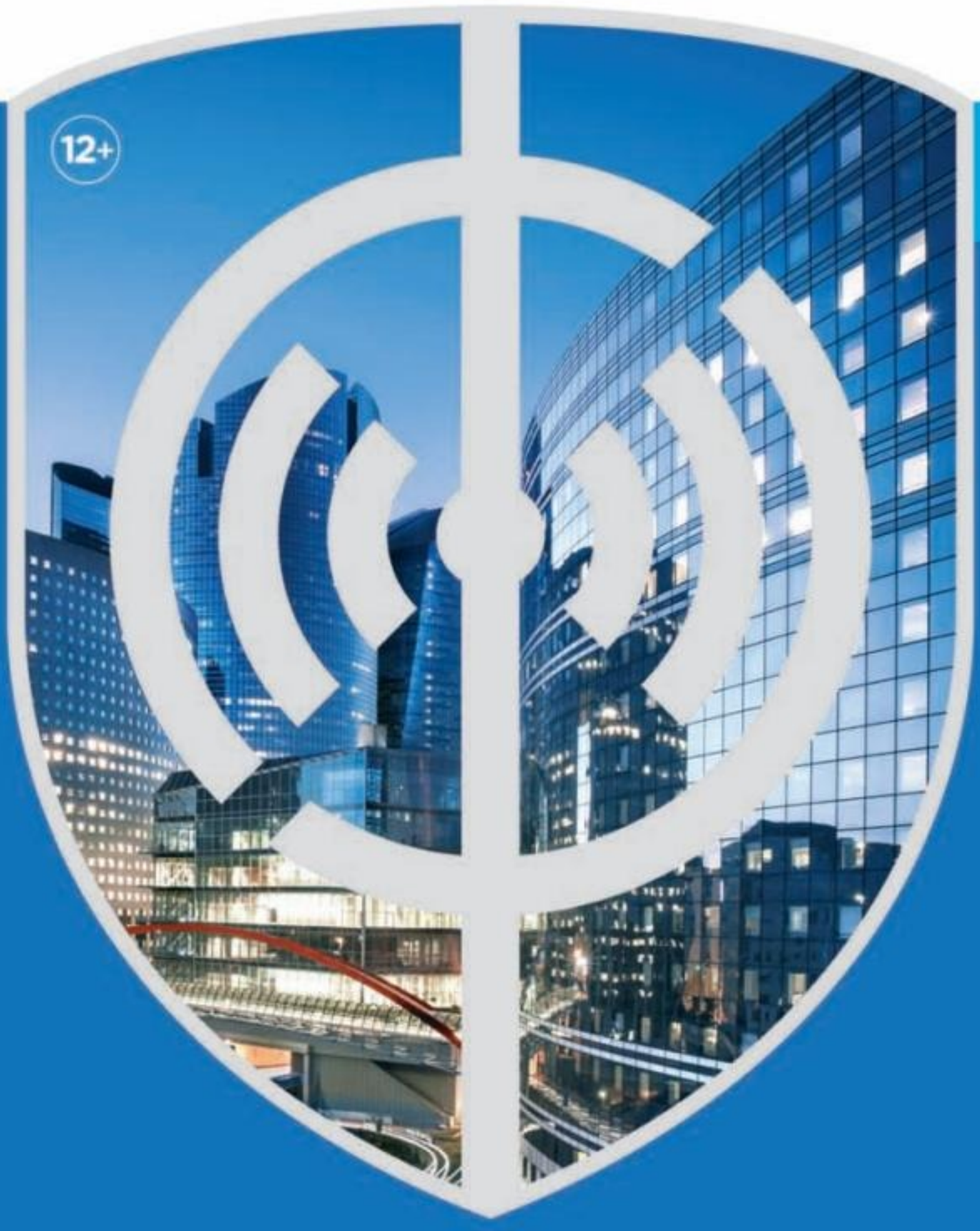
В то же время машины дают нам роскошь "не смотреть" – беспилотные автомобили все увидят сами, а интеллектуальные видеосистемы найдут злоумышленника.

Машины следят за нами. И об этом тоже надо помнить. ■

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

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

securika St. Petersburg



Санкт-Петербург

30 октября – 1 ноября 2018

ВК «Ленэкспо»

- СКУД и системы охраны периметра
- Системы охранного телевидения и наблюдения
- Системы и средства обеспечения пожарной безопасности
- Системы связи и оповещения
- Технические средства и программное обеспечение для защиты информации
- Средства охраны труда

Организаторы:

primexpo ITE

+7 (812) 380 6008/00
security@primexpo.ru
securika-spb.ru

Забронируйте стенд
securika-spb.ru

КОЛОНКА РЕДАКТОРА

Телега впереди лошади

Почти после каждого серьезного ДТП на железнодорожных переездах страны ответственные за безопасность мужи принимают соответствующие меры, выполнение которых должно, по их убеждению, снизить (а лучше исключить) возможность подобных аварий. При этом принимаются поправки к нормативным документам, в частности к федеральному закону об автомобильных дорогах и о дорожной деятельности (от 08.11.2007 № 257-ФЗ), соответственно рождается целый ряд подзаконных актов. Согласно им к обязательным элементам обустройства железнодорожных переездов отнесены "работающие в автоматическом режиме специальные технические средства, имеющие функции фото- и киносъемки, видеозаписи для фиксации нарушений правил дорожного движения...".

Все бы ничего, но боюсь, что теперь только на них и будут уповать. Ведь мы в который раз ставим телегу впереди лошади. Сошлюсь на печальный зарубежный опыт.

После теракта в редакции журнала "Шарли Эбдо" городской глава Ниццы говорил, что в его городе, утыканном видеокамерами (1256 штук на 340 тыс. населения), террористы "не смогут проехать и трех кварталов, не будучи замеченными". Увы, это не предотвратило трагические события в этом городе 14 июля 2016 г. Судя по принятым в России решениям, мы наступаем на западноевропейские грабли.

В глобальной сети масса видеозаписей, сделанных, кстати, аппаратурой для видеофиксации нарушений, на которых покадрово можно наблюдать столкновения локомотивов с различными видами автотранспорта: фиксируется гибель людей, сход вагонов и цистерн с рельсов и все остальные присущие ДТП моменты. Если такие вещи происходят при наличии телекамер, тогда какое отношение видеофиксация имеет к обеспечению безопасности на железнодорожном переезде?

Надо просто определиться, что мы собираемся делать: предотвращать возможные аварии или собирать штрафы? Это разные вещи, и не надо подменять понятия.

Встает вопрос: кого наказывать после аварии, если сами виновники ДТП чаще всего погибают? Остается только ожидать, что тем нарушителям, кому повезло, кому удалось проскочить, придет через три месяца штраф и у них заберут права. Но на этой же машине будет ездить другой лихач. И таким образом это будет продолжаться до тех пор, пока кто-нибудь не погибнет.

Вне правил железнодорожные переезды проезжают, безусловно, не все, а только некоторые категории водителей. Те, у кого отказали тормоза, уснувшие за рулем, кто сильно торопится. Яркий пример тому – ДТП в зоне Вишняковского железнодорожного переезда в Подмосковье. Это (рис.1) можно назвать апофеозом человеческой глупости и беспечности, когда в нетерпении поскорее проехать и сэкономить секунды взрослые люди полностью перекрывают движение в двух направлениях минимум на 30–40 мин.

Следует особо отметить, что ни в одном из случаев видеокамера не может предотвратить аварии и возможные жертвы. Напрашивается вывод: либо законотворцы повелись на тех, кто лоббирует свои финансовые интересы в продаже камер, либо просто перепутали причину со следствием. Причина железнодорожной катастрофы – это не отсутствие видеокамеры, а отсутствие физической защиты в зоне переезда.

Понятно, что малогабаритная камера и надпись "Ведется видеонаблюдение" вряд ли кого-то остановят. Другое дело – серьезное инженерное оборудование: мощный физический барьер может гарантированно удерживать большегрузный автотранспорт, независимо от того, кто им управляет – террорист или кто-либо другой.

К примеру, на высокоскоростных направлениях уже установлены мощные противотаранные шлагбаумы с огромными тяжелыми стрелами, которые опускаются за 10–15 с, перекрывая одновременно весь проезд шириной 7,5 м. И пока не было ни одного случая, чтобы кто-то умышленно въехал в эту стрелу. Это вам не сигнальный шлагбаум, который ломают каждые два дня, как-никак – полторы тонны стали. Увидев такой массивный барьер, водители сразу же снижают скорость. И останавливает их не сам шлагбаум, а зрительный образ – нечто более мощное, чем их джипы и грузовики.

Это подтверждают железнодорожники – дежурные по переездам: "С установкой противотаранных шлагбаумов работать стало намного легче. Раньше приходилось выбегать, махать, перекрывать проезд. Красный свет загорался, все его игнорировали, пытались проскочить. А сейчас только заморгал светофор – все замирает, никто не дергается, понимая, что это серьезная вещь и тут лучше не рисковать. И как результат – нет аварий".

Это еще одно подтверждение тому, что безаварийность работы зависит не от наличия видеокамер, а от установки и надежной работы серьезных инженерных препятствий, в частности противотаранных шлагбаумов.

В настоящее время на объектах ОАО "РЖД" противотаранные устройства (ПТУ) управляются с пульта дежурного по переезду. Для исключения роли так называемого человеческого фактора (который привел к столкновению "Ласточки" с автобусом на переезде Рощино под Санкт-Петербургом в феврале этого года) ведущими компаниями разработаны предложения по интеграции ПТУ в состав переездной автоматики с системой контроля наличия/отсутствия препятствий на железнодорожных путях. Эти новации касаются и автономных (необслуживаемых) переездов. К сожалению, в РЖД на них не реагируют.

Помимо обеспечения безопасности движения состава и автотранспорта в зоне переезда, актуален вопрос о регулировании движения пешеходов через железнодорожные пути. Предлагается в местах пешеходных переходов устанавливать заграждения с автоматически управляемыми калитками и светозвуковые табло, предупреждающие о приближении состава.

В такой структуре система видеонаблюдения решала бы больше задач, чем просто ведение посмертного учета.

Пришла пора концептуально менять подходы к работе. Давайте учиться правильно "запрягать".

Рис. 1. Скриншот ДТП с BMW на переезде в Вишняково

Игорь Васильев
Редактор раздела
"Комплексная безопасность",
главный конструктор
ЗАО "ЦеСИС НИКИРЭТ"

ЦеСИС®

ЦЕНТР СПЕЦИАЛЬНЫХ ИНЖЕНЕРНЫХ СООРУЖЕНИЙ

ПРОТИВОТАРАННЫЕ УСТРОЙСТВА

СТОЛБ ПРОТИВОТАРАННЫЙ МЕХАНИЧЕСКИЙ (БОЛЛАРД)

Предназначен для временного ограничения проезда автотранспортных средств на объектах с возможной террористической угрозой или в местах, где существует опасность неконтролируемого въезда автотранспортных средств на территорию проведения мероприятий с массовым скоплением людей.

Особенности

- Устойчив к таранному удару транспортного средства **массой** не более **6.8 т.**, движущегося со скоростью **до 80 км/ч**;
- Полная автономность функционирования;
- Конструкция оптимизирована для эксплуатации во всех климатических зонах Российской Федерации;
- Простота установки и обслуживания;
- Эксплуатация без подключения электропитания и подогрева приводных механизмов;
- Экономия на обустройстве дренажной системы;
- Сменный кожух с заказным логотипом;
- Срок службы – не менее 20 лет.

ПРЕПЯТСТВИЕ ЗАГРАДИТЕЛЬНОЕ ПРОТИВОТАРАННОЕ (ПЗП) «ПРЕПОНА-П»

Предназначено для регулирования движения автотранспортных средств путем создания физического препятствия (барьера) в виде платформы, перемещающейся в вертикальной плоскости.

Особенности

- Устойчиво к таранному удару транспортного средства **массой** до **6.8 т.**, движущегося со скоростью до **80 км/ч**;
- Устройство в закрытом положении является пассивным препятствием типа «лежачий полицейский»;
- В системе привода установлена предохранительная муфта, защищающая его от разрушающего воздействия таранного удара;
- Рабочие поверхности выполнены из рифленого металла для увеличения сцепления шин при пересечении ПЗП;
- Срок службы - не менее 10 лет.

ЗАО «ЦеСИС НИКИРЭТ»
440067, г. Пенза, ул. Чаадаева, 62
т/ф: (8412) 37-40-48, 37-40-50

info@cesis.ru, snabsbit@cesis.ru
www.cesis.ru, www.cesis-proekt.ru

Автотранспортные КПП.

Практика интеграции в систему охраны

Сергей Боряк
Инженер-программист
ООО "Радиорубеж"

Сегодня большинство охраняемых объектов оснащены системами контроля и управления доступом (СКУД), причем как для персонала, так и для автотранспортных средств. На некоторых объектах въезд и выезд автотранспорта производится через автотранспортные шлюзы. Данная тема уже освещалась в отраслевой прессе. Например, в статье "Транспортные проходные. Практические рекомендации" (каталог "СКУД–2014", стр. 70–73) рассматривались общие вопросы построения системы безопасности в зоне автотранспортного КПП. Идеология построения и алгоритм работы автотранспортного шлюза описаны в статье "Автотранспортный контрольно-пропускной пункт. Принцип модульной сборки" (журнал "Системы безопасности" № 1, 2017 г.). Данная статья посвящена практическому опыту интеграции устройств сторонних производителей

Деятельность государства направлена на усиление защищенности различных объектов повышенной опасности (Федеральный закон от 09.02.2007 г. № 16-ФЗ (в ред. от 06.07.2016 г.) "О транспортной безопасности", постановление Правительства Российской Федерации от 5 мая 2012 г. № 458 "Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса" и др.).

Бывает, что с целью соответствия всем нормативам проект предусматривает установку множества видов средств физической защиты (СФЗ) различных производителей. Вот тут-то и возникает ряд проблем с интеграцией продукции разных разработчиков с разной идеологией на одном объекте. Порой даже в пределах одной фирмы взаимодействие между разработчиками программного обеспечения, управляющих блоков, исполнительных механизмов и пассивных охранных средств оставляет желать лучшего, не говоря уже про "сотрудничество" конкурирующих в той или иной степени фирм.

Залог успешной интеграции

На рынке выделяются лидеры, на которых и начинают ориентироваться остальные. Например, некоторые интегрированные системы охраны (ИСО) на рынке получают настолько широкое распространение, что часто заказчики выносят обязательным условием совместимость с данным аппаратно-программным комплексом всех устанавливаемых средств.

Следует отметить как положительный момент, что разработчик сам способствует такой интеграции. Очевидно, для него расширение перечня совместимых СФЗ не менее важно, поэтому он сам выпускает устройства, которые помогают стороннему оборудованию легко встраиваться в ИСО, например контроллер доступа. В прилагаемой к нему документации имеются схемы подключения различных устройств с алгоритмами их работы.

Интеграция в СКУД таких изделий, как шлагбаумы, противотаранные устройства (ПТУ), откатные и распашные ворота, несомненно, интересует производителей и инсталляторов средств физической защиты.

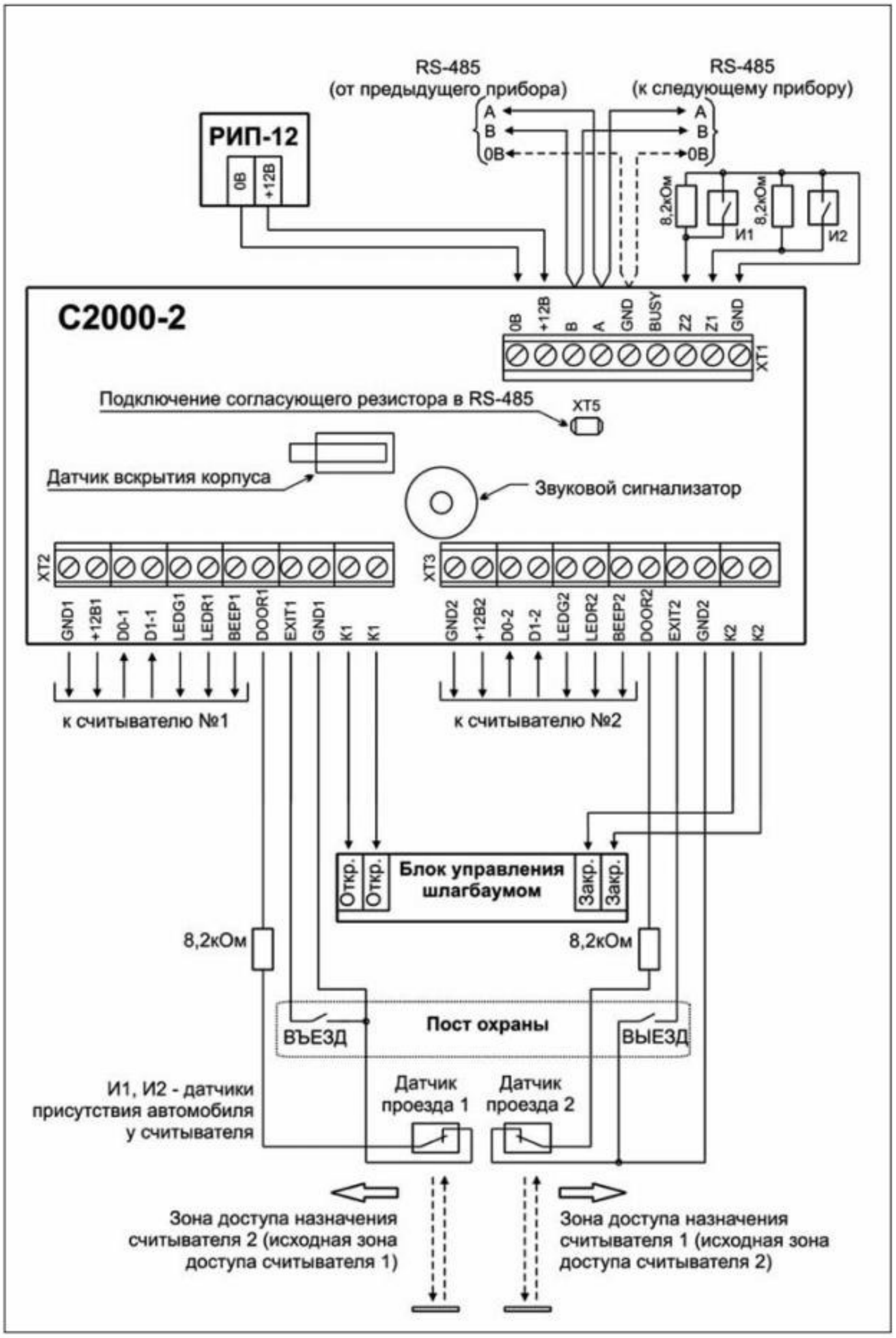


Рис. 1. Схема подключения контроллера в режиме "Шлагбаум"

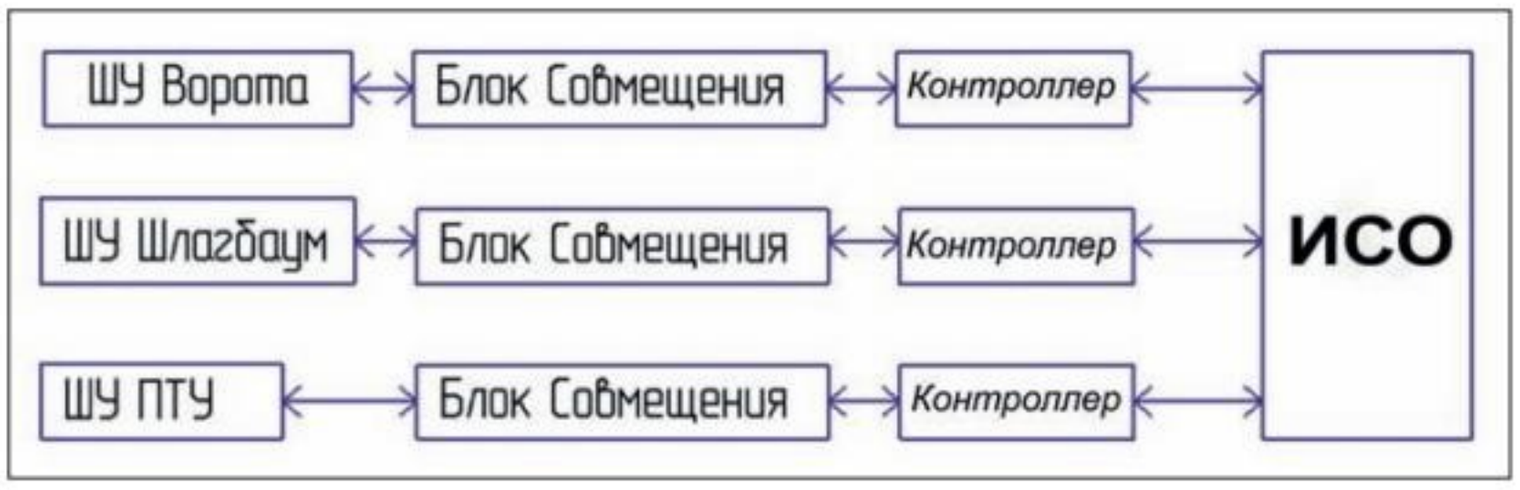


Рис. 2. Общая схема интеграции СФЗ в систему охраны

Работа управляемых устройств на КПП

Возьмем, к примеру, такое часто используемое типовое устройство, как шлагбаум, схема подключения блока управления которого представлена на рис. 1. Данное устройство, как несложно догадаться, – некая условность, подразумевающая все устройства, которые при помощи команд "Открыть/Закрыть" могут соответственно переходить в два состояния – "Открыто/Закрыто" – и ограничивают перемещение между зонами объекта, тем самым контролируя количество перемещаемых идентификаторов (машин, людей).

По схеме подключения контроллера (рис. 1) видно, что разработчики предусмотрели, как и куда подключать считыватели идентификационных карт, датчики опасной зоны, кнопки управления и даже светофоры.

Все, казалось бы, правильно, но есть один проблемный момент: не все управляемые устройства реагируют на команды контроллера в точности так, как задумано разработчиком. Например, во время движения стрелы шлагбаума (или створок ворот) из состояния "Открыто" в состояние "Закрыто" совершенно неожиданно контроллером посылается команда "Открыть", и тут различные устройства могут повести себя по-разному: одни проигнорируют новую команду и продолжат закрываться, другие остановятся, а третьи прервут выполняемую команду и начнут выполнение последней полученной.

К сожалению, здесь требования, предъявляемые к интегрируемым в систему охраны устройствам, не совпадают с заводскими алгоритмами работы изделий других производителей.

Разумеется, нелогично было бы менять алгоритмы работы и управления существующих СФЗ, которые удовлетворяют многих заказчиков, лишь из-за того, что у других потенциальных заказчиков другие требования.

Поэтому разработчики программного обеспечения (ПО) предлагаемых для ИСО сторонних СФЗ предусмотрели возможность нескольких способов управления, не исключающих друг друга. Так, при помощи так называемого блока совмещения, представляющего собой съемный модуль, настраивают поведение входов и выходов шкафа управления СФЗ под любые требования систем верхнего уровня, в том числе и алгоритмы ИСО. Схема такой интеграции приведена на рис. 2.

Нестандартные инсталляции

Вышеописанным образом можно выполнить далеко не все требования заказчика. Например, в ИСО существует понятие "шлюз", но оно не подразумевает автомобильный шлюз и в ПО нет стандартного метода реализации автотранспортных КПП (АТ КПП).

Грамотный агрегатор, разумеется, так или иначе сможет построить простейший АТКПП с одним режимом "Вторые ворота не откроются, пока не закрыты первые", для чего достаточно логически связать два контроллера при помощи входов Busy. Но ведь существуют и другие режимы, например "Сквозной проезд", "Прорыв" и т.д., которые также обязательны к реализации с возможностью переключений. Помимо того, нередко встречаются АТКПП с тремя и более СФЗ на въезде и выезде.

Чуть более продвинутый агрегатор применит на каждом СФЗ схему согласно рис. 2 и логически объединит группы контроллеров уже в сетевом контроллере или в программном обеспечении сервера. Однако здесь сразу же теряется требуемая автономность работы АТКПП в случае нарушения связи.

Разработка оптимального решения

В ходе совместной работы разработчиков ИСО и программистов, обеспечивающих работу интегрируемых СФЗ, была сделана специальная прошивка универсального блока управления (УБУ), которая совместно с доработанным алгоритмом "Шлюз" контроллера позволяет реализовать полноценное управление АТКПП.

Структурная схема подключения СФЗ транспортного шлюза к контроллеру под управлением ИСО представлена на рис. 3.

Разработчики программного обеспечения (ПО) предлагаемых для ИСО сторонних СФЗ предусмотрели возможность нескольких способов управления, не исключающих друг друга. Так, при помощи так называемого блока совмещения, представляющего собой съемный модуль, настраивают поведение входов и выходов шкафа управления СФЗ под любые требования систем верхнего уровня, в том числе и алгоритмы ИСО

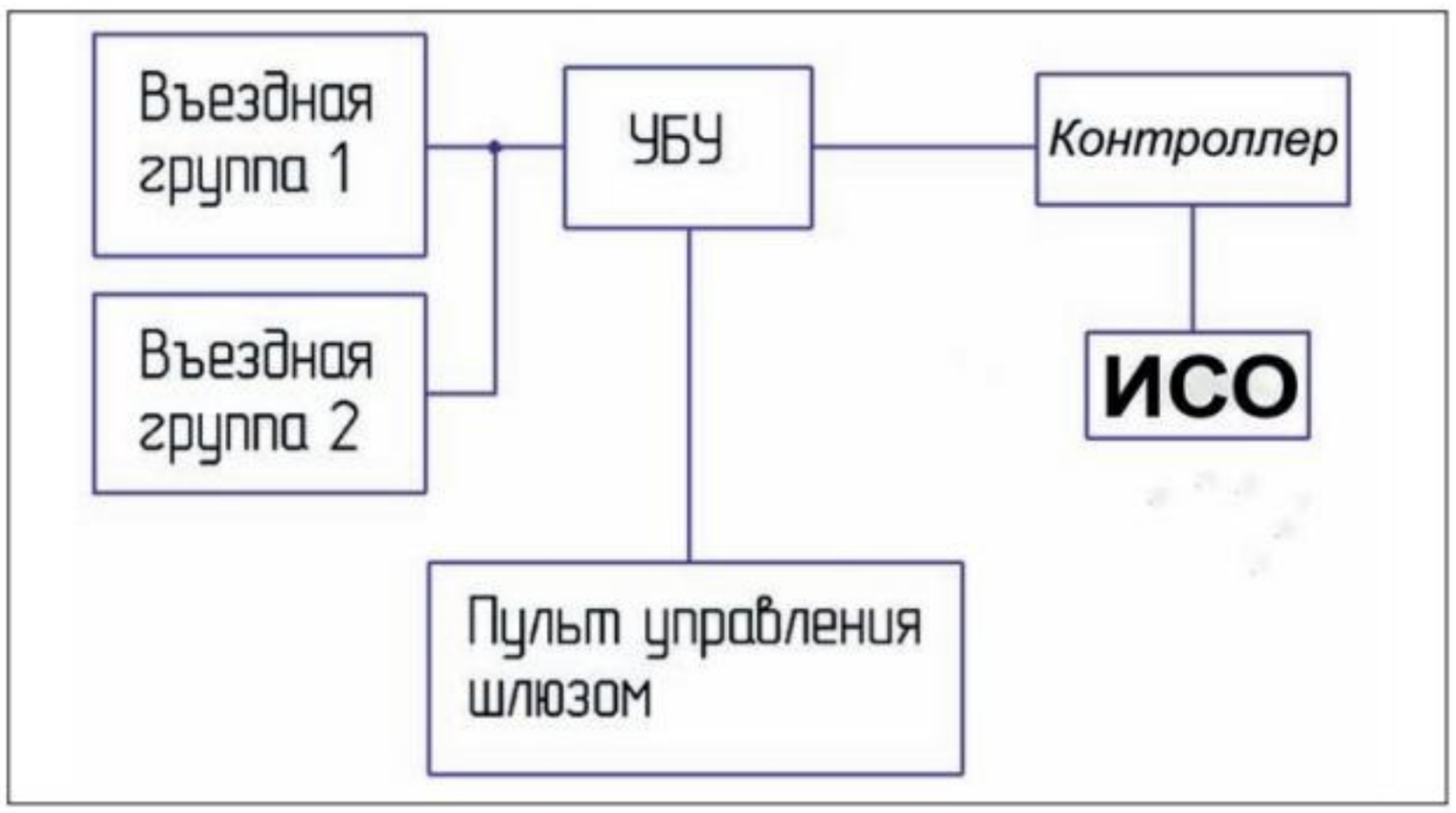


Рис. 3. Схема подключения АТКПП к ИСО

Здесь под термином "Въездная группа" может подразумеваться целая группа изделий, размещенных по одну сторону от досмотровой площадки, например ворота, противотаранный шлагбаум и светофор. Причем для контроллера эта группа будет являться классической "дверью шлюза", имеющей состояния "Открыто/Закрыто" и выполняющей команды "Заблокировать/Разблокировать".

Пульт управления шлюзом представляет собой панель ручного управления. Он может включать все возможные индикаторы состояний шлюза и соответствующие команды, определяемые требованиями проекта.

УБУ выступает в роли связующего звена между аналоговыми цепями пульта управления и контроллера, включенного в шину RS-485 протокола ИСО, и заградительными устройствами. Он полностью реализует все запрограммированные режимы работы шлюза ("Только въезд", "Только выезд", "Въезд/Выезд", "Сквозной проезд", "Блокировка", "Прорыв" и т.д.).

Таким образом, совместно разработанные решения позволяют:

- осуществить оперативную интеграцию технических средств физической защиты стороннего производства с программно-аппаратными средствами системы охраны;
- реализовать систему контроля и учета доступа на АТКПП как логическую единицу в интегрированной системе охраны. ■

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

КОЛОНКА РЕДАКТОРА

Безопасность транспорта под контролем государства

Прошедший 2017 год стал поистине эпохальным для объектов транспортной инфраструктуры.

Новое в законодательстве

Вступил в силу ряд постановлений Правительства РФ об утверждении требований транспортной безопасности и антитеррористической защищенности для различных категорий объектов транспортной инфраструктуры. То есть транспортная инфраструктура фактически стала одной из первых "гражданских" отраслей, требования к безопасности которой регулируются специальными обязательными нормативными актами.

Основным руководящим документом в технической части стало постановление Правительства РФ от 26.09.2016 № 969 "Об утверждении требований к функциональным свойствам технических средств по обеспечению транспортной безопасности...".

Этот документ формализует требования к охранной сигнализации, СКУД, видеонаблюдению (в том числе интеллектуальному – видеоаналитике), оповещению, приему, передаче, сбору и обработке информации.

Из интересующих нас подсистем под регулирование попала охранная сигнализация, требования к противопожарной защите отдельно не уточнялись.

Основные требования к охранной сигнализации свелись к обязательному соответствию до сего момента декоративному (добровольному) ГОСТ Р 52435–2005 "Технические средства охранной сигнализации".

Из интересных моментов также можно отметить требование к наличию у системы мониторинга сигнализации режима "исключения" (то есть Bypass). Оператор получает возможность отключить любой канал сигнализации, после чего его система перестает реагировать или даже фиксировать события, поступающие от него. Эта функция скорее противоречит бывшей ранее классической идеологии систем охраны, идущей от требований УВО.

Становится фактически обязательным наличие у системы охранной сигнализации АРМ на базе ПК, которые могли бы отображать состояние объекта на графических интерактивных планах помещений.

В очередь за сертификатами

Головной организацией, осуществляющей сертификацию ТСО на соответствие требованиям ПП № 969, стало ФКУ НПО "Специальная техника и связь" МВД России. На официальном сайте этой организации опубликованы списки всех заявок на сертификацию ТСО и тех ТСО, которые уже прошли все проверки и получили сертификаты. Так как сама процедура сертификации фактически рождалась уже после вступления в силу руководящих документов, по понятным причинам не все оборудование даже самых именитых производителей успело получить сертификаты. На сегодняшний день проектировщики систем и заказчики вынуждены закладывать оборудование "авансом", рассчитывая на появление сертификатов до сдачи объектов в эксплуатацию.

Как уже было сказано, отдельные требования к системам противопожарной защиты выдвинуты не были. Базовым руководящим документом для разработки проектов систем остается СП 5.13130.2009, а для техники – ГОСТ Р 53325–2012. При этом общие требования дополняются отраслевыми документами. Например, СП 120.13330.2012 "Метрополитены", СП 121.13330.2012 "Аэродромы", СП 153.13130.2013 "Свод правил. Инфраструктура железнодорожного транспорта. Требования пожарной безопасности" и т.п. Для уникальных или особо крупных объектов традиционно разрабатываются отдельные СТУ.

Эффективный мониторинг распределенных объектов

Если попробовать обобщить историю развития систем безопасности транспортной инфраструктуры, то основной интересной задачей, которая приходит на ум, будет создание эффективного мониторинга распределенных объектов. Прежде всего это, конечно, относится к объектам РЖД и метро, но также актуально и для аэропортов, каждый из которых является единым объектом очень большой площади. Именно структурные подразделения РЖД и метрополитена были одними из первых, кто внедрял мониторинг как охранной, так и противопожарной защиты объектов (станций, разъездов, стрелочных узлов и т.п.) с использованием IP-решений еще 10–15 лет назад. Логичным продолжением этих инициатив "снизу" стала разработка ФГУПом "ЗащитаИнфоТранс" универсального и обязательного для внедрения информационного протокола для передачи данных от всех подсистем ТСО на верхний уровень в единую систему технического мониторинга и контроля (СС ТМК) в рамках работ по ПП № 969.

Российская продукция в приоритете

В целом мы видим усиление контроля со стороны государства не только за противопожарной защитой, но и за защитой транспортной инфраструктуры в целом. Кроме этого, продолжает проводиться линия по импортозамещению. В частности, настоятельная рекомендация прикладывать к пакету документов для получения "транспортного" сертификата российский сертификат соответствия системы менеджмента качества производства создает определенные трудности для поставщиков импортных решений.

Транспортная инфраструктура стала одной из первых "гражданских" отраслей, требования к безопасности которой регулируются обязательными нормативными актами

Максим Горяченков
Редактор раздела
"ОПС, пожарная безопасность",
руководитель отдела технической
поддержки ЗАО НВП "Болид"

OPTEX

Sensing Innovation

СЕРИЯ BXS

УЛИЧНЫЕ ПАССИВНЫЕ ИК-ИЗВЕЩАТЕЛИ

Область детекции 24 м (2 зоны по 12 м в каждую сторону от извещателя), 4 независимых пироэлемента (по 2 на каждую зону), независимые настройки дальности и тревожные выходы для каждой зоны

УНИКАЛЬНЫЕ ТЕХНОЛОГИИ ОРТЕХ

Двойное экранирование пироэлемента, многоуровневая система обработки сигнала SDMA, исключающая ложные тревоги от животных и влияния окружающей среды, цифровая система защиты от маскирования (версии AM)

БЫСТРЫЙ МОНТАЖ И УДОБНАЯ НАСТРОЙКА

Специальная конструкция корпуса, удобная система обозначений и индикаторов, для быстрого подключения, гибкая настройка области детекции для исключения нежелательных зон

ШИРОКИЙ МОДЕЛЬНЫЙ РЯД

Стандартная модель, модель с дополнительной системой защиты от маскирования и беспроводные версии

СОВРЕМЕННЫЙ ДИЗАЙН И БОЛЬШОЙ ВЫБОР ЦВЕТОВЫХ РЕШЕНИЙ

НАДЕЖНОСТЬ, УДОБСТВО И ВЕЛИКОЛЕПНЫЙ ДИЗАЙН

Новая серия BX Shield — это многоцелевые уличные извещатели, сочетающие в себе современный дизайн и легендарное качество ОРТЕХ

Обеспечение пожарной безопасности железнодорожного подвижного состава:

важны качественные, а не количественные результаты

Функционирование железнодорожного транспорта представляет собой сложный и специфический процесс, стабильность которого зависит от слаженной работы всех его участников. Начальник отдела организации пожарного надзора и пожарной автоматики ФГП ВО ЖДТ России Николай Мингалев рассказал об итогах 2017 г. в обеспечении пожарной безопасности на объектах ОАО "РЖД", уровне оснащения подвижного состава техническими средствами защиты, а также о наиболее актуальных задачах и путях их решения

Николай Мингалев

Начальник отдела организации пожарного надзора и пожарной автоматики ФГП ВО ЖДТ России

– Какая работа проводится ведомственной охраной для профилактики пожаров на объектах ОАО "РЖД"?

– Пожарные инспекторы ведомственной пожарной охраны ФГП ВО ЖДТ России на протяжении всего года ведут планомерную работу по качественному проведению детальных и контрольных пожарно-технических обследований на стационарных объектах и подвижном составе железнодорожного транспорта – им подвергаются каждый стационарный объект и каждая единица подвижного состава. По итогам проведенной работы оформляется предписание на устранение выявленных нарушений требований пожарной безопасности с указанием конкретных сроков и вручается руководителю структурного подразделения ОАО "РЖД", а если нарушение влечет за собой потенциальную угрозу и может послужить возникновению пожара, то наши пожарные инспекторы выносят предписание о приостановлении эксплуатации объекта, отдельного помещения, единицы подвижного состава или электрооборудования, угрожающего безопасности пассажиров или работников компании. В этом случае, пока выявленное нарушение не устранено, эксплуатация запрещена.

Кроме того, должностные лица ФГП ВО ЖДТ России, на которых возложены организация и осуществление профилактики пожаров, наделены правами направлять представления руководителям структурных подразделений компании о привлечении к дисциплинарной ответственности лиц, нарушающих требования пожарной безопасности и не принимающих должных мер к устранению выявленных нарушений.

Основной задачей пожарного инспектора ведомственной пожарной охраны ФГП ВО ЖДТ России является достижение качественных, а не количественных результатов работы.

– Как вы можете описать итоги 2017 г. в части обеспечения пожарной безопасности на объектах ОАО "РЖД"? Какова динамика пожаров на объектах и подвижном составе ОАО "РЖД"?

– Общее количество пожаров на объектах и подвижном составе компании в 2017 г. увеличилось с 86 до 104 случаев (+21% к 2016 г.). За три года (2014–2016 гг.) наблюдалась тенденция к снижению количества пожаров на объектах и подвижном составе ОАО "РЖД". Однако по итогам 2017 г. об этом говорить не приходится – произошло значительное ухудшение состояния пожарной безопасности на локомотивах. Так, по сравнению с 2016 г. количество пожаров на локомотивах увеличилось на 19% (с 47 до 56 случаев).

– Какие новые технологии и средства защиты применяются для охраны объектов и подвижного состава ОАО "РЖД" от пожаров?

– Объекты оборудуются системами противопожарной защиты. Это и пожарная сигнализация, и системы пожаротушения, и система оповещения о пожаре и управления эвакуацией людей. На транспорте в основном все они автоматические и в случае необходимости сработают без участия человека.

В автоматических системах пожаротушения применяется инновационный состав Novec 1230 – это своего рода жидкость без цвета и запаха, иногда называемая сухой водой. Визуально жидкость похожа на чистую воду и является диэлектриком, слабо смачивает и не является растворителем, вследствие этого она и получила название "сухая вода". Имеет слабые молекулярные связи, распадается под действием ультрафиолета, не влияет на работающую электронику, не разрушает бумажные документы. Эти свойства обеспечили применимость Novec 1230 в системах пожаротушения для серверных помещений и другой электроники, постов электрической централизации.

– Какие мероприятия для обеспечения противопожарной защиты подвижного состава и стационарных объектов ОАО "РЖД" вы считаете самыми важными?

– В данной работе главное – не ликвидировать пожар, а предотвратить его возникновение. С этой целью ведется постоянная работа по оснащению как железнодорожного подвижного состава, так и стационарных объектов ОАО "РЖД" техническими средствами противопожарной защиты (автоматическими установками пожарной сигнализации и пожаротушения – АУПС и АУПТ).

Немаловажным является осуществление качественного проведения профилактических мероприятий, направленных на недопущение возникновения возгорания, таких как обучение персонала требованиям правил пожарной безопасности (в том числе и по программам пожарно-технического минимума), умение работников компании пользоваться первичными средствами пожаротушения и индивидуальными средствами спасания при пожаре.

Несколько слов хочется сказать о пожарных поездах, которые принимают непосредственное участие в тушении пожаров и ликвидации ЧС.

На РЖД в постоянной боевой готовности находятся 310 пожарных поездов

Тушение пожара в локомотиве

На сети железных дорог компании находятся в режиме постоянной боевой готовности 310 пожарных поездов, в том числе три из них на территории Республики Крым (на станциях Симферополь, Джанкой и Айвазовская).

Деятельность боевых расчетов пожарных поездов по тушению пожаров и проведению аварийно-спасательных работ осуществляется в соответствии с требованиями Федерального закона 69-ФЗ "О пожарной безопасности", нормативных правовых актов федеральных органов исполнительной власти, а также методических рекомендаций по тушению пожаров на железнодорожном транспорте, разработанных специалистами ведомственной пожарной охраны и ОАО "РЖД".

В рамках реализации инвестиционного проекта ОАО "РЖД" "Пожарная безопасность" в период с 2011 г. построены и введены в боевой расчет 134 пожарных поезда нового поколения, которые оснащаются новейшим пожарным оборудованием для эффективного тушения пожаров.

– Насколько важна работа систем оповещения о пожаре и управления эвакуацией для защиты пассажиров?

– Система оповещения и управления эвакуацией (СОУЭ) – одна из наиболее важных составляющих системы безопасности. Основное назначение системы оповещения – это предупреждение находящихся, например, в здании вокзала людей о пожаре или другой чрезвычайной ситуации, а также координация их действий при осуществлении эвакуации. СОУЭ представляет собой комплекс организационных мероприятий и технических средств, предназначенных для решения этих задач.

– На чем, по вашему мнению, нельзя экономить при оснащении железнодорожного транспорта и объектов инфраструктуры техническими средствами противопожарной защиты?

– На безопасности экономить нельзя – это прописная истина. Ведь за словом "безопасность" стоят жизни и здоровье людей. Поэтому пожарными инспекторами ведомственной пожарной охраны при проведении обследований объектов инфраструктуры железнодорожного транспорта особое внимание уделяется оснащению именно современными системами противопожарной защиты, на что, в свою очередь, ОАО "РЖД" выделяет средства для достижения желаемого результата.

– Как, на ваш взгляд, обстоит дело с защищенностью транспорта и объектов ОАО "РЖД" от пожаров?

– Весь подвижной состав РЖД оборудуется современными средствами обнаружения и тушения пожаров. На всех типах локомотивов эксплуатируются автоматические установки пожарной сигнализации и пожаротушения. В РЖД существует четкая система техобслуживания и ремонта локомотивов. Работы выполняются сервисными организациями и локомотиворемонтными заводами. Капитальный ремонт локомотива (КР) выполняется для восстановления эксплуатационных характеристик, исправности локомотива и его ресурса, близкого к полному.

Основными требованиями РЖД при закупке локомотивов и других видов подвижного состава в части оснащения системами противопожарной защиты (АУПС и АУПТ) являются:

- выполнение соответствующих требований действующих нормативных правовых актов и документов по пожарной безопасности в части защиты локомотивов АУПС и АУПТ;
- соответствие АУПС и АУПТ требованиям действующих нормативных правовых актов и документов по пожарной безопасности;
- высокая надежность систем;
- соотношение цены и качества;
- возможно большая унификация;
- простота и невысокая стоимость эксплуатации и технического обслуживания.

– С какими трудностями вы сталкиваетесь в работе по обеспечению пожарной безопасности на объектах ОАО "РЖД"? Чем они вызваны? Как должны быть решены?

– Одна из трудностей при осуществлении профилактики пожаров – это неактуальность нормативной базы. Старые документы уже не отвечают современным требованиям, а новые еще не утверждены. Например, в настоящее время завершается согласование последней редакции проекта "Правил противопожарного режима при эксплуатации железнодорожного подвижного состава", которые должны заменить ППБО-109-92.

– В каком направлении, по вашему мнению, будут развиваться технологии обеспечения пожарной безопасности на РЖД?

– Все применяемые в пожарной безопасности технологии должны быть безопасны для людей и соответствовать следующим требованиям:

- высокая надежность;
- простота, невысокая стоимость эксплуатации;
- большая унификация систем. ■

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

Нюансы выбора и правильного расположения громкоговорителей

Роман Мишин
Независимый эксперт

Казалось бы, по данной теме много написано и белых пятен в этой области техники нет. К тому же многие производители систем оповещения предлагают различные программы для расчета количества и выбора типа громкоговорителей, однако не всегда построенная по этим рекомендациям система звучит так, как надо. В данной публикации я постараюсь обратить внимание на отдельные подводные камни, о которые то тут, то там спотыкаются и проектировщики, и интеграторы систем оповещения

Рис. 1. Типы громкоговорителей

Ошибки в проектировании происходят от того, что зачастую системы звукофикации и оповещения рассматриваются в общем классе слаботочных систем объекта и основное внимание уделяется правильному электрическому сопряжению устройств, что, без сомнения, важно. Но иногда получается так, что корректно электрически построенная система оповещения звучит плохо, неразборчиво, не создает требуемый уровень громкости и т.п. Именно о том, как предупредить такие ситуации, и пойдет речь в дальнейшем.

Заблуждение первое. Существует прямая связь между мощностью и громкостью системы

Это самое распространенное заблуждение. Его суть состоит в том, что часто при написании технических заданий или требований на систему оповещения указывают требуемую звуковую мощность, напрочь забывая о том, что прямой связи между мощностью громкоговорителя и тем, насколько громко он звучит, нет, она лишь косвенная!

Как быть? Прежде всего, отталкиваться не от мощности, а от требуемого уровня звукового давления, который должна обеспечивать система. Именно уровень звукового давления, а не мощность влияет на то, насколько громко звучит тот или иной громкоговоритель. Определить меру громкости звучания поможет параметр, называемый чувствительностью. Он обязательно указывается в технических характеристиках, в описании или паспорте на устройство. Именно чувствительность определяет, насколько хорошо тот или иной громкоговоритель преобразует электрический сигнал в акустические колебания. Чем выше чувствительность, тем громче громкоговоритель. Такой параметр, как мощность громкоговорителя, будет нужен лишь затем, чтобы рассчитать суммарную мощность трансляционных усилителей и их количество.

Заблуждение второе. Тип громкоговорителя зависит от его направленности

Второе заблуждение состоит в том, что тип громкоговорителя однозначно сопоставляют с его направленностью, что в наше время не совсем так. Классическая точка зрения: ненаправленными громкоговорителями считают потолочные устройства, направленными – рупорные громкоговорители, а так называемые колонки относят к промежуточному классу. Однако не стоит забывать, что существуют рупорные громкоговорители и с квазикруговой диаграммой направленности, линейные массивы колонок с управляемой процессором диаграммой направленности, а также такой класс громкоговорителей, как звуковые прожекторы. Этот параметр надо уточнять в техническом описании.

Добавлю, что узкой диаграммой направленности для громкоговорителей считается угол 30 град., широкой – 60 град. и более.

Диапазон звуковых частот

Важным параметром, от которого зависит качество звучания и разборчивость транслируемых объявлений, является диапазон воспроизводимых звуковых частот. Здесь рекомендации до предела просты. Если система будет использоваться только для трансляции безличных речевых сообщений, то вполне достаточно диапазона от 150–200 Гц до 5–5,5 КГц. Если в какой-то мере требуется идентифицировать голос говорящего, то целесообразно расширить диапазон воспроизведения хотя бы до 8 КГц, поскольку именно в диапазоне 4–8 КГц сосредоточены форматные составляющие речи, благодаря которым мы узнаем голос собеседника. Если же предполагается транслировать и рекламные объявления с музыкальным сопровождением, то для такого случая необходимы будут громкоговорители, обеспечивающие полосу воспроизведения от 100 Гц до 10–12 КГц и более.

Расстановка громкоговорителей

Пожалуй, это и есть самый трудный момент при проектировании. К тому же от того, насколько правильно установлены громкоговорители, напрямую зависят и качество звучания, и громкость, и мощность, необходимые для системы оповещения.

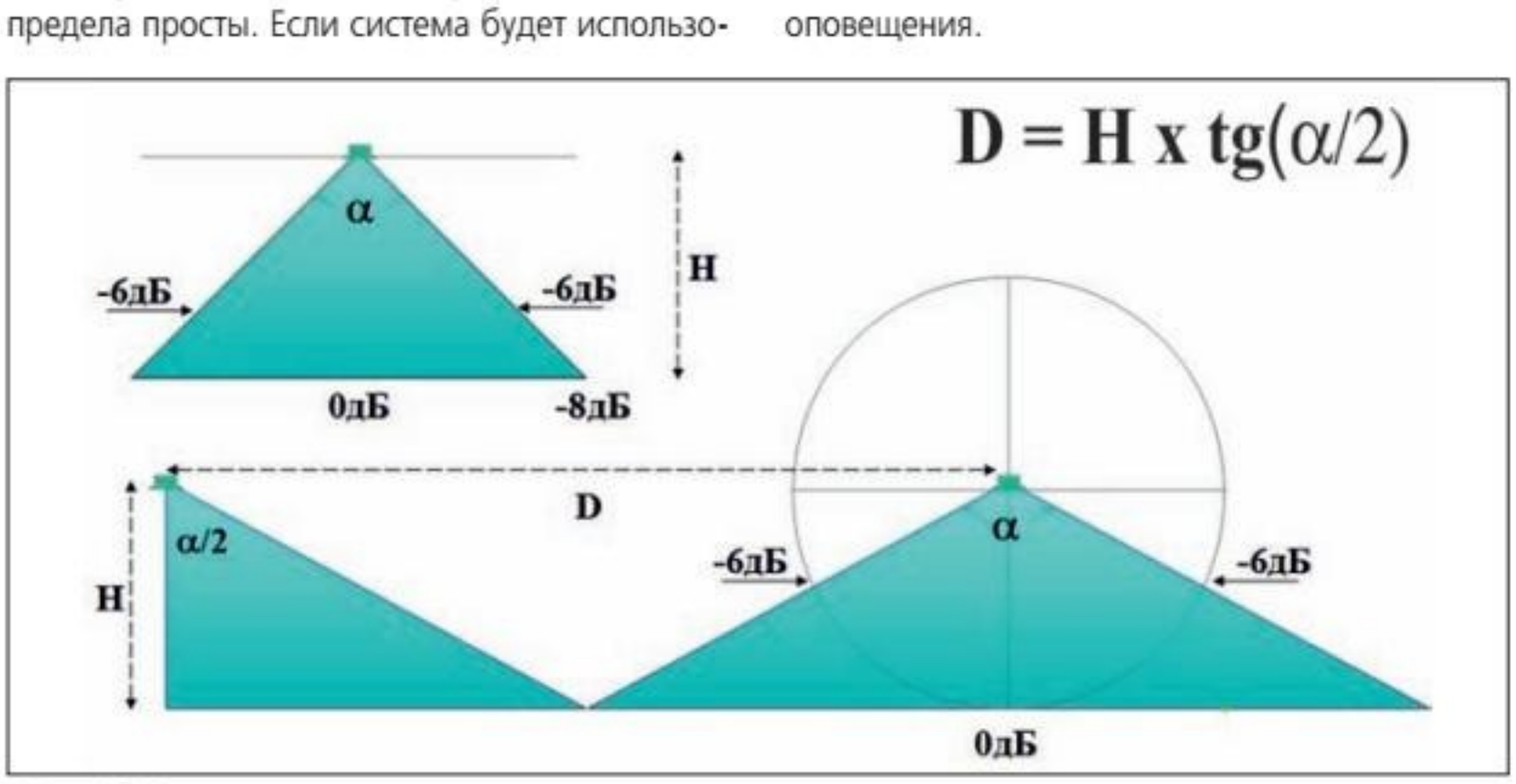


Рис. 2. Определение расстояния между потолочными громкоговорителями в зависимости от высоты подвеса H и угла раскрыва диаграммы направленности

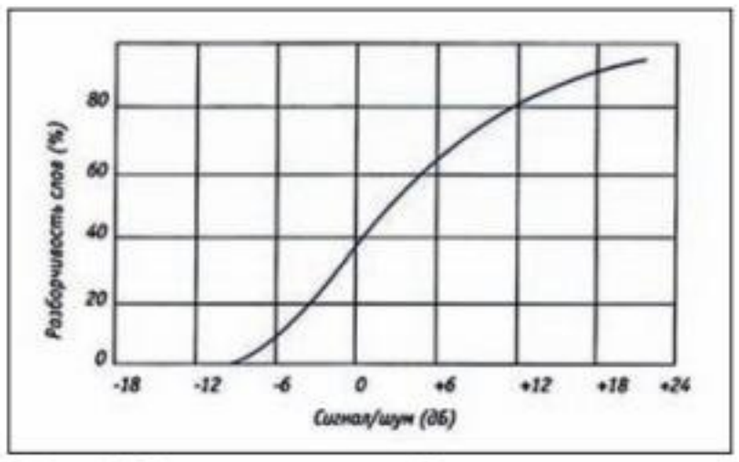


Рис. 3. Зависимость разборчивости от отношения "сигнал/шум"

При определении точек установки громкоговорителей следует учитывать множество факторов:

- пространственную конфигурацию помещения или территории;
- окружающий уровень шума;
- материал стен помещения;
- наличие и направление ветра для открытых территорий.

В помещениях

В помещениях большую роль в плане акустики играют такие параметры, как форма помещения, его объем и коэффициенты поглощения звука стен, потолка и пола. Эти параметры оказывают заметное влияние на частотную характеристику звукового давления, а следовательно и на качество воспроизведения. Одна и та же аппаратура в различных помещениях будет звучать по-разному. Если в помещении присутствуют шторы, ковры, мягкая мебель, обладающие большим коэффициентом звукопоглощения, то система будет звучать несколько тише по сравнению с помещением, где гладкий потолок и стены, которые весьма мало поглощают звук и в значительной степени его отражают.

Следует учитывать также, что всякое помещение представляет собой достаточно сложную акустическую систему, обладающую рядом собственных резонансных частот. При возбуждении в помещении каких-либо звуков, содержащих составляющие таких же частот, возникают резонансные колебания воздуха внутри помещения. Такое явление приводит к усилению звуков этих частот и изменению спектрального состава звукового сигнала, то есть к изменению тембра. Однако для систем оповещения это не так важно, поскольку начиная уже с частоты 150–200 Гц для не очень малых помещений плотность спектра собственных колебаний настолько велика, что явление резонанса становится малозаметным.

Следует отметить, что бОльшие помещения являются более благоприятными для звуковоспроизведения, так как основные резонансные частоты с увеличением размеров понижаются и оказываются за пределами нижней границы рабочего диапазона частот. Единственным исключением, пожалуй, могут служить лишь длинные узкие коридоры офисных зданий. В этом случае, как правило, применяют много небольших потолочных или настенных громкоговорителей. При этом потолочные располагают по оси коридора, а настенные – на одной из стен. Расстояние между громкоговорителями рассчитывают, исходя из требуемого уровня звукового давления, обеспечивающего достаточную разборчивость речи и громкость, диаграммы направленности громкоговорителя, а также условия обеспечения отсутствия эха. Примерный расчет расстояния между потолочными громкоговорителями D показан на рис. 2.

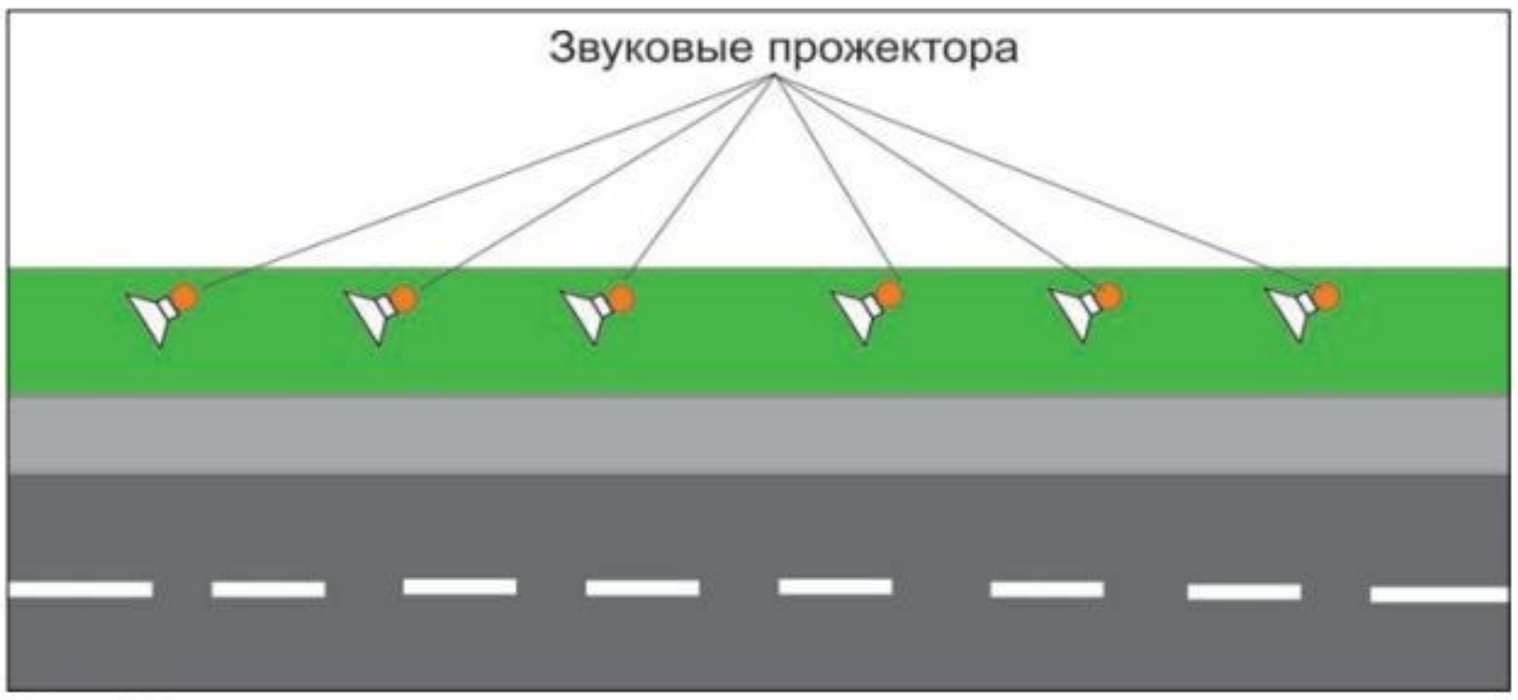


Рис. 4. Примерная расстановка звуковых прожекторов для улицы

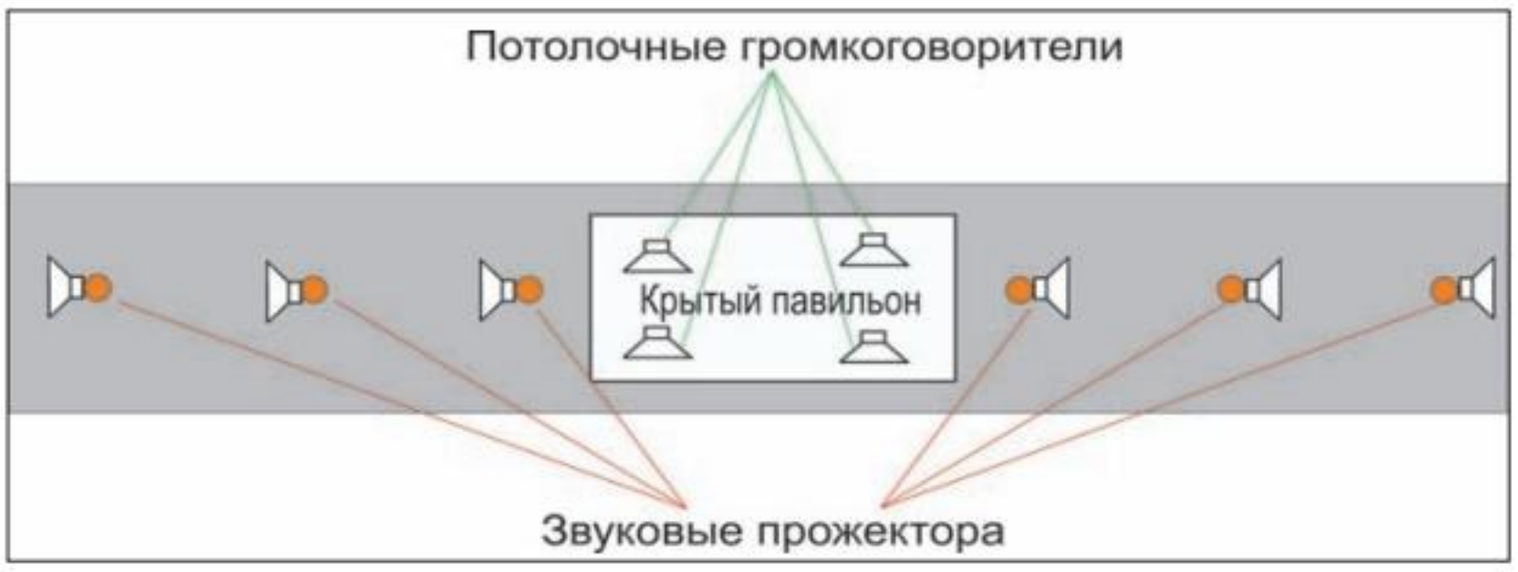


Рис. 5. Примерная расстановка громкоговорителей на станционной платформе

На открытых территориях

Для открытых территорий, как правило, применяют различные типы рупорных громкоговорителей различной направленности. Помимо уровня окружающего шума для открытых пространств, следует учитывать тип застройки на территории, ее конфигурацию (площадь, улица, объект сложной формы с протяженным периметром и т.п.). Например, при построении системы оповещения небольшого населенного пункта обычно расчет производят как для открытой местности, а затем, в зависимости от типа застройки (одноэтажная, малоэтажная или многоэтажная), вводят соответствующий поправочный коэффициент.

Если же на территории присутствует источник повышенного шума, то весьма полезно при проведении предпроектного обследования пройтись по этой территории с шумомером, благо что в настоящее время существуют мобильные приложения для смартфонов, реализующие эту функцию. Следует отметить, что достаточная разборчивость (более 80%) реализуется при превышении уровня звукового сигнала над шумом не менее чем на 12–15 дБ (см. рис. 3).

Еще один скользкий момент связан с ветром. Вернее, с розой ветров в месте расположения озвучиваемого объекта. Если последняя такова, что преобладают ветры определенного направления либо они в одном направлении гораздо сильнее, то этот фактор тоже полезно учесть, располагая громкоговорители с подветренной стороны так, чтобы звук не сдувало с нужной территории.

Отдельно стоит обозначить протяженные объекты, такие как улицы, периметральные ограждения платформ железнодорожных станций. Здесь вполне логичным представляется использование громкоговорителей типа "звуковой прожектор". Эти устройства представляют собой компактные широкополосные громкоговорители с узкой диаграммой направленности. Мощность и чувствительность их меньше, чем у рупорных собратьев, однако они очень подходят для систем типа "пешеходное радио", а также для трансляции объявлений на станционных платформах. Дело в том, что звук в этих случаях должен распространяться в определенном направлении, причем качество звука должно быть достаточно высоким для обеспечения достаточной разборчивости в условиях шума. Чтобы избежать наложения звуковых волн от различных громкоговорителей, их располагают так, чтобы излучение велось в одном направлении, на котором нет близко расположенных массивных преград. Для примера приведем варианты расстановки звуковых прожекторов для озвучения улицы и совместного использования потолочных громкоговорителей и звуковых прожекторов для станционной платформы (рис. 4, 5).

Резюме

Конечно, рассмотреть все возможные варианты в объеме данной публикации не представляется возможным, однако надеюсь, что основную идею подхода к созданию корректно работающих систем озвучения, состоящую в нераздельной оценке не только известных из описания параметров, но и ситуационных данных, мне удалось донести до читателя. ■

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

Пожарная безопасность в ОАО "РЖД"

В ОАО "РЖД" ежегодно формируется комплексная программа "Пожарная безопасность", охватывающая все функциональные филиалы, в которой отражены основные мероприятия в области пожарной безопасности.
Полное исполнение законодательства в области пожарной безопасности является одной из приоритетных задач ОАО "РЖД"

Основными источниками пожарной опасности на подвижном составе и объектах инфраструктуры железнодорожного транспорта могут являться электрооборудование локомотивов, технические неисправности, некачественное обслуживание электрических сетей. В пассажирском подвижном составе это могут быть котлы отопления, неосторожное обращение с огнем посторонних лиц.

Причиной пожаров может стать также нарушение государственных стандартов и правил погрузки (трение грузов, самовозгорание). Значительную опасность представляют неисправность электрооборудования и приборов отопления, а также аварии и крушения.

Подвижной состав ОАО "РЖД" оборудуется современными средствами обнаружения и тушения пожаров

Стандарты компании в области пожарной безопасности

Для обеспечения пожарной безопасности в ОАО "РЖД" создана система управления пожарной безопасностью. Разработаны следующие стандарты компании:

- СТО РЖД 1.15.009-2013 "Система управления пожарной безопасностью в открытом акционерном обществе "Российские железные дороги". Основные положения";
- СТО РЖД 1.15.007-2009 "Система управления пожарной безопасностью в открытом акционерном обществе "Российские железные дороги". Декларирование пожарной безопасности";
- СТО РЖД 1.15.010-2009 "Система управления пожарной безопасностью в открытом акционерном обществе "Российские железные дороги". Организация обучения";
- СТО РЖД 15.019-2017 "Система управления пожарной безопасностью в ОАО "РЖД". Порядок организации и проведения производственного контроля".

Новое в 2017 г.

В 2017 г. произошел ряд изменений в нормативно-правовом поле.

Так, фактически вступило в действие изменение № 1 в своде правил СП 153.13130.2013 "Инфраструктура железнодорожного транспорта. Требования пожарной безопасности" после регистрации Федеральным агентством по техническому регулированию и метрологии 21 августа 2017 г. Внесение изменений и дополнений в свод правил позволило гармонизировать систему нормативного регулирования пожарной безопасности на железнодорожном транспорте в соответствии с современными требованиями.

Риск-ориентированный подход

В ОАО "РЖД" для системного осуществления обеспечения пожарной безопасности на объектах защиты принято направление риск-ориентированного подхода в обеспечении пожарной безопасности. Для этого в настоящее время в ОАО "РЖД" разработаны и введены в действие следующие документы: "Методика расчета пожарного риска на железнодорожных вокзалах", "Методика расчета пожарного риска в информационно-вычислительных центрах ОАО "РЖД", "Методика расчета пожарного риска на постах ЭЦ, ДЦ, ГАЦ и домах связи", "Методика расчета пожарного риска на тяговом подвижном составе".

С 2011 г. введены в строй 134 пожарных поезда нового поколения

Политика импортозамещения

ОАО "РЖД" в полной мере поддерживает государственную политику в сфере импортозамещения и при обеспечении объектов защиты средствами пожаротушения и системами противопожарной защиты по возможности отдает предпочтение отечественным производителям.

Кроме технического оснащения, в компании большое внимание уделяется повышению культуры пожарной безопасности, квалификационной и психологической подготовленности работников компании. При таком подходе пожарная безопасность рабочих мест и стационарных объектов становится внутренней потребностью работника, приводящей к осознанию личной ответственности и самоконтролю в процессе выполнения работ.

В ОАО "РЖД" используется автоматизированная система управления "Пожарная безопасность" (АСУПБ). Функции АСУПБ:

- осуществление контроля работы пожарных поездов, мониторинг пожаров и загораний на объектах защиты ОАО "РЖД";
- контроль профилактической работы на объектах защиты ОАО "РЖД";
- содержание информации о стационарных объектах защиты ОАО "РЖД" и их оснащенности пожарной техникой. ■

Пресс-служба ОАО "РЖД"

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

GST

United Technologies

Эталон качества и доступных цен!

25 ЛЕТ ИННОВАЦИЙ

УСПЕХ В 80 СТРАНАХ

УМНЫЕ СИСТЕМЫ

www.utcfssecurityproducts.eu,
www.ahi-carrier.ru

AHI CARRIER FZC

Волоконно-оптические тепловые линейные пожарные извещатели: что предлагает российский рынок?

Владимир Фомин
Профессор кафедры пожарной автоматики Академии ГПС МЧС России, к.т.н., доцент

Волоконно-оптические системы пригодны не только для передачи информации, но и в качестве локальных распределенных измерительных датчиков. Физические величины измерения, например температура или давление, могут воздействовать на оптическое волокно и менять свойства световодов в определенном месте. В середине 1990-х гг. в США были внедрены волоконно-оптические линейные тепловые извещатели различных наименований и принципов действия, наиболее известным из которых является датчик типа "Оптический с измерением коэффициента отражения методом совмещения прямого и отраженного испытательных сигналов" (Optical Time Domain Reflectomery, OTDR)

Классическая техника временной оптической рефлектометрии OTDR основана на определении разности времени между моментами передачи светового импульса и приема обратнорассеянного света, а также зависимости интенсивности рассеянного света от времени (то есть от расстояния вдоль кабеля). Поскольку обратное рэлеевское рассеяние зависит от температуры, оно может быть использовано для измерения температуры по длине кабеля.

Немного истории

Работы по применению волоконно-оптического кабеля для измерения температуры проводились и в России. В институте "Гипроуглеавтоматизация" Комитета по угольной промышленности при Министерстве топлива и энергетики РФ в конце 1990-х гг. на основе волоконно-оптической техники разработано линейное средство контроля температуры, которое способно не только генерировать сигнал о начавшемся пожаре при достижении температуры воздушной среды аварийного уровня, но и обеспечить постоянный мониторинг температуры во всем диапазоне ее реальных изменений. Это позволяет более надежно и своевременно диагностировать процессы возгорания на ранней стадии.

Разработанное в институте "Гипроуглеавтоматизация" устройство (далее – термокабель) представляет собой многоканальную измерительную систему, в которой волоконный световод является одновременно и средой передачи информации, и совокупностью чувстви-

Таблица 1. Технические характеристики комплекса ОПК

Контроль температуры воздушной среды:	
● **пределы измерения, °С**	**-30...+95**
● **диапазон установок предупредительного порога, °С**	**-25...+60**
● **диапазон установок аварийного порога, °С**	**-40...+80**
Определение градиента нарастания температуры:	
● **минимальный отрезок времени для определения градиента нарастания температуры, с**	**180**
● **значение предупредительной уставки, °С/мин**	**0,5**
Предел допускаемой основной абсолютной погрешности, °С	**3,0**
Предел допускаемого значения дополнительной абсолютной погрешности, не более, °С	**1,5**
Время накопления информации на формирование сигнала "номер пикета – температура", с	**60**
Максимальная длина световода, м	**1500**
Пространственное разрешение (длина элементарного участка измерения), м	**20**
Допустимый радиус изгиба кабеля, не менее, мм	**300**
Время прогрева, не более, мин.	**30**
Стабильность показаний, не менее, сут.	**7**
Потребляемая мощность, не более, ВА	**50**
Рабочее напряжение, В	**12**

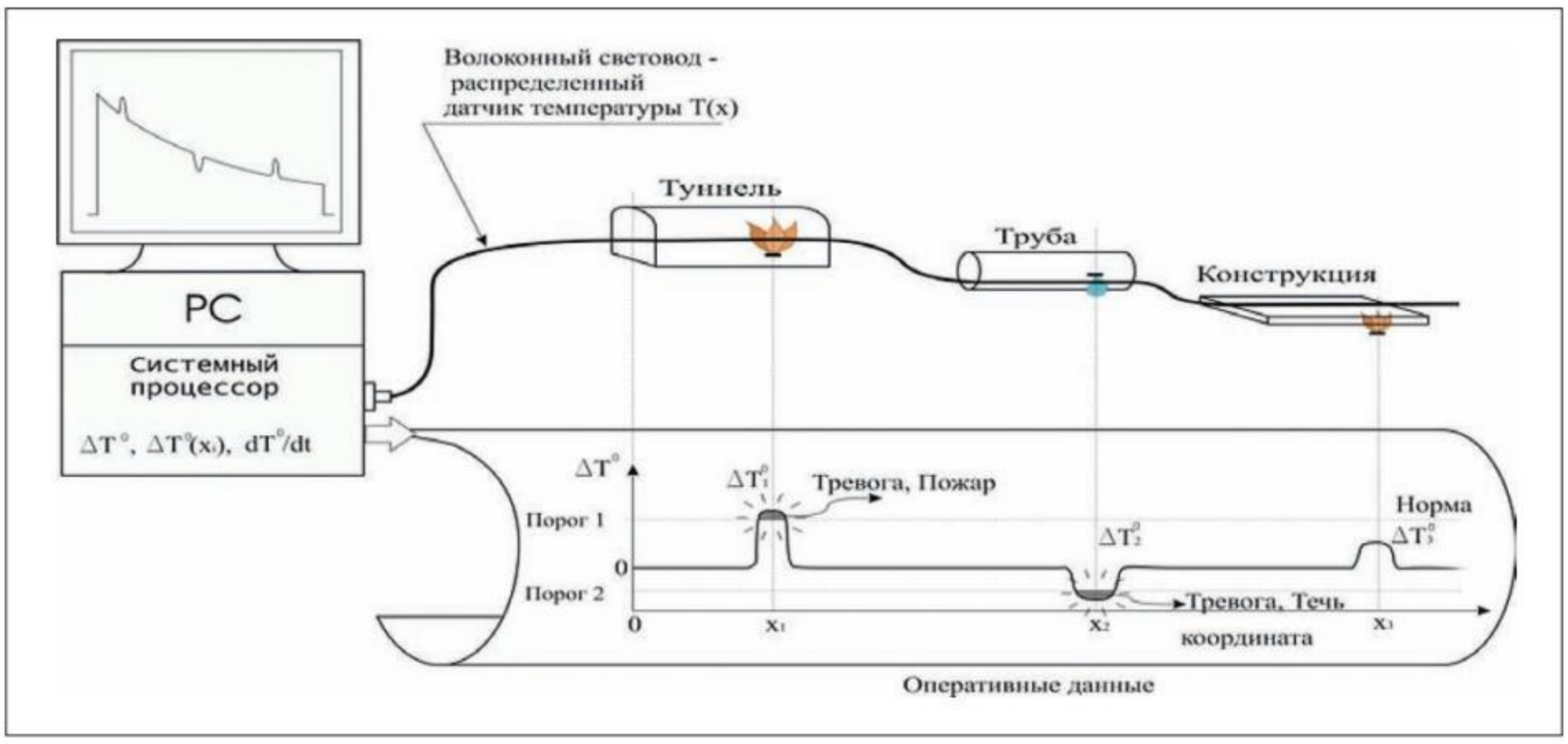


Рис. 1. Применение волоконно-оптического кабеля

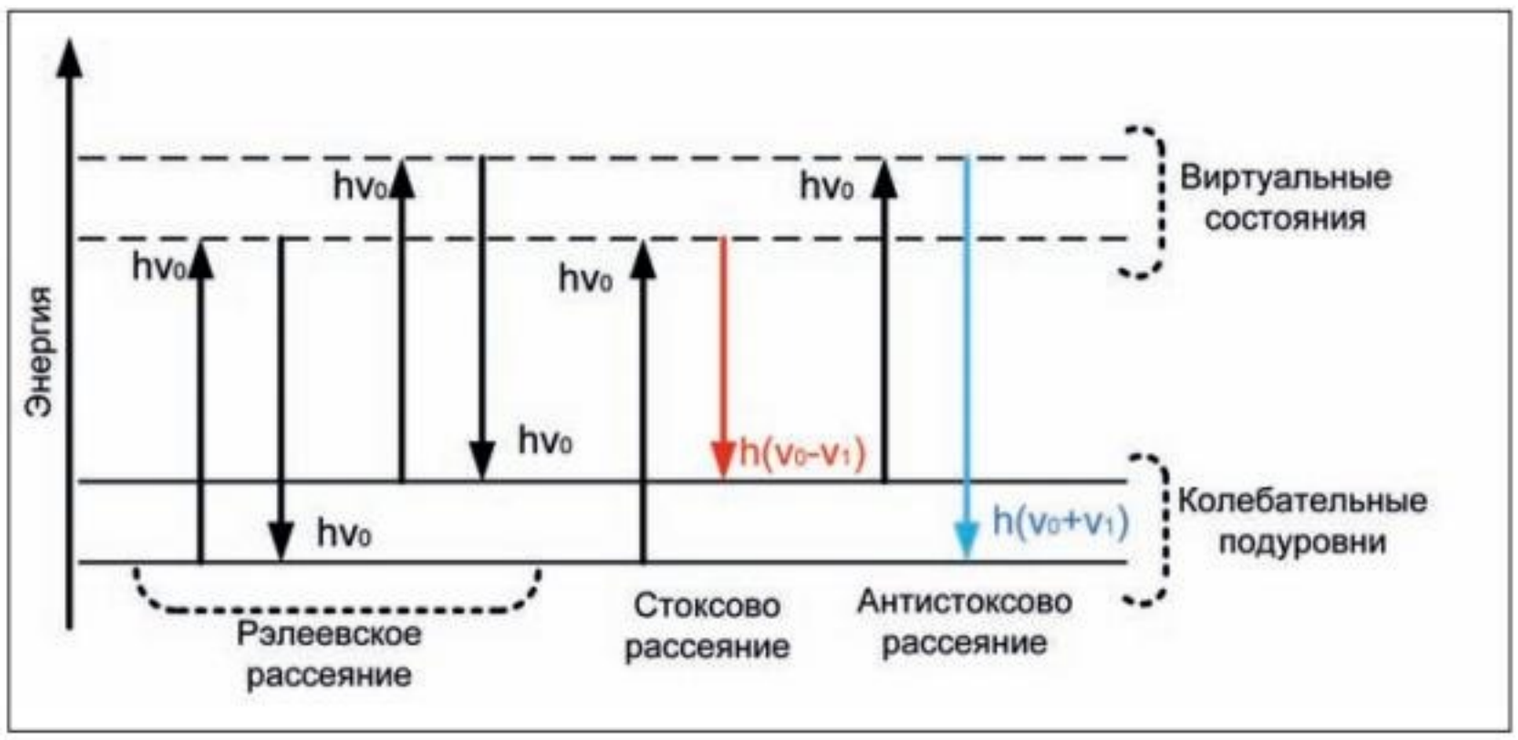


Рис. 2. Рэлеевское и рамановское рассеяние света

тельных элементов, реагирующих на изменения температуры окружающей воздушной среды в каждом из измерительных участков. При этом формируется сигнал, несущий информацию о номере участка по длине и температуре воздушной среды в пределах этого участка (каждому участку соответствует волоконно-оптический канал в 20 погонных метров термокабеля).

Принцип работы волоконно-оптического кабеля

В волоконно-оптический кабель посылается световой импульс. В отсутствие заметных температурных градиентов вдоль кабеля импульс отражается от конца световода и возвращается через время, определяемое двойной длиной световода. При наличии температурных изменений на любом участке световода часть энергии светового импульса отражается на другой длине волны. Регистрируя по принципу радиолокации время возврата импульса, определяется координата аномалии. Измеряя амплитуду сигнала отраженного импульса на смещенной частоте, определяется температура в месте аномалии и ее градиент.

Волоконно-оптический кабель по своей физической сущности электрически пассивен, вследствие чего он невосприимчив по отношению к электромагнитным помехам и полям любой напряженности. Кроме того, он негорюч, взрывобезопасен и стоек к коррозии. Термокабель получил промышленное название "Комплекс раннего обнаружения пожаров на ленточных конвейерах (комплекс ОПК)". Его технические характеристики представлены в табл. 1.

Успешное проведение испытаний

В течение 2001 г. комплекс ОПК проходил эксплуатационные испытания на ОАО "Шахта Инская" ("Беловоуголь") в системе противопожарной защиты конвейерных ставов в главном стволе № 3 и главном конвейерном квершлаге. За время испытаний отказов в работе комплекса не наблюдалось. Технические характеристики комплекса подтверждены эксплуатационными испытаниями на шахте. Комплекс надежно измеряет температуру воздушной среды в контролируемой выработке по всей ее длине и обеспечивает передачу информационных сигналов в автоматизированную систему контроля за пожароопасностью.

На рис. 1 схематично представлено применение волоконно-оптического кабеля в качестве пожарного извещателя и датчика температуры на различных объектах.

Методы измерения температуры

Для измерения температуры с помощью световодов, изготовленных из кварцевого стекла, особенно подходит так называемый эффект Рамана. Свет в стеклянном волокне рассеивается на микроскопически малых колебаниях плотности, размер которых меньше длины волны (рис. 2). В отличие от входящего, обратнорассеянный свет содержит как компоненту с начальной длиной волны (обусловленную эластичным, или рэлеевским, рассеянием), так и компоненты, подвергшиеся спектральному сдвигу на частоту, соответствующую резонансной частоте колебаний рассеивающих узлов (комбинационное рамановское рассеяние). Компоненты со смещенной длиной волны образуют в спектре рассеянного света линии-спутники, которые делятся на стоксовы (сдвинуты к большим длинам волн и меньшей частоте) и антистоксовы (сдвинуты к меньшим длинам волн и большей частоте).

Комбинационное рамановское рассеяние значительно (на три порядка) слабее рэлеевского, поэтому оно не может быть измерено с помощью техники OTDR. Однако оно используется в более сложной технике частотной оптической рефлектометрии (Optical Frequency Domain Reflectometry, OFDR).

Интенсивность антистоксовой полосы рамановского рассеяния зависит от температуры, в то время как стоксова полоса почти не зависит от температуры. Измерение локальной температуры в любом месте световода следует из отношения интенсивности антистоксового и стоксового света. Благодаря оптическому методу обратного комбинационного рассеяния можно измерять температуру вдоль стеклянного волокна как функцию места и времени.

Тепловые линейные пожарные извещатели российского производства

Технику OFDR для обнаружения пожара первой стала использовать компания AP Sensing, США, в тепловом линейном взрывобезопасном лазерном извещателе LHS (Linear Heat Series). Он состоит из измерительного блока AP Sensing и оптического кабеля. Извещатель защищает зону протяженностью до 2х8 км при обеспече-

Таблица 2. Основные технические характеристики ИП-132-1-Р "Горизонт"

Наименование параметра	Значение
Время непрерывной работы, не менее, ч	24
Диапазон рабочих температур, °С	0...+55
Измеряемый температурный диапазон (в зависимости от типа кабеля и качества оптического волокна), °С	- 200...+650
Температурное разрешение, °С	От 0,1
Тип волокна	Многомодовое, 50/125 или 62,5/125 мкм
Длина волны лазера, нм	975 или 1550
Диапазон длин при детектировании, км	0,5/2/4/8/12/15
Шаг измерения по длине, м	1
Номинальное напряжение питания, В	24 (DC), 220 (AC)
Потребляемая мощность, Вт	17–40
Время одного измерения, с	От 1
Точность определения температуры (предел допускаемой основной погрешности), не хуже, °С	± 0,5 (после калибровки ±0,1)
Точность определения места обрыва волоконно-оптического кабеля, не более, м	1
Габаритные размеры (высота х ширина х глубина), мм	131х432х415
Масса, не более, кг	10
Электрические интерфейсы	RS-232/RS-485, USB, RJ-45, реле "сухой контакт", опционально Modbus TCP/IP
Количество каналов	1, 2, 4, 8 или 16
Допустимая потеря сигнала в системе, дБ/км	15
Степень защиты, не ниже	IP40 по ГОСТ 14254–96, IP67 при установке в защитный бокс
Класс лазерной безопасности	1М согласно ГОСТ IEC 60825-1–2013
Полностью распределенные температурные измерения	До 15 000 на 1 канал

Рис. 3. Извещатель ИП-132-1-Р "Горизонт"

нии высокой точности определения места расположения очага 1–3 м.

В России две компании разработали и выпускают волоконно-оптические тепловые линейные пожарные извещатели, реализующие OFDR. Извещатели напрямую конкурируют с иностранными аналогами, которые стоят значительно больше, и не уступают их техническим характеристикам.

Извещатель ИП-132-1-Р "Горизонт"

Тепловой линейный пожарный извещатель ИП-132-1-Р "Горизонт" (рис. 3) разработан и выпускается компанией ООО "КабельЭлектроСвязь".

Световой импульс лазера распространяется по оптическому волокну, небольшая часть света рассеивается. Рассеяние лазерного импульса появляется непосредственно благодаря молекулярным колебаниям в оптическом волокне. Измерение температуры основано на измерении оптического рамановского обратного рассеивания с использованием оптической рефлектометрии во временной области (рис 4.). Температура в этой системе измерений пропорциональна соотношению мощностей стоксовской и антистоксовской компонент рамановского излучения, которые регистрируются в виде температурной зависимости по длине кабеля.

Основные технические характеристики ИП-132-1-Р "Горизонт" представлены в табл. 2.

Извещатель ИП 132-1-Р "Елань"

Тепловой линейный пожарный извещатель ИП-132-1-Р "Елань" (рис. 5) разработан и выпускается компанией ООО "Этра-спецавтоматика".

Предназначен для обнаружения загораний, сопровождающихся повышением температуры, в неотапливаемых или отапливаемых закрытых помещениях различных зданий и сооружений, а также на кораблях, судах, объектах подвижного состава железнодорожного транспорта и других промышленных объектах (электрооборудование подгрупп IIA, IIB, IIC температурного класса Т6 по ГОСТ Р 52350.14–2006) и передачи сигнала "Пожар" приемно-контрольному прибору.

Область применения извещателя – линейно-протяженные помещения либо с большими площадями потолков (тоннели, кабельные коллекторы, производственные цеха, складские комплексы, торговые центры).

Извещатель подходит для взрывоопасных зон помещений и наружных установок, согласно ГОСТ Р 52350.10–2005, ПУЭ издание 6 гл. 7.3 и другим нормативным документам, регламентирующим применение электрооборудования во взрывоопасных зонах.

Состоит из чувствительного элемента (ЧЭ) и блока обработки (БО). В качестве ЧЭ извещателя используется оптоволоконный кабель, прокладываемый в контролируемой зоне.

ИП-132-1-Р "Елань" совместим с большинством ПКП и полностью соответствует требованиям ГОСТ Р 53325.

По принципу действия ИП относится к тепловым извещателям с использованием материалов, изменяющих оптическую проводимость в зависимости от температуры. Для определения места изменения температуры в оптоволоконном кабеле применяется полупроводниковый лазер, метод основывается на эффекте Рамана. Извещатель, получив информацию по температуре оптического волокна от чувствительного элемента, проводит дорасчет данных для получения температуры на оболочке кабеля.

В состав чувствительного элемента извещателя входят собственно оптоволоконный кабель и терминатор, которые могут располагаться во взрывоопасных зонах. Для стыковки с БО используется оптический коннектор.

ЧЭ извещателя имеет маркировку взрывозащиты по ГОСТ Р ЕН 13463.1–2009 Ex op is IIC T6 Ge или Ex op is I Ma.

Технические характеристики ИП 132-1-Р "Елань" приведены в табл. 3, а в табл. 4 – эксплуатационные ограничения.

Ключевые технологические преимущества

Волоконно-оптические тепловые линейные пожарные извещатели имеют несомненные преимущества перед другими типами извещателей.

Таблица 3. Технические характеристики ИП 132-1-Р "Елань"

Наименование параметра	Значение
Обеспечиваемые температурные классы	● A1, A2, A3, B, A1R, A2R, A3R, BR, R (ЧЭ с кабелем ОКС"п"-М1-01-1МГ2-0,7) ● A1, A2 A3, B, C, D, E, F, G, A1R, A2R, A3R, BR, CR, DR, ER, FR, GR, R (ЧЭ с кабелем ОКС"ф"-М1-01-1МГ2-0,7)
Длина зоны контроля, м	4
Длина линейного ЧЭ (оптоволоконного кабеля):	
● максимальная, м	8000
● минимальная, м	16
Количество зон контроля:	
● максимальное	2000 (= длина ЧЭ/длина зоны)
● минимальное	4 (= длина ЧЭ/длина зоны)
Мощность лазерного излучения не более, мВт	10
Напряжение питания БО, В	10–28
Потребляемый ток БО, не более, А	1,5
Сопротивление замкнутых контактов реле БО, не более, Ом	30
Степень защиты оболочки блока обработки	IP42
Маркировка взрывозащиты:	
● блок обработки	● [Ex op is T6 Ga] IIC или [Ex op is Ma] I
● чувствительный элемент	● Ex op is IIC T6 Ga или Ex op is I Ma (ЧЭ с кабелем ОКЛ-Н-01-4-16-10/125–0,36/0,22–3,5/18–0,25)
Габариты блока обработки ИПТЛ "Елань" (ширина х высота х глубина, без учета креплений), не более, мм	260x380x130
Вес БО ИП, не более, кг	4

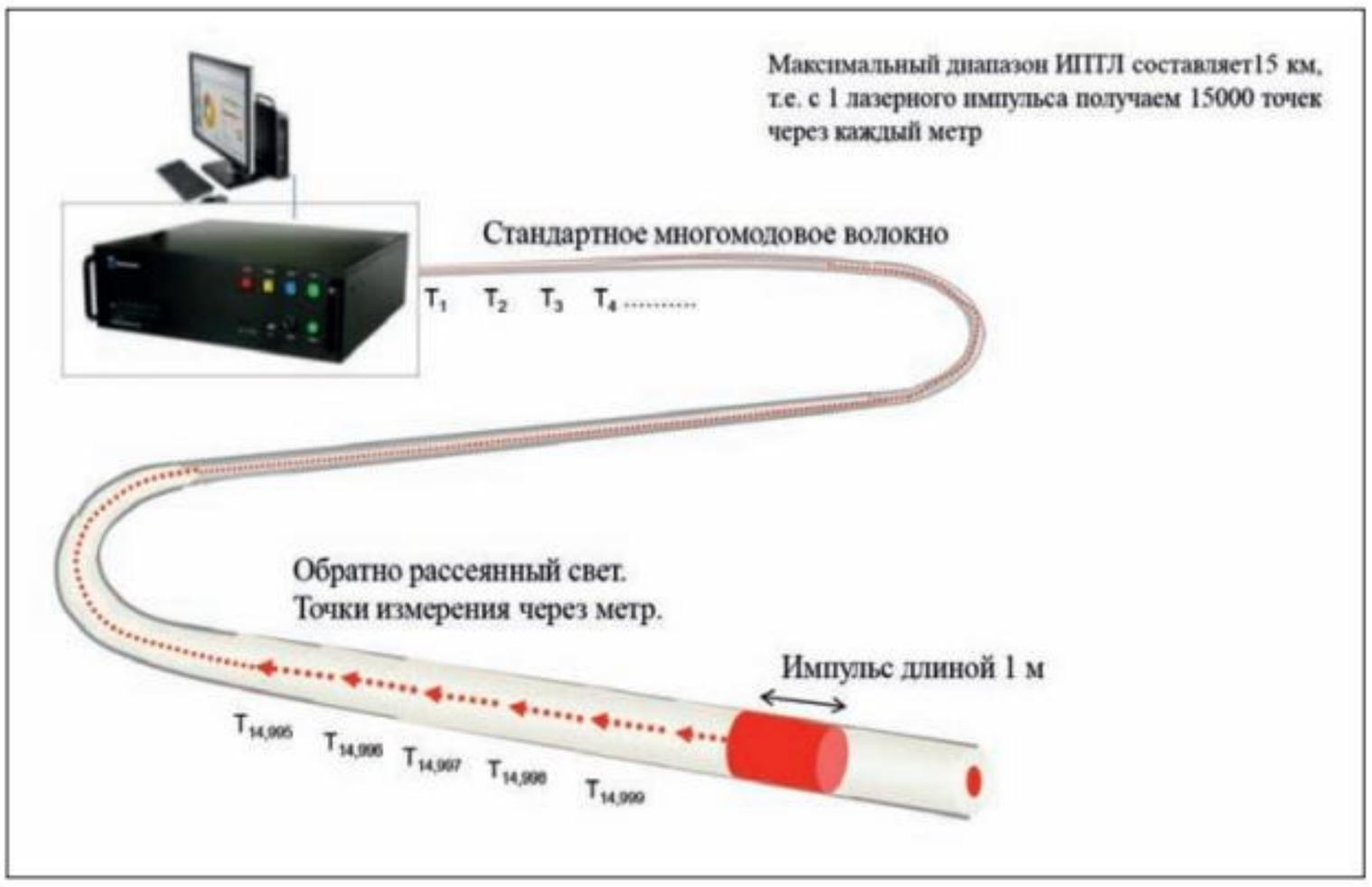


Рис. 4. Принцип оптического рефлектометра

Таблица 4. Эксплуатационные ограничения извещателя ИП 132-1-Р "Елань"

Параметр	Ограничения	
	Минимально	Максимально
Блок обработки		
Допустимая температура в месте размещения БО извещателя при эксплуатации, °С	+10	+50
Допустимая относительная влажность в месте размещения БО извещателя при эксплуатации, % RH	10	70
Допустимое напряжение питания БО извещателя, В	10	28
Чувствительный элемент		
Допустимая относительная влажность в месте размещения чувствительного элемента, % RH	0	100
Допустимая температура в месте размещения ЧЭ ОКС"п"-М1-01-1МГ2-0,7, °С	-40	-70
Допустимая температура в месте размещения ЧЭ ОКС"ф"-М1-01-1МГ2-0,7, °С	-55	-140
Блок релейного расширителя		
Допустимая температура в месте размещения БРР извещателя при эксплуатации, °С	-10	-70
Допустимая относительная влажность в месте размещения БРР извещателя при эксплуатации, % RH	10	95

Рис. 5. Блок обработки ИП132-1-Р "Елань"

- Электрически нейтральны, применение неэлектрических средств измерения, оптоволоконного кабеля позволяет использовать извещатели на предприятиях нефтегазового комплекса, химических производствах, предприятиях металлургии и энергетики, в тоннелях, коллекторах, кабельных каналах, в складских комплексах и торговых центрах.
- Могут эксплуатироваться в условиях воздействия солевого тумана, влаги, пыли, агрессивных сред, вибрации.
- Линейный чувствительный элемент можно проложить в непосредственном контакте с защищаемым оборудованием, в любых труднодоступных местах.
- Невосприимчивы к электромагнитному излучению.
- Безопасны даже при повреждении чувствительного элемента в условиях взрывоопасной атмосферы, не приведут к взрыву.
- Быстрые измерения: для определения температуры требуется от 1 с.
- Контроль изменения состояния по температуре в режиме реального времени.
- Контроль больших площадей, большая протяженность зоны обнаружения.
- Точное определение места пожара.
- Устойчивы к различным внешним воздействиям (тепло, холод, влажность, коррозия, механические воздействия, агрессивные среды).
- Минимальные затраты на обслуживание: волоконно-оптический кабели имеют срок службы до 25 лет.
- Оборудование нового поколения сертифицировано согласно ФЗ № 123-ФЗ от 22.07.2008 г. и соответствует ГОСТ Р 53325–2012. ■

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

КОЛОНКА РЕДАКТОРА

В ногу со временем

Железнодорожный транспорт занимает ведущую позицию в транспортной сети России. Несомненными преимуществами железнодорожного транспорта являются массовость перевозок пассажиров и грузов, высокая пропускная и провозная способность железных дорог, которая исчисляется миллионами тонн грузов и огромным количеством пассажиров, систематичность перевозок с достаточно высокой скоростью, приемлемая стоимость, а также высокий уровень безопасности и более низкая степень ущерба окружающей среде. Российские железные дороги отличаются высокой технической оснащенностью, которая включает в себя качественное оборудование путей, протяженную электрифицированность линий сети, железнодорожные подъездные пути к крупным предприятиям, мощный парк современных локомотивов и автоматизированную систему управления.

Ликвидация причин аварий, нештатных ситуаций, исключение дефектов в работе являются важными задачами поддержания развития экономики железнодорожного транспорта. Большая часть сотрудников в РЖД ответственно подходит к исполнению своих должностных обязанностей, что выражается в обеспечении эффективной и, самое главное, безаварийной работы. В то же время на железных дорогах число нештатных ситуаций не снижается и отмечается ухудшение ситуации с безопасностью движения. Впоследствии увеличивается угроза здоровью и жизни людей, теряются перевозимые грузы, портится техника, что приводит к огромным убыткам на предприятии. В этой связи в железнодорожную отрасль регулярно внедряют модернизированное оборудование и современные автоматические средства.

Наибольшую актуальность в последнее время приобретают беспроводные системы безопасности, а именно персональные браслеты. Такие устройства обеспечивают автоматическое оповещение о приближении поезда, дистанционное управление заградительной сигнализацией, контроль выполнения работниками своих обязанностей благодаря датчику неподвижности. Помимо этого, персональный носимый браслет используется для решения задач безопасности перевозимых грузов, а также позволяет обеспечить пожарную и охранную безопасность на вокзалах и терминалах.

Михаил Левчук
Редактор рубрики
"Беспроводные технологии",
исполнительный директор
ООО "Аргус-Спектр"

Беспроводные технологии для обеспечения безопасности на железнодорожном транспорте

Железнодорожный транспорт является одним из самых востребованных способов перевозки пассажиров и грузов в России. Для обеспечения безопасных перевозок и эффективной работы сотрудников в РЖД регулярно производится модернизация оборудования и внедрение новых средств автоматики. В статье рассмотрим примеры реализованных проектов и пилотных зон с использованием беспроводных систем безопасности на железнодорожном транспорте

Василь Кровяков
Начальник технического отдела
ООО "СМ-Уфа"

Обеспечение безопасности перевозки пассажиров и охраны труда сотрудников является одним из приоритетных направлений деятельности РЖД.

Переезд

Железнодорожный переезд является одним из наиболее опасных и ответственных участков пути. Несмотря на то что все переезды оборудованы автоматической светозвуковой сигнализацией, предупреждающей о приближении поезда, нештатных ситуаций избежать не удается. Ежедневно на путях гибнут 3–4 человека. Только за 2017 г. на переездах было зафиксировано 266 дорожно-транспортных происшествий. Учитывая, что скорости передвижения и трафик с каждым годом растут, в РЖД проводится модернизация и внедрение нового оборудования для предотвращения чрезвычайных ситуаций. Примером является беспроводная система оповещения дежурного по переезду и дистанционного управления заградительной сигнализацией.

Принцип работы системы заключается в том, что при приближении поезда к переезду информация в автоматическом режиме поступает на персональный носимый браслет дежурного по переезду (вибрация, текст, звук), а также отображается на блоке индикации и управления, установленном на посту.

После поступления сигнала дежурный по станции должен убедиться в корректном срабатывании автоматики переезда и отсутствии посторонних предметов на путях. В случае обнаружения нештатной ситуации он обязан включить заградительную сигнализацию для машиниста. В случае нештатной ситуации, например, если на путях находится транспортное средство или животное, дежурный нажимает кнопку на браслете и для приближающегося поезда включается запрещающий сигнал семафора.

Еще одна важная задача – это контроль выполнения дежурным по станции своих обязанностей. Датчик неподвижности позволяет следить за тем, чтобы сотрудник не заснул или не вышел за зону рядом с постом охраны. В случае нарушения информация поступает диспетчеру.

Станция

Рассмотрим использование беспроводной системы оповещения и контроля персонала на станциях на примере Московского центрального кольца. Сегодня оно обслуживает не только грузовые, но и пассажирские перевозки высокой интенсивности. На каждой станции ежедневно работают несколько рабочих бригад. Станции оборудованы автоматикой, которая отслеживает перемещение поездов с указанием расстояния и номера пути.

Одна из важных задач обеспечения безопасной работы сотрудников – своевременное оповещение о приближении поезда. При этом стоит учитывать следующие условия:

- интервал движения поездов меньше пяти минут;
- необходимо оповещать только ту бригаду, которая находится в непосредственной близости от пути, по которому едет поезд;
- высокий уровень фонового шума на станции.

Эффективно выполнить эти задачи позволяют персональные носимые устройства с GPS/ГЛОНАСС, интегрированные в общую систему автоматизации станции. На сервер системы с узлов автоматизации поступает информация о приближении поезда с указанием координат и номера пути. Одновременно с этим передаются координаты всех носимых устройств рабочих бригад. Персональное оповещение о приближении поезда приходит в автоматическом режиме тем сотрудникам, которые находятся в непосредственной близости от пути следования состава.

Помимо автоматического оповещения, система поддерживает функцию отправки групповых или персональных сообщений на браслеты с контролем доставки, что позволяет оперативно передавать поручения бригадам.

Рис. 1. Персональное оповещение. Передача сигнала "Тревога"

Другая задача – контроль состояния и местонахождения сотрудников. В случае нештатной ситуации необходимо нажать тревожную кнопку. Информация о происшествии с указанием координат поступит на центральный пункт диспетчера. Аналогичным образом передается тревога при неподвижности. Данные о тревогах и история перемещения каждого сотрудника сохраняются на сервере и позволяют контролировать выполнение бригадами своих обязанностей и получать статистику по числу нештатных ситуаций.

Перегон

Все железные дороги требуют непрерывного контроля состояния путей и сооружений (в том числе тоннелей и мостов), их текущего содержания и ремонта.

Данные работы связаны с повышенной опасностью, поскольку в большинстве случаев ведутся без остановки движения поездов, скорости движения которых превышают 110 км/ч, на перегонах отсутствует стационарная автоматизация. В момент приближения поезда к участку пути, на котором ведутся работы, необходимо экстренное оповещение работников, и наиболее эффективным способом оповещения является персональное оповещение.

Передающим устройством оборудуется локомотив, и при приближении на расстояние до трех километров от проведения работ информация автоматически поступает на устройства персонального оповещения рабочих. Помимо этого, в случае возникновения чрезвычайной ситуации сигналист может экстренно передать сигнал "Тревога" на центральный пункт с указанием координат.

Перевозка грузов

В России ежегодно перевозятся сотни тысяч грузовых вагонов, более миллиарда тонн грузов. Поскольку грузы имеет большую стоимость, а время доставки, как правило, составляет несколько дней, необходимо обеспечить сохранность имущества на всем протяжении пути.

Применение беспроводных систем безопасности позволяет существенно повысить степень защиты грузов и сотрудников ведомственной охраны или военнослужащих, а также скорость реагирования в случае несанкционированного проникновения или другой нештатной ситуации. Комплект оборудования для охраны грузов включает в себя центральный блок, ретрансляторы, охранные извещатели и устройства персонального оповещения.

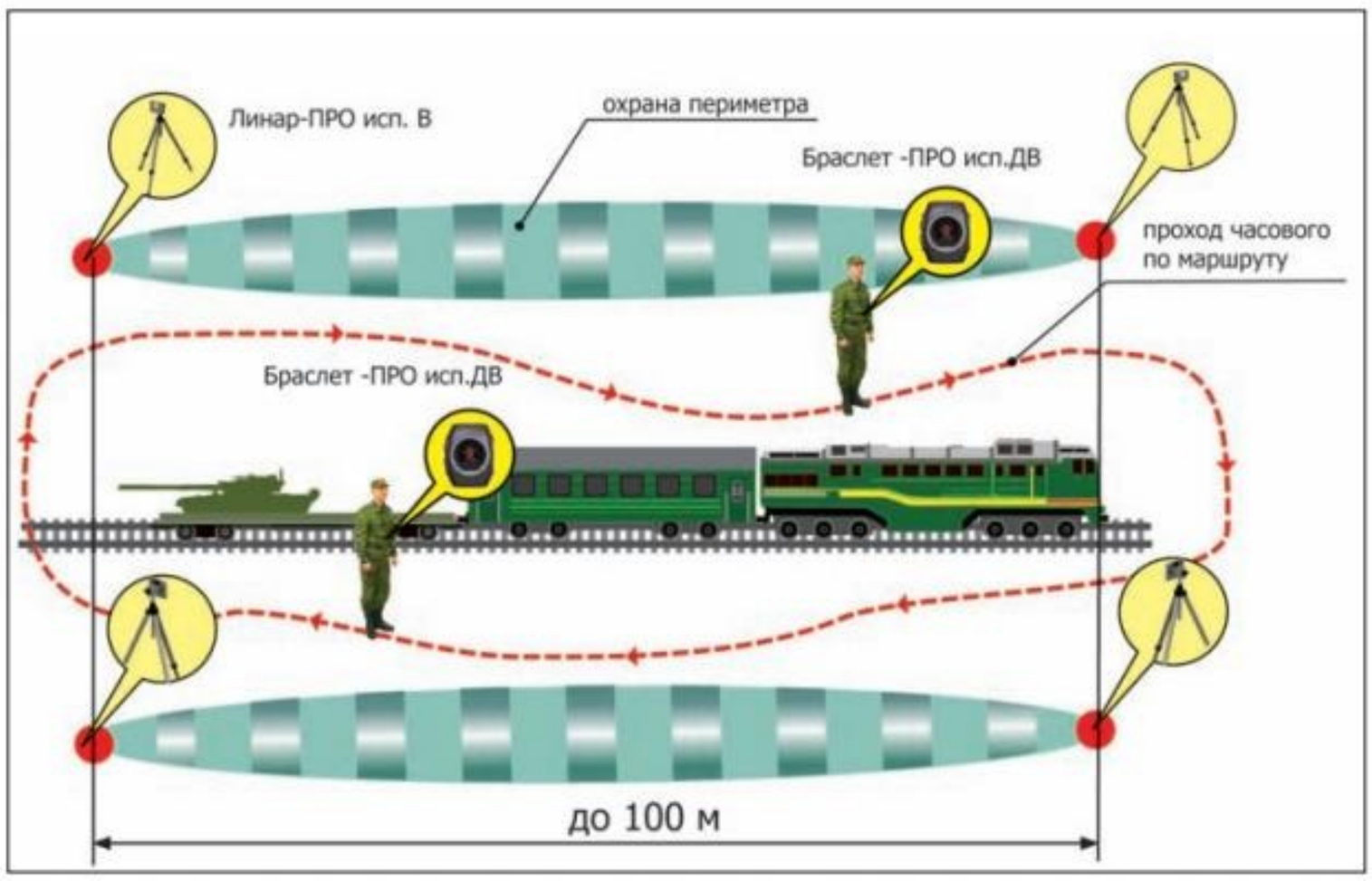


Рис. 2. Позиционирование караулов по сопровождению воинских грузов и создание рубежной охраны с целью недопущения несанкционированного проникновения или порчи охранного объекта

Развертывание такого комплекта занимает 30–40 минут, не требует прокладки проводов и подведения внешнего питания и обеспечивает:

- определение места проникновения (как внутрь вагонов, например при движении, так и пересечение охраняемого периметра во время стоянки);
- оповещение сотрудников о тревогах в автоматическом режиме;
- контроль состояния и местонахождения сотрудников.

Терминалы и вокзалы

В отдельный пункт можно выделить пожарную безопасность объектов, находящихся в эксплуатации, – железнодорожных вокзалов и станций, которые являются объектами массового пребывания людей. Поэтому крайне важно обеспечить максимально надежный уровень их безопасности, включая пожарную, как во время эксплуатации, так и при проведении реконструкции. По данным РЖД, только в 2018 г. планируется отремонтировать 127 таких объектов. Преимущества современных беспроводных систем безопасности в данном случае:

- время монтажа в пять раз меньше, чем в проводных системах;
- не требуется вывод объекта из эксплуатации при установке оборудования;
- не требуется прокладка линий связи после проведения реконструкции;
- обеспечение работоспособности системы за счет резервирования и автоматической перестройки маршрутов даже при выходе из строя части оборудования (например, при пожаре);
- стоимость под ключ не дороже проводных систем.

Использование беспроводных систем позволяет решить еще одну важную задачу – обеспечить персональное оповещение и локализацию персонала и сотрудников службы безопасности внутри помещения. Персональные носимые устройства получают координаты установленных извещателей, что гарантирует точность определения местонахождения каждого браслета вплоть до помещения (извещателя).

С другой стороны, развернутые на станциях системы персонального оповещения и контроля сотрудников позволяют быстро и без затрат на прокладку линий связи и установку контрольных приборов развернуть систему пожарной/охранной безопасности.

Развитие и перспективы

Учитывая стремление руководителей отрасли к повышению безопасности, уровень развития технологий, а также успешные примеры использования современных беспроводных систем сигнализации и оповещения на железной дороге, есть уверенность, что в скором времени удастся существенно повысить безопасность людей и эффективность отрасли в целом. ■

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

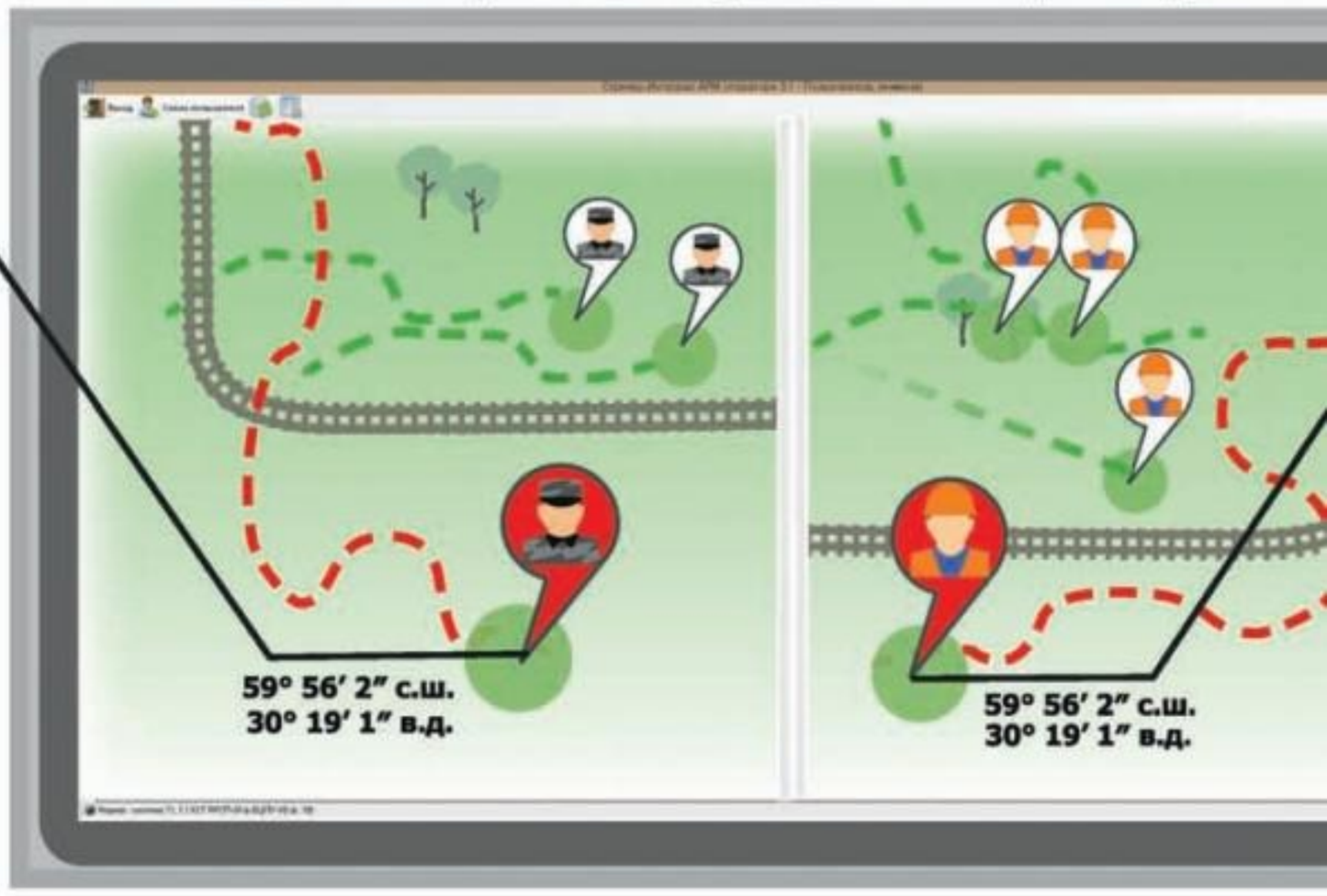
СТРЕЛЕЦ БРАСЛЕТ

ГЛОНАСС / GPS

ГДЕ ВАШ ПЕРСОНАЛ?

ОХРАНА

Локализация на пульте оператора



1. ЛОКАЛИЗАЦИЯ

- определение местоположения браслета **вне** здания.
- определение местоположения браслета **внутри** здания.

ВПЕРВЫЕ В МИРЕ!

2. ПЕЙДЖИНГ

оповещение (пейджинг до 140 знаков):

- общее (о пожаре);
- групповое (о сборе специалистов);
- персональное (вызов).

3. КНОПКА «ВЫЗОВ»

Тревожная кнопка (вызов с браслета с указанием места тревоги).

СИСТЕМА ПЕРСОНАЛЬНОГО ОПОВЕЩЕНИЯ С ЛОКАЛИЗАЦИЕЙ ПЕРСОНАЛА ВНЕ И ВНУТРИ ЗДАНИЙ

КАК ОПОВЕСТИТЬ?

РАБОЧИЕ НА ПУТЯХ

НАЗНАЧЕНИЕ:
- кнопка тревожной сигнализации (КТС)
- оповещение: вибро, экран, звук
- трекинг: ГЛОНАСС / GPS, локализация

ДО 2048 БРАСЛЕТОВ
в системе

РАДИОКАНАЛ:
дальность 5 / 50 км (при ретрансляции)

ОПОВЕЩЕНИЕ
2000 УСТРОЙСТВ за 1 мин.

АВТОНОМНАЯ РАБОТА
до 3-х месяцев работы

ДИАПАЗОН
рабочих температур -50...+55°С

Подробнее о системе:

www.argus-spectr.ru стрелец.рф

КОЛОНКА РЕДАКТОРА

Распределенная многофилиальная СКУД

Рассуждая о распределенных системах безопасности, устанавливаемых в компаниях с филиальной структурой, стоит говорить не столько о системах контроля и управления доступом (СКУД), сколько об интегрированных системах безопасности (ИСБ), так как для крупных распределенных объектов логично объединение всех систем в единый комплекс. СКУД в таких комплексах часто играют важную роль, поскольку имеют развитую внутреннюю логику, позволяющую выходить за рамки типовых действий и реакций обычной системы контроля доступа.

Если внедряемая система является мультибрендовой, построенной на основе оборудования разных производителей, ключевую роль будет играть управляющее программное обеспечение (программная платформа), которое, собственно говоря, и позволяет сопрягать в рамках единой ИСБ оборудование разного назначения. Важнейшей функцией такого ПО становится не только организация управления каждой из подсистем, но и программирование их эффективного взаимодействия. Именно это приводит к синергетическому эффекту, повышающему совокупную ценность ИСБ в глазах потребителя. В противном случае на объектах просто бы устанавливали набор разнокалиберных СКУД, ОПС, CCTV и прочего оборудования со своим управлением. Заказчик прекрасно понимает свою выгоду и способен оценить эффективность разных подходов к формированию системы безопасности своего объекта.

В филиальной системе безопасности важной составляющей является функция централизации управления и сбора данных. Современная ИСБ многофилиального объекта глазами заказчика – прежде всего инструмент получения нужной информации в режиме реального времени, поскольку само управление базируется на правильном понимании текущего состояния всех филиалов компании. Высокая мощность и надежность как аппаратной, так и программной части, резервирование ключевых функций, шифрация трафика на магистралях передачи данных, работа отдельных частей в автономном режиме – только малая часть требований к распределенным многофилиальным системам.

В нашем разделе эксперты расскажут о ПО в области СКУД и ИСБ.

Алексей Гинце

Редактор раздела "Системы контроля и управления доступом", директор по связям с общественностью компании "ААМ Системз"

Системы автомобильной идентификации дальнего радиуса действия

Задача идентификации транспортных средств, а также водителя, управляющего автомобилем, все чаще возникает в самых различных областях и сферах. Бизнес и корпоративная среда создают спрос на получение комфортного и безопасного доступа на офисные парковочные территории с возможностью интегрирования в существующую СКУД. Государственные организации хотят отслеживать и вести учет использования автопарка вместе с идентификацией личности водителя. Промышленным предприятиям необходимо стабильное и устойчивое считывание идентификаторов в любых, даже самых неблагоприятных условиях

Александр Фомин
Инженер технического отдела компании "ААМ Системз"

Рассмотрим технологии, которые позволяют реализовать абсолютное большинство актуальных задач и создать гибкие, комфортные и надежные системы дальней автомобильной идентификации.

Радиочастотные технологии

Большинство задач по дистанционной автомобильной идентификации принято решать при помощи технологии, основанной на высокочастотном электромагнитном излучении. В этой технологии для радиочастотной идентификации используется модулированное обратное рассеяние. Транспондеры, хранящие идентификатор, посылают свой код в считыватель посредством модулирования и отражения сигнала, переданного считывателем. Для уменьшения влияния нежелательных отражений сигнала применяется круговая поляризация, которая, в частности, допускает любую ориентацию меток.

Идентификационные метки

Существуют три общих класса идентификационных меток:

- активные (используется батарейное питание);
- полупассивные (не используют собственную батарею питания, а получают энергию от поля, излучаемого считывателем);
- пассивные, также называются BAP – Battery Assisted Passive (используют радиоинтерфейс

Крепление устройства "бустера" на лобовом стекле автомобиля

и протокол обмена пассивной системы, но есть батарея питания. Дополнительное питание чипа таких меток улучшает их характеристики по дальности чтения и стабильности регистрации).

Важным отличием пассивных меток от активных является то, что первые не излучают радиосигнал. Пассивные метки, отвечая на сигнал считывателя, только модулируют нагрузку своей антенной системы в момент ее нахождения в поле несущей частоты считывателя. Считыватель обнаруживает и детектирует эти слабые отраженные модуляции на фоне непрерывного излучения несущей частоты через свою приемопередающую антенну.

Промышленные системы дистанционной идентификации с частотой 2,45 ГГц

Системы, использующие данную технологию, состоят из считывателей, работающих на частоте 2,45 ГГц, и вышеописанных полупассивных меток. Они обеспечивают исключительно надежное срабатывание на расстоянии до 10 м при движении объекта со скоростью до 200 км/ч. Применение столь высокочастотного излучения позволяет обширно использовать данную систему в сложных условиях окружающей среды, а также при наличии объектов, вызывающих затухание и ослабление электромагнитного излучения.

Полупассивные метки имеют встроенный источник питания, рассчитанный на срок службы обычно до 6–8 лет. Данные, хранящиеся на транспондере, защищены при помощи шифрования, а также сам беспроводной интерфейс связи между считывателем и меткой подвергается шифрованию, что делает невозможным несанкционированный доступ к системе.

Кроме того, есть специальные метки – "бустеры", позволяющие передавать код бесконтактных карт. Существует поддержка наиболее популярных видов карт – как Proximity (125 кГц), так и Smart (13,56 МГц). Такие "бустеры" выполнены в виде устройства, которое крепится на лобовое стекло автомобиля и имеет слот для установки низкочастотных карт. При попадании в поле считывателя "бустер" транслирует номер установленной в него карты. При этом считывание происходит на большой дальности, недостижимой для самих Proximity- или Smart-считывателей и меток. Такое решение позволяет использовать одни и те же карты как для доступа внутрь помещения, так и при автомобильной идентификации водителя.

Очень полезным свойством таких "бустеров" является то, что они также обладают своим собственным уникальным номером и способны передавать его вместе с номером карты (с некоторым временным промежутком). Это позволяет осуществлять не только идентификацию водителя, но и идентификацию автомобиля.

Считыватели, работающие на частоте 2,45 ГГц, обычно оснащены выходом стандартного интерфейса Wiegand и могут быть без каких-либо сложностей подключены к подавляющему большинству систем контроля доступа.

Таким образом, системы, работающие на технологической платформе 2,45 ГГц, рекомендуются для использования на промышленных и индустриальных объектах, позволяют надежно идентифицировать транспортные средства в различных условиях и дают ответ на следующий вопрос: кто именно и на каком автомобиле перед нами находится (въезжает или выезжает с объекта)?

Системы дальней идентификации технологии UHF

Система UHF (Ultra High Frequency) использует электромагнитные волны большей длины, чем предыдущая, и работает в диапазоне частот 866,3–867,6 МГц. Метки, используемые системой, не содержат источника питания (являются пассивными) и используют принятую от считывателя энергию, которая после изменения снова передается в считыватель. Этот принцип называется модулированным обратным рассеянием. Метки можно также назвать устройствами изменения поля. Полученная от считывателя энергия ВЧ-радиосигнала модулируется вместе с данными с чипа, содержащего идентификатор. Для того чтобы метка была считана, она должна находиться в прямой видимости считывателя.

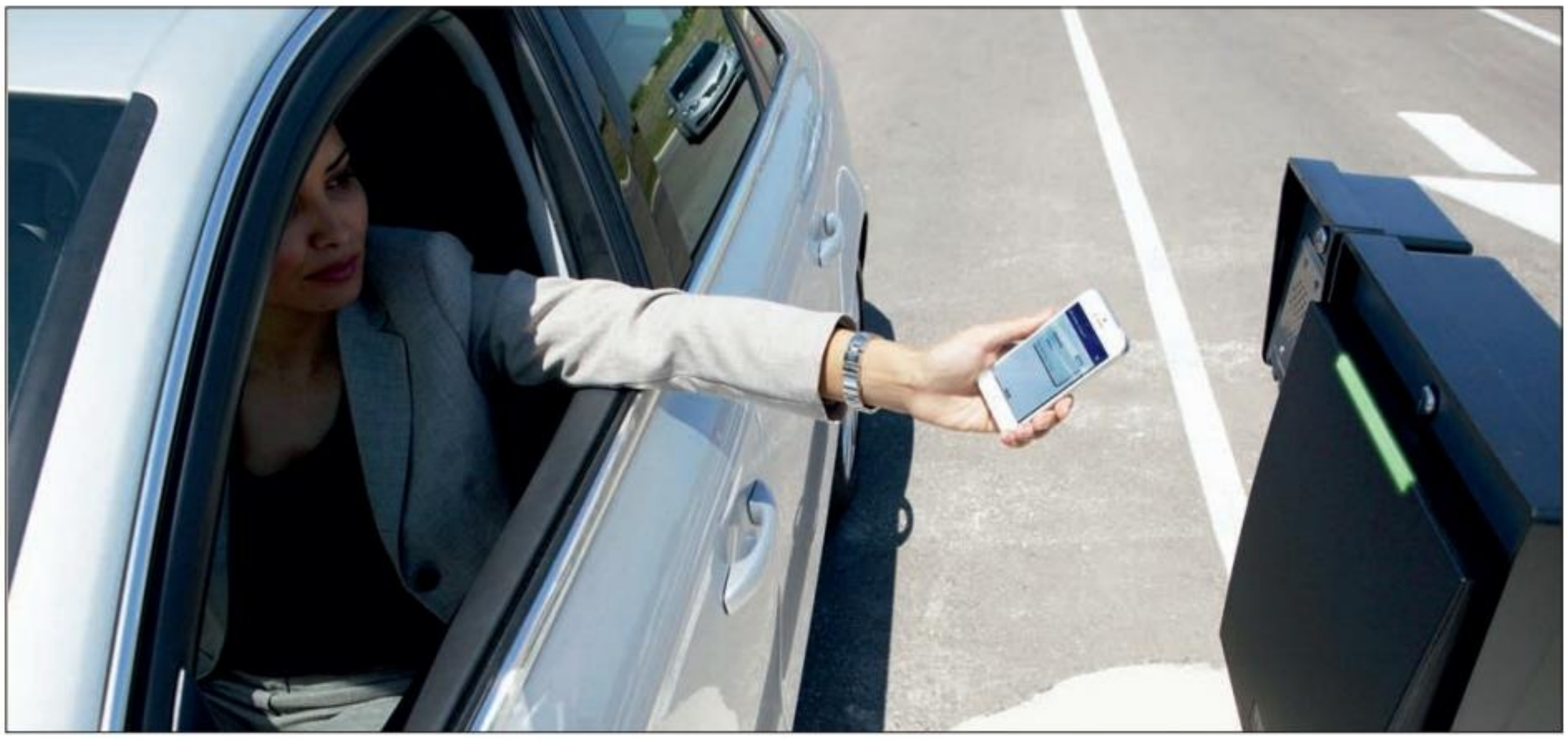
Большинство синтетических материалов прозрачны для ВЧ-сигналов и при небольшом ослаблении в целом не составляют преграды. Снег и лед также не помеха для ВЧ-сигналов, пока они в кристаллическом виде. Однако водная пленка в непосредственной близи от считывателя вызывает снижение дистанции чтения. Сильный дождь не создаст проблем до тех пор, пока на передней крышке считывателя или на метке не образуется водная пленка. Для снижения влияния нежелательных отражений сигнала используется круговая поляризация, что также позволяет свободно ориентировать метку.

Системы UHF исторически появились при решении логистических задач при учете продукции и, исходя из этого, имеют следующие достоинства:

- дистанция регистрации меток для пассивных систем до 10 м;
- эффективный "антиколлизионный" механизм, позволяющий считывать одновременно до 300 уникальных меток в зоне регистрации;
- высокая скорость считывания метки – до сотен раз в 1 с;
- низкая цена простой метки-наклейки.

Сами метки создаются по стандарту EPC Gen2 (Electronic Product Code Class 1 Generation 2), который разработан международной организацией GS1 EPC Global. Как правило, они выполнены в виде наклеек на лобовое стекло, но существует реализация в формате комбинированной пластиковой карты, содержащей в себе как UHF-часть, так и более низкочастотный чип с антенной (Proximity 125 кГц или Smart 13,56 МГц). Это позволяет использовать одну и

Организация въезда на парковку при помощи UHF-считывателя



Организация въезда на парковку при помощи мобильного доступа

ту же карту как для дистанционного доступа, так и для классического прохода в помещение через стандартные считыватели.

UHF-считыватели оснащены выходом Wiegand и способны передавать номер считанного идентификатора в существующую СКУД.

Данная технология UHF является идеальной для решения корпоративных задач и обеспечения комфортного проезда на парковку, обеспечивает идентификацию на расстоянии до 10 м и использует дешевые метки, не имеющие источника питания и, соответственно, ограничения срока службы.

Системы распознавания автомобильных номеров

Данные системы используются в том случае, если не представляется возможной заблаговременная выдача бесконтактных меток для автомобилей посетителей, но необходимо обеспечить комфортный проезд на территорию. Считыватели в таких системах уже включают в себя все необходимые компоненты системы распознавания номеров: видеокамеру, инфракрасную подсветку и блок обработки данных. Все эти устройства заключены в единый компактный корпус, устойчивый к атмосферному воздействию, и позволяют производить считывание номеров на расстоянии до 10 м при движении транспортного средства со скоростью до 140 км/ч.

Данные считыватели могут как служить автономными контроллерами и самостоятельно осуществлять управление шлагбаумом на основании составленных белых и черных списков автомобильных номеров, так и передавать идентификатор, соответствующий автомобильному номеру, при помощи специального модуля преобразования буквенно-цифровой посылки, содержащей номер автомобиля, в сигнал формата Wiegand.

Настройка же таких считывателей, как правило, производится через Web-интерфейс, который предоставляет полный перечень всех возможных функций управления.

Существует ряд строгих инструкций по монтажу такого рода считывателей для обеспечения наилучшего качества распознавания изображения, а также стоит принимать во внимание большое количество мешающих факторов. Самый важный и первичный фактор, определяющий качество считывания, – это, конечно, состояние самого государственного номера автомобиля. Если он будет загрязнен, поврежден или сильно засвечен каким-либо посторонним источником света, то распознавание будет невозможным.

Таким образом, системы распознавания автомобильных номеров, использующие для этого инфракрасные видеокамеры, являются хорошей альтернативой радиочастотным технологиям для автоматической идентификации транспортного средства на больших расстояниях, не требуют выдачу идентификационных меток, однако имеют ряд факторов, существенно влияющих на качество распознавания.

Доступ на парковку по мобильному телефону

Развитием технологии Bluetooth является Bluetooth LE (Bluetooth Low Energy), которая используется в современных системах мобильного доступа, поддерживаемых ведущими производителями компонентов СКУД.

Мобильный доступ (Mobile Access) – это система, в которой в качестве идентификатора используется мобильное устройство (смартфон, планшет, умные часы). При использовании интерфейса связи BLE дальность идентификации может достигать 10 м, что позволяет успешно применять такое решение, например, для пропуска на парковку.

Особенностью мобильного доступа является то, что мобильный идентификатор может быть выдан удаленно через Интернет, а пользователю лишь необходимо установить соответствующее мобильное приложение. На данный момент производители поддерживают широкий спектр современных смартфонов на базе iOS и Android, так что воспользоваться мобильным доступом сможет практически каждый человек, который имеет смартфон с модулем BLE. Это удобно для обеспечения комфортного гостевого доступа на охраняемую территорию, так как нет необходимости в предварительной выдаче физического идентификатора.

Такие считыватели имеют как стандартный выход интерфейса Wiegand, так и поддержку современного защищенного протокола OSDP. Номер считанного мобильного идентификатора будет передаваться в существующую СКУД точно так же, как и от любого другого считывателя.

Безопасный и комфортный проезд на территорию

Системы автомобильной идентификации дальнего радиуса действия реализованы на различных технологических платформах, имеющих свои преимущества и особенности применения. Использование таких систем позволяет ответить нам не только на вопрос "Какой автомобиль?", но и на вопрос "Кто управляет автомобилем?", а также предоставить посетителям комфортный проезд на контролируемую территорию без необходимости покидать транспортное средство для проведения процедуры аутентификации.

Конечно, среди большого количества различных технологий и производителей оборудования конечному пользователю или проектировщику зачастую трудно сориентироваться и сделать правильный выбор в пользу того или иного решения. Специалисты ряда отечественных компаний, занимающихся вопросами дистанционной регистрации автотранспорта, накопили большой опыт применения таких систем в России и помогут подобрать оптимальное решение для конкретной задачи. ■

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

Решения dormakaba для спортивных объектов:

высочайший уровень безопасности и комфорта

При проектировании спортивных арен возникает масса сложностей, ведь принимаемые проектные решения должны обеспечивать самый высокий уровень безопасности и в то же время удовлетворять требованиям заказчика. В портфеле решений dormakaba имеется много интересных, а порой и уникальных продуктов, о которых мы расскажем в этой статье

Стадион не должен простаивать без дела в перерывах между спортивными мероприятиями, а должен быть центром притяжения горожан. Следовательно, требования, предъявляемые к современным спортивным аренам в том числе и с точки зрения обеспечения безопасности, многогранны.

Входная группа

Посещение стадиона начинается с входных групп, именно на этой зоне сосредоточен основной фокус комплексной системы безопасности стадиона, центральное место которой заслуженно занимают турникеты dormakaba, интегрированные с билетно-кассовой системой в единый программно-аппаратный комплекс, предоставляющий санкционированный допуск болельщиков на игру любимой команды и обеспечивающий беспрепятственную эвакуацию в случаях чрезвычайных ситуаций. Для решения этой непростой задачи идеально подходят трехштанговые тумбовые турникеты TPB-E01, которые можно установить на мобильные платформы, что обеспечивает дополнительную гибкость в организации пропускной системы. Полноростовые турникеты с эвакуационной калиткой TTS-M03 отлично зарекомендовали себя как решение, обеспечивающее эвакуацию с территории стадиона.

Контроль доступа в служебные помещения

Служебные помещения стадиона, VIP-зоны, въезды и выезды на территорию спортивного комплекса могут быть надежно защищены одной из самых надежных и защищенных СКУД в мире – dormakaba Exos 9300. Топология системы, применяемые интерфейсы, протоколы, алгоритмы передачи и шифрования данных исключают возможность несанкционированного доступа к служебной информации и копирования носителей электронных пропусков. Система включает в себя как традиционное проводное решение, так и беспроводные компоненты, которые с успехом можно использовать для оборудования внутренних цельностеклянных дверей, например, в VIP-зонах. dormakaba Exos 9300 через OPC-сервер, протоколы BACnet, SNMP может быть интегрирована с внешними системами в единый комплекс инженерно-технических средств безопасности.

Управление эвакуационными выходами

Система управления эвакуационными выходами dormakaba TMS позволяет оборудовать эвакуационные и аварийные выходы электромеханическими и электромагнитными запорными устройствами, обеспечивающими надежное запирание дверей при ежедневной эксплуатации и гарантированную разблокировку в случае эвакуации. Исполнительные устройства, контроллеры, дверные терминалы, блоки управления и индикации объединяются по цифровой шине DCW (DORMA CONNECT AND WORK) в единую систему. Отображение состояния и управление дверьми осуществляется в графическом интерфейсе ПО TMS Soft.

Дверные решения

Внешний вид входных и внутренних дверей оказывает значительное влияние на общий облик и интерьер стадиона. Именно поэтому

специалисты компании уделяют большое внимание комплексному оснащению дверей фурнитурой и исполнительными механизмами. В продуктовом портфеле компании присутствует все необходимое оборудование: дверные доводчики, электромеханические и электромагнитные замки, электрозащелки, моторные замки, оборудование антипаники и дверная фурнитура. Специальные решения на базе автоматических приводов dormakaba ED 250 и оборудования антипаники PHA 2500 позволяют автоматизировать эвакуационные двери, которые будут открываться автоматически в случае пожара и служить дополнительным клапаном подачи свежего воздуха, увеличивая эффективность системы автоматики противопожарной защиты стадиона.

Доступ для маломобильных групп населения

Большое внимание компания уделяет решениям, позволяющим повысить удобство и комфорт посетителей стадиона. Решения dormakaba на базе автоматических приводов позволяют создать безбарьерную среду для маломобильных групп населения, удачным примером которой можно назвать "Безбарьерный санузел". В специальный слот электроники распашного автоматического привода ED250 вставляется плата (функциональная карта), где зашита логика работы "Безбарьерного санузла", кнопок управления, индикаторов "Свободно/Занято" и других исполнительных механизмов. Таким образом, именно привод без участия дополнительных контроллеров управляет всеми устройствами, которые используются в данном решении.

Трибуны

В качестве решений для таких помещений, как VIP-ложи, могут применяться раздвижные стеклянные стены dormakaba HSW. Это стильная, легкая в обслуживании и абсолютно прозрачная безрамная система стеклянных стен, имеющая встроенные функциональные элементы, обеспечивающие их быструю трансформацию в открытое или закрытое положение.

Разделение пространства

На современном стадионе могут проходить различные мероприятия, требующие мобильности в организации пространства. Здесь на помощь приходит уникальное решение компании dormakaba – автоматические мобильные звукоизолирующие стены VARIFLEX. В случае необходимости в считанные минуты по заданному сценарию стеновые панели VARIFLEX, передвигаясь по трекам, сами изменят планировку помещения.

Успешные международные проекты

На стадионах по всему миру можно встретить решения компании dormakaba, обеспечивающие высочайший уровень безопасности объектов и достойный уровень комфорта, позволяющий сполна насладиться спортивным праздником. Вот только некоторые спортивные объекты на территории России и СНГ, на которых установлено оборудование dormakaba:

- спортивные объекты XXII зимних Олимпийских игр (Сочи, 2014 г.);
- БСА "Лужники", спорткомплекс "Олимпийский" (Москва);
- Центральный стадион (Екатеринбург);
- Ледовый дворец "Арена-Авангард" (Омск);
- Ледовый дворец спорта "Татнефть Арена" (Казань);
- высокогорный спортивный комплекс "Медео" (Алма-Ата)
- Дворец спорта "Казахстан", футбольный стадион "Астана-Арена" (Астана);
- НСК "Олимпийский" (Киев);
- стадион "Донбасс Арена" (Донецк).

У экспертов компании накоплен огромный опыт по оснащению спортивных объектов, которым они готовы поделиться с заказчиками строительства стадионов, архитекторами, проектными организациями и генеральными подрядчиками. ■

dormakaba

Адрес и телефоны
ООО "дормакаба Евразия"
см. стр. 151 "Ньюсмейкеры"

Платформы для интеграции систем безопасности на территориально распределенных объектах с филиальной структурой

Мнения экспертов

Интеграция систем безопасности на территориально распределенных объектах подразумевает объединение большого количества программно-технических инструментов на единой платформе для управления различными подсистемами в филиалах. Эксперты компаний "Октаграм", "Итриум СПб", "КРОК", "ААМ Системз", "Болид", Технологической платформы "Комплексная безопасность промышленности и энергетики", Bosch Security Systems и "АРМО-Системы" поделились профессиональным мнением о ключевых параметрах таких платформ, эффективном управлении единым информационным пространством и предложили рекомендации по их грамотному выбору

Какие ключевые свойства платформ вы бы выделили для интеграции систем безопасности на территориально распределенных объектах с филиальной структурой?

Николай Татарченко
Технический директор
ГК "Октаграм"

Глеб Рыбаков
Начальник отдела разработки программных средств
ООО "Итриум СПб"

Иван Царев
Руководитель направления слаботочных систем
компании "КРОК"

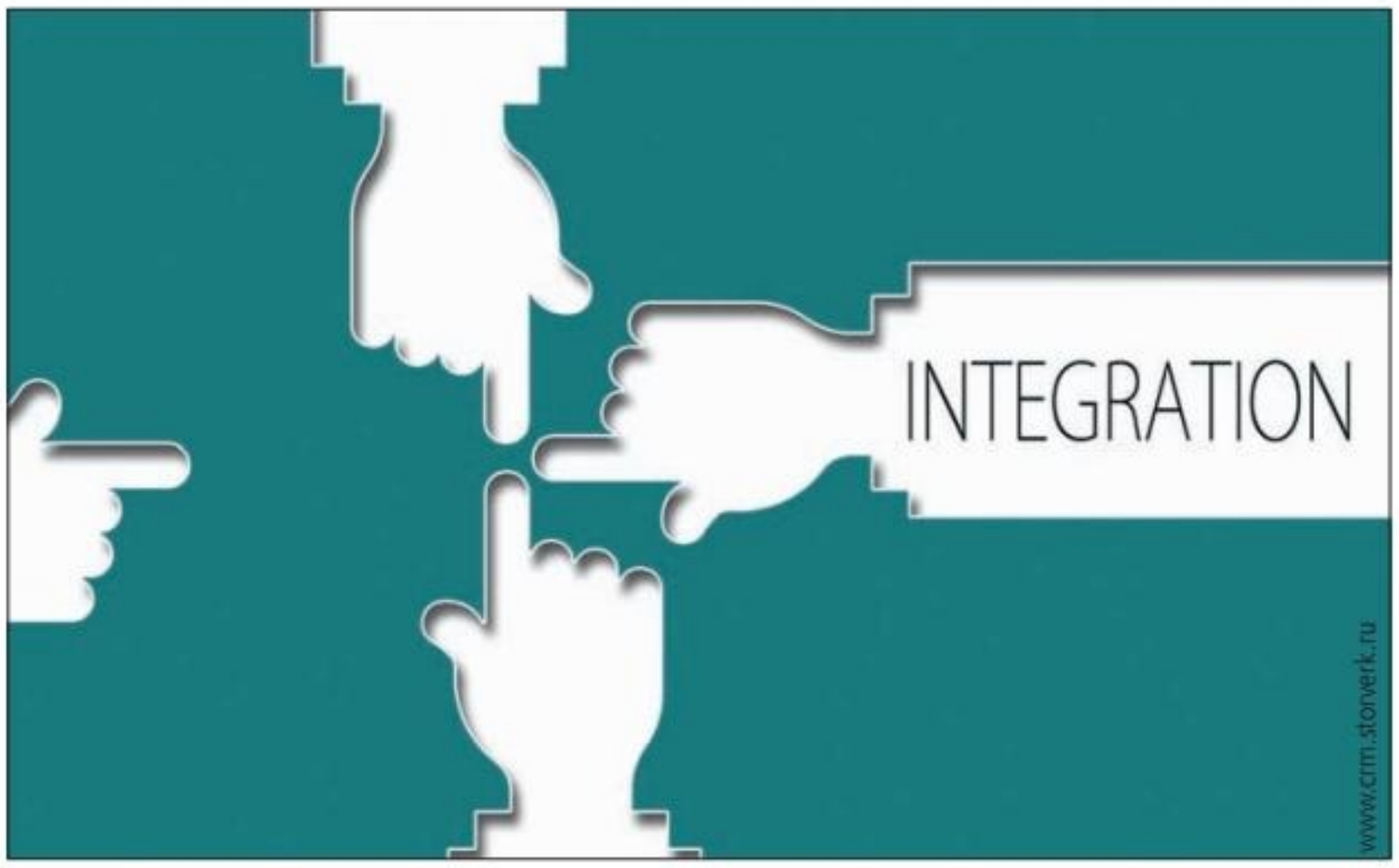
Марина Казарицкая
Руководитель проекта LyriX
компании "ААМ Системз"

Николай Татарченко:

1. Зрелость выбранной платформы, то есть количество различных готовых решений, реализованных на ее основе к моменту ее рассмотрения. Большее количество различных решений говорит о множестве функций платформы, об универсальности и гибкости. Чем более зрелая платформа, тем легче подобрать готовый набор и избежать переплаты за "нестандартные" функции или свести эту переплату к минимуму.
2. Легкость масштабирования. Если одно и то же оборудование подходит для небольших офисов и крупных филиалов, то это упрощает проектирование, облегчает логистику и монтаж.
3. Возможность составить "типовые монтажные наборы" для каждого типа офиса. Такой подход упрощает процесс монтажа, повышает его надежность и снижает сроки.
4. Мультивендорность системы. Если платформа позволяет подключать периферийное оборудование от разных производителей, то это снизит не только стоимость проекта, но и издержки на обслуживание. В будущем такую систему будет легче сменить или дополнить. Не секрет, что, например, при одном и том же качестве извещателей "протокольные" обходятся дороже аналогичных, выпускаемых компаниями, специализирующимися только на извещателях.
5. Однотипность и взаимозаменяемость оборудования, применяемого для разных задач. Снижается количество ЗИПа, повышается "живучесть" системы (при отсутствии ЗИПа возможно более важные модули системы отремонтировать путем замены их снятыми на том же объекте и менее критичными в данный момент). Однотипность оборудования и его простота снижают требования к персоналу на этапе монтажа и эксплуатации.

Глеб Рыбаков:

Эффективное объединение разрозненных территориально распределенных объектовых систем и средств безопасности в единую информационную систему – непростая задача. В филиалах, скорее всего, уже развернуты какие-то средства и системы, причем зачастую – совершенно разных моделей и производителей. Для многих интеграционных платформ на рынке реклама лукаво заявляет поддержку "всего и вся", но на практике такая интеграция оказывается поверхностной, ограниченной по возможностям, например, транслируются не все возможные события или отсутствует поддержка функций управления (только однонаправленное взаимодействие). Потому возможность глубокой, с сохранением максимума функциональных возможностей интеграции объектовых систем и средств в единое



Максим Горяченков
Руководитель отдела технической поддержки ЗАО НВП "Болид"

Алексей Марков
Заместитель председателя, ответственный за стратегическое развитие ТП "Комплексная безопасность промышленности и энергетики"

Дмитрий Пехов
Технический эксперт компании Bosch Security Systems

Вячеслав Петин
Директор Департамента технической поддержки ООО "АРМО-Системы"

информационное пространство напрямую определяет эффективность создаваемого интегрированного решения и степень контроля потребителя над конечной системой.

В интегрированной суперсистеме между филиалами будет циркулировать большой объем данных: события, пропуска, видео, метаданные. Таким образом, системы филиалов должны быть подключены к сети с высокой пропускной способностью и возможностью двустороннего информационного обмена, то есть к IP-сети. Географическая распределенность филиальной сети обычно обуславливает невозможность создания полностью своей сетевой инфраструктуры и, как следствие, ведет к необходимости использования общих проводных и беспроводных каналов и сетей, таких как сеть Интернет и сети сотовых операторов. В связи с этим интеграционная платформа должна не только выполнять эффективную маршрутизацию данных в такой гетерогенной сети, но также и обеспечивать необходимый уровень защиты информационного обмена с применением современных и/или сертифицированных алгоритмов и средств.

Необходимость использования ненадежных, неконтролируемых каналов между филиалами диктует несколько серьезных требований к интеграционной платформе. Во-первых, в отсутствие связи с "внешним миром" объектовая система должна сохранять свою работоспособность и продолжать функционировать автономно. Во-вторых, платформа должна гарантировать доставку данных (возможно, с задержкой на время потери связи), обеспечивать их целостность, разрешать коллизии в данных (при независимой модификации одних и тех же данных). Представим систему распределенного доступа, в которой два оператора в двух разных филиалах вносят изменения в права доступа одного и того же сотрудника. И в это время из-за аварии на магистрали отсутствует связь между филиалами. По тому, как поведет себя платформа по факту восстановления связи, каким образом и как быстро она "справится" с возникшей коллизией в данных, можно судить о ее эффективности.

В-третьих, платформа должна работать на IP-каналах любого качества сервисов, с гибкой адаптацией к пропускной способности и приоритизацией видов передаваемой информации. Наконец, обязательной является поддержка резервных и альтернативных типов каналов связи на случай сбоев.

Платформа должна обеспечивать прозрачный или облачный доступ ко всем данным в интегрированной системе. Пользователь не должен задумываться о том, на каком конкретно физическом сервере какого филиала хранится интересующая его информация. Если он хочет построить отчет по доступу сотрудника на все филиалы сети, то платформа должна автоматически агрегировать все необходимые данные с различных серверов, пользователю же интегрированная система должна представляться единым целым. Конечно, при этом платформа должна позволять администратору определить виртуальную структуру системы (которая может не совпадать с физической), разграничив права на доступ к разным частям единого информационного пространства.

И последнее, самое главное свойство – возможность организации единой системы управления инцидентами. Такую систему характеризуют:

1. Наличие карточки инцидента по каждому требующему внимания событию. Карточка инцидента должна увязывать в единый документ всю связанную с событием информа-

цию – от последних событий доступа в этой части объекта до отобранных оператором видеоматериалов. Карточка является основным документом для принятия решений, особенно для вышестоящих сотрудников из других филиалов.

2. Наличие типовых процедур обработки инцидентов, зависящих от типа возникшей ситуации и прочих данных. При обработке инцидента оператор следует типовой процедуре, что уменьшает вероятность ошибки и повышает контроль над процессом. При этом у администратора платформы должна быть возможность настройки и адаптации таких типовых процедур в соответствии со спецификой бизнес-процессов предприятия.

3. Возможность диспетчеризации карточек инцидентов между филиалами и кооперативной обработки инцидентов операторами из разных филиалов. При этом платформа должна обеспечивать операторов всеми необходимыми инструментами коммуникации, например такими, как голосовая связь (обычно VoIP).

Иван Царев:

У таких платформ можно выделить целый ряд ключевых свойств. Если начать с самого очевидного, то это поддержка многофилиальной структуры. Платформа должна не только развертываться на локальных объектах, но и собирать все филиалы в единый ситуационный центр, обеспечивая верхний уровень управления и контроля.

Для оперативного реагирования в случае нештатной ситуации платформа должна быстро справляться с обработкой большого количества поступающей информации. Из этого вытекает следующее свойство – наличие возможности приоритизации сигналов, трево и ошибок. Система должна распознавать, какую именно информацию нужно эскалировать в ситуационный центр, а какую необходимо оставить на локальном уровне. Кроме того, платформа должна иметь максимальный набор готовых интеграционных модулей с разными системами безопасности (системы контроля и управления доступом, тревожная и охранная сигнализации, видеонаблюдение и т.д.) наиболее распространенных производителей. Отдельно замечу, что решение, использующее различный состав вендоров на разных объектах, обязательно должно быть проработано. В противном случае его реализация может оказаться очень дорогой.

Если говорить о каких-то более формальных вещах, то здесь важно наличие сертификации и поддержки в России, в том числе с возможностью сервисного обслуживания компаниями-интеграторами.

Марина Казарицкая:

Надежность и масштабируемость. Не любая система, обеспечивающая надежность в масштабах малого объекта, "потянет" крупный холдинг с филиалами в десятках разных городов. Поэтому следует выбирать ту, которая уже зарекомендовала себя в соответствующей нише. Система также должна быть способна, следуя за развитием бизнеса, наращивать мощности: от малой системы до многофилиальной с территориально удаленными друг от друга объектами.

Максим Горяченков:

Можно выделить три большие задачи, которые решаются при построении единой системы безопасности распределенного предприятия.

Первая и самая очевидная – создание единого поста охраны, который бы обрабатывал все тревожные сообщения и управлял службами физической защиты объектов. Фактически это задача создания собственного ПЦО. Вторая тоже сводится к созданию системы мониторинга, однако не столько тревог, сколько неисправностей. В этом случае заказчик может значительно оптимизировать обслуживание систем безопасности и автоматики, если предприятие представляет собой сеть небольших и средних магазинов. Сюда же можно отнести мониторинг состояния камер видеонаблюдения и регистраторов, установленных в банкоматах. Функционал системы в данном случае будет развиваться в сторону учета и контроля фактов выезда обслуживающего персонала на объекты и своевременного устранения неисправностей.

Третья задача – интеграция системы безопасности и системы кадрового учета (ERP-системы управления предприятием). Такая интеграция дает возможность вести единую базу данных пользователей систем контроля доступа и охранной сигнализации, добавлять новые и редактировать существующие записи сотрудников сразу в нескольких локальных системах различных филиалов. При внедрении подобной системы ответственный работник центрального аппарата всегда сможет иметь доступ на любой удаленной объект организации. Горизонтальные связи между филиалами в части перемещения персонала будут строиться намного проще. Мониторинг же сведется к централизованному получению отчетов по учету рабочего времени и нарушениям трудовой дисциплины.

Таким образом, ключевое свойство локальных систем безопасности – максимальная открытость. Они должны не только иметь возможность передавать максимум данных о своем состоянии на верхний уровень и получать оттуда команды управления, но и изменять свою конфигурацию для решения третьей задачи.

Алексей Марков:

Ввиду того что интеграция в современном понимании – это не только стабильные и непрерывные каналы связи, но и возможность передачи сложных вычислений между сервисными приложениями, ключевыми свойствами интеграционных платформ являются:

- гибкое построение и управление логикой бизнес-процессов и отделение ее от логики работы пользовательских приложений;
- широкие возможности по визуализации и созданию приложений поверх существующей ИСБ с привязкой к конкретному объекту;
- использование передовых технологий, таких как облачные сервисы и машинное обучение, для уменьшения отвлекаемых у ИСБ ресурсов и стоимости.

Базовой технологией построения интеграционных платформ на текущем этапе развития является гибридная интеграция с привлечением облачных технологий. В случае профессиональной реализации это лучший способ оптимизировать существующие ресурсы ИСБ и обеспечить связность "всего и вся". После внедрения гибридная интеграционная платформа позволяет быстро и легко интегрировать приложения, данные и процессы, без пространственных ограничений.

Что это дает пользователю? В совокупности с широким функционалом визуализации предоставляется возможность идеальной настройки интерфейса от всех систем ИСБ филиальной сети на централизованных рабочих местах с дополнительной функцией машинного обучения интеграционного ядра и гибкой корректировки экранных форм в процессе повседневной работы системы и, как итог, удобство и эффективность применения при минимальных затратах.

Дмитрий Пехов:

Чтобы выделить ключевые свойства платформ, давайте сначала обратимся к наиболее частым вопросам, которые хотят решить заказчики при построении таких систем, порой инвестируя ради этого значительные средства:

- получение данных от существующих разнородных подсистем в унифицированном виде (принцип "единого окна") для увеличения эффективности их обработки и формирования более релевантной реакции;
- оптимизация скорости получения информации сотрудниками службы безопасности для принятия оперативных решений;
- возможность комплексного расследования инцидентов и создания связанных отчетов;
- увеличение уровня защищенности объектов благодаря параллельной совместной работе нескольких подсистем;
- централизация информационных активов для обеспечения доступности и целостности полученных данных;
- защита от локальной компрометации данных в филиалах;
- упрощение мониторинга и администрирования различных подсистем для уменьшения рисков отказа оборудования и снижения расходов на обслуживание;
- создание автоматических шаблонов поведения системы при нештатных ситуациях в зависимости от данных, получаемых от различных подсистем.

В современном мире начинают размываться границы между ИСБ, ССОИ, SCADA, PSIM и BMS. Кроме того, все больший акцент делается на синергию Information и Physical Security, безусловными драйверами данной философии выступают крупные ИТ-интеграторы, которые имеют достаточно ресурсов и компетенций для внедрения подобных комплексных решения Enterprise-класса.

Параллельно с этим передовые технологии, которыми мы уже привыкли активно пользоваться в повседневной жизни, набирают популярность и в промышленных решениях, связанных с безопасностью. Например, серьезным импульсом для применения систем распознавания лиц в рамках крупных распределенных объектов стала популяризация данной технологии в смартфонах.

Все это ложится в основу тех требований, которые сегодня предъявляются к платформам для территориально распределенных объектов с филиальной структурой. Основываясь на нашем многолетнем опыте построения систем безопасности для корпоративных заказчиков в России и СНГ, мы можем сделать заключение, что для интеграционной платформы основными сегодня являются следующие свойства:

- поддержка принципа иерархичности серверов (возможность создания серверов локального (регионального) уровня и центральных серверов);
- возможность распределения нагрузки между управляющими серверами, серверами баз данных и коммуникационными серверами;
- поддержка программным обеспечением верхнего уровня большого количества стандартных протоколов для подключения сторонних продуктов;
- эргономичность интерфейса ПО и легкая масштабируемость;
- наличие гибкой системы разграничения прав пользователей и полностью кастомизируемый для каждого оператора интерфейс;
- отказоустойчивость. Поддержка ПО верхнего уровня механизмов кластеризации и виртуализации;
- возможность настройки маршрутизации событий между локальными операторами с поддержкой уведомления ключевых лиц об их бездействии;
- полная совместимость всех программных компонентов (серверное ПО, шлюзы, конфигурационные утилиты) системы между собой и с актуальными версиями и обновлениями СУБД и ОС;
- модульная, легко масштабируемая архитектура аппаратной базы;
- универсальность контроллеров. Возможность организации на базе системы управления доступом также системы охранного мониторинга. Например, для участков объекта, которые не требуют использования профессиональных пультов управления СОТС, построение мониторинга на базе расширителей входов контроллера СКУД может быть идеальным решением, которое позволит существенно сэкономить бюджет заказчика;
- скорость передачи, обработки и отображения данных, получаемых ядром ПО от контроллеров;
- высокая надежность аппаратных компонентов. Территориально распределенные объекты в большинстве случаев подразумевают наличие труднодоступных участков. К тому же периоды регламентного обслуживания напрямую влияют на стоимость владения системой;
- шифрование каналов связи между контроллерами и серверным ПО надежными криптоалгоритмами. Например, связь между контроллерами Bosch AMC2 и программным компонентом защищена с помощью шифрования AES-256 и динамического обмена сеансовыми ключами. Такой подход эффективно предотвращает атаки "человек-посередине" и подмену данных.

На наш взгляд, в силу большого количества нюансов, связанных со стандартизацией в области протоколов обмена данными в системах безопасности, до сих пор преимущество на стороне тех производителей, которые имеют ресурсы не только разрабатывать и поддерживать программные продукты для интеграции, но и могут предложить заказчику полный набор аппаратных компонентов и дополнительных сервисов.

Вячеслав Петин:

Одно из ключевых свойств любой платформы для ИСБ – это возможность интеграции всех систем безопасности: СКУД, ОПС, ТСН. Кроме того, к современным ИСБ зачастую предъявляется требование интеграции и с системами автоматизации зданий, такими как вентиляция, кондиционирование, отопление, освещение и др.

Считаю особо важным, чтобы распределенная ИСБ имела мультисерверную архитектуру, потому что в этом случае каждый объект клиента может работать автономно и независимо от центрального сервера при потере связи с ним. При этом системой будет управлять региональный сервер на локальном объекте, все рабочие станции сохранят работоспособность, в обычном режиме будет выполняться мониторинг и выдача пропусков. Когда связь с центром будет восстановлена, БД регионального сервера реплицируется с БД центрального.

Я бы выделил также как необходимое свойство для ИСБ ее масштабируемость, поскольку клиент должен иметь возможность подключить к уже существующей системе свои новые подразделения.

Кроме того, в рамках ИСБ должна быть реализована единая интегрированная база данных и параллельное лицензирование в отношении клиентских станций, то есть лицензия привязывается к учетной записи, а не к конкретной машине.

Поскольку крупные распределенные системы создаются для больших корпораций с региональными офисами в разных странах, ИСБ должна поддерживать мультиязычность и одновременную работу в нескольких часовых поясах.

Отмечу, что основные современные платформы для интегрированных систем безопасности (Bosch, Honeywell, Lenel) могут обслуживать неограниченное число пользователей, входов/выходов и периферийных устройств, а также имеют широкий набор инструментов для интеграции со сторонним оборудованием и ПО, при этом каждая из этих систем уже имеет огромный набор готовых интеграций.

Хочу отметить еще одно важное свойство современной ИСБ – это полноценное резервирование серверов БД системы, когда при выходе из строя какого-либо из них система продолжает полноценно функционировать.

МОСКВА, ВДНХ, ПАВИЛЬОН № 75
23–26 ОКТЯБРЯ 2018

XXII МЕЖДУНАРОДНАЯ ВЫСТАВКА

INTERPOLITEX

СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

WWW.INTERPOLITEX.RU

ОРГАНИЗАТОРЫ

МВД РОССИИ

ФСБ РОССИИ

РОСГВАРДИЯ

ОРГАНИЗАТОР ВЫСТАВКИ «ГРАНИЦА»

ПС ФСБ РОССИИ

ЭКСПОНЕНТ-КООРДИНАТОР ОТ МВД РОСИИ

ФКУ «НПО «СТИС» МВД РОССИИ

ГЕНЕРАЛЬНЫЙ УСТРОИТЕЛЬ

ЗАО «ОВК «БИЗОН»

Как эффективно структурировать единое информационное пространство территориально распределенного объекта и как им потом управлять?

Николай Татарченко:

Возможны:

1. Сеть с единым центром мониторинга и управления.
2. Сеть с распределенной цепочкой региональных узлов мониторинга и управления.
3. Полностью распределенная сеть с репликацией (частичной) данных.

Такие структуры имеют разные показатели "надежность/цена". Выбор структуры зависит от минимального необходимого уровня надежности комплекса, наличия кадров в каждом регионе и бюджета проекта.

Управлять этой структурой нужно исходя из выбранного варианта ее организации и наличия кадров в каждом регионе. При использовании аутсорсинга для этих целей необходимо учитывать, наряду с квалификацией персонала, опытом работы, наличием соответствующих сертификатов и разрешений, значимость данного проекта для подрядчика. В любых условиях эксплуатации наличие многоранговой системы оповещения о нештатной работе системы является обязательным условием успешного функционирования объектов.

Глеб Рыбаков:

Выбор структуры, которая будет эффективна в каждом конкретном случае, напрямую зависит от специфики объектов, решаемых задач, выполняемых в организации процессов и требований заказчика.

В общем случае мы рекомендуем сохранять достаточную автономность объектовых систем, оставляя их владельцами своих данных и конфигураций. Это позволит сохранить работоспособность системы филиала при отсутствии связи с "внешним миром". Взаимодействие филиалов и подключение их к центральной части должно осуществляться по стандартизованным, открытым протоколам (вроде ONVIF) на принципах равноправного двунаправленного обмена данным. Части интегрированной системы должны периодически обновлять сведения (данные, конфигурацию) от других филиалов. Таким образом, несмотря на то что каждая филиальная система администрируется независимо, благодаря единым "правилам игры" сохраняется целостность и актуальность информации в едином пространстве.

В части вопроса управления задачу следует рассматривать в контексте и с увязкой с задачами управления всей информационной инфраструктурой предприятия, вовлекая соответствующие ИТ-ресурсы и структурные подразделения предприятия.

Иван Царев:

Чтобы эффективно организовать единое информационное пространство территориально распределенного объекта, необходимо правильно выстроить как кадровую, так и аппаратно-техническую структуры. Распределение должностных обязанностей происходит на основании созданной модели угроз. Она представляет собой целый перечень возможных негативных событий, которые варьируются в зависимости от таких факторов, как назначение объекта, его местоположение и т.д. В итоге выстраивается организационная система, в которой четко установлено, кто, на каком уровне и за что отвечает. То есть, другими словами, обуславливаются зоны ответственности конкретного филиала, вышестоящего объекта, ситуационного центра системы. Затем, уже на локальных уровнях, происходит распределение ролей сотрудников на той или иной позиции и, соответственно, определяется информация, которая необходима каждой роли для принятия решения.

Если говорить об аппаратно-технической структуре, то на каждом локальном объекте нужно организовать отдельное диспетчерское место и отдельный диспетчерский центр. В этот диспетчерский центр должен сводиться максимум информации о подохранном объекте – от систем контроля и управления доступом до системы охранного видеонаблюдения, которая может быть построена в том числе на основе аналитики. Далее в этой структуре выделяются основные сигналы, которые в дальнейшем транслируются в единый ситуационный центр распределенных объектов. Его расположение заказчик выбирает на свое усмотрение. Зачастую важным критерием является равноудаленность остальных объектов от этого центра.

Таким образом, информационное пространство должно учитывать логику деления ролей, логику распределения оборудования и градацию ситуации. Должно быть четко определено, какие угрозы безопасности можно решить на локальном, местном уровне своими силами, а какие необходимо эскалировать дальше, например на региональный или федеральный уровни.

Марина Казарицкая:

Важнейшая функция любой платформы для крупной ИСБ – предоставление статистики для принятия верных управляющих решений руководством во всех звеньях компании. Подразумеваем прежде всего богатые возможности различных отчетов: по событиям, по сообщениям, по учету рабочего времени, списки людей на территориях и др.

Марина Казарицкая:

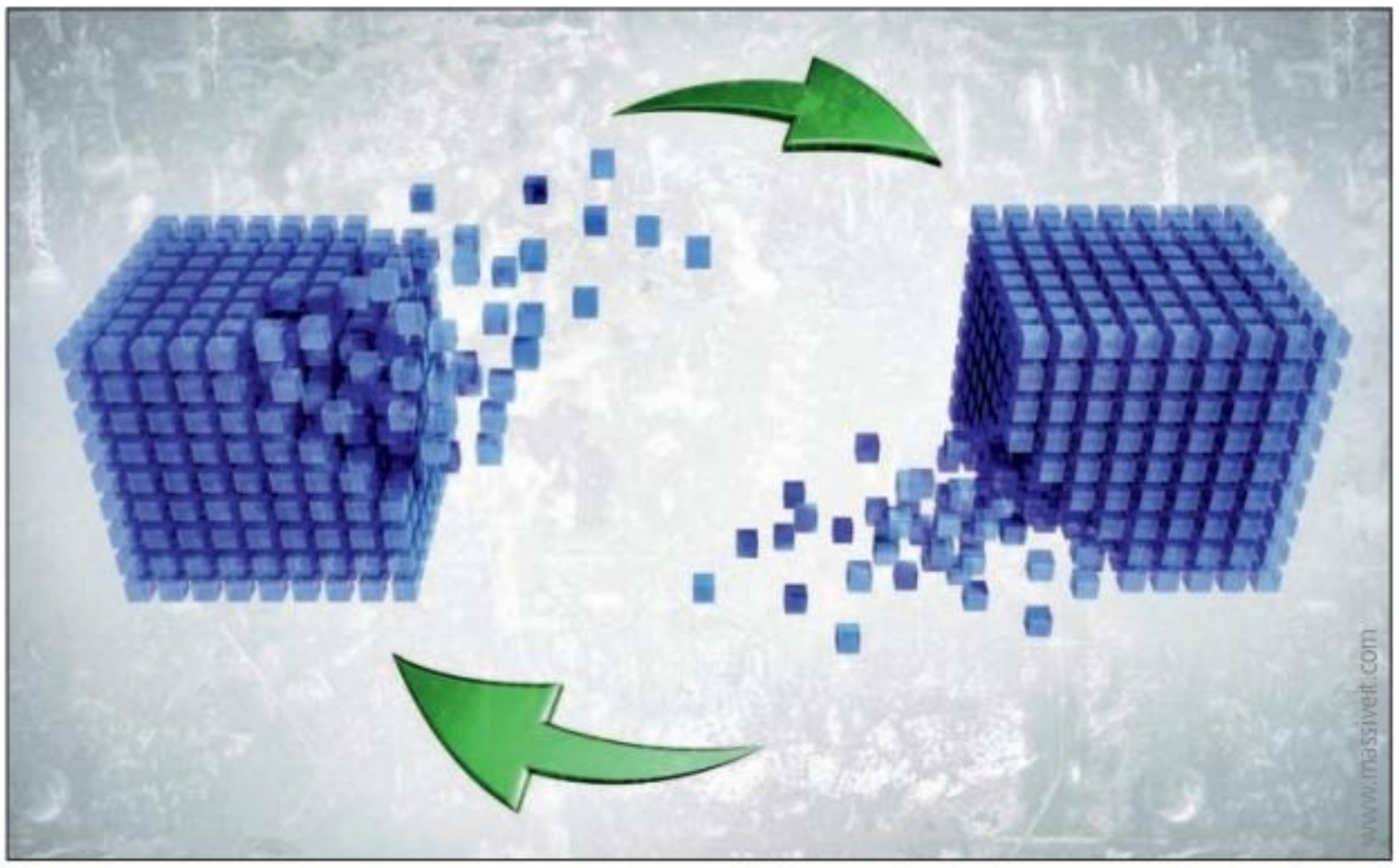
Информационное пространство ИСБ состоит из:

1) кадровой информации;
2) информации о событиях системы;
3) информации о состоянии оборудования различных подсистем.

Необходимо обеспечить актуальность и надежность передачи различных видов информации между территориально удаленными друг от друга филиалами, а также возможность удаленного управления подсистемами.

Для эффективного управления территориально распределенным объектом также необходимы механизмы, позволяющие как оперативно реагировать на ситуацию в реальном времени, так и проводить ее анализ для принятия стратегических решений. Можно сказать, что важнейшая функция любой платформы для крупной ИСБ – предоставление статистики для принятия верных управляющих решений руководством во всех звеньях компании. Подразумеваем прежде всего богатые возможности различных отчетов: по событиям, по сообщениям, по учету рабочего времени, списки людей на территориях и др.

Максим Горяченков:
При создании ПЦН для сотен и тысяч объектов зачастую бывает целесообразно организовывать 3-звенную архитектуру. В этом случае второй региональный уровень, контролирующий объекты одной области или макрорегиона, будет заниматься непосредственным управлением локальными службами безопасности с получением большинства событий с объектов. А ситуационный центр самого верхнего уровня получает только информацию об инцидентах в критически важных зонах (например, кассовые узлы и т.д.) и общую статистику о количестве неисправностей и тревог, причинах их возникновения, способах и сроках решения. Подобный подход обусловлен невозможностью "переварить" одним ситуационным центром огромное количество поступающих с объектов событий.
При решении второй и третьей задач большого смысла организовывать трехзвенную структуру нет. Главная причина – отсутствие необходимости обработки массы поступающих данных в реальном времени, ибо задачи по мониторингу в большей степени сводятся к аналитике и формированию различных отчетов.



Дмитрий Пехов:
В современном мире, когда общество становится все более информационным, интегрированная система безопасности компании уже не может эффективно работать в изоляции от других служб и информационных активов. Ее структура должна так же органично вписываться в общую ИТ-парадигму заказчика, как и остальные компоненты

Алексей Марков:
Наиболее широко применяемой в крупных территориально распределенных компаниях является 3-уровневая структура информационного пространства ИСБ:
- информация для руководства компании;
- информация для центральной диспетчерской службы;
- информация для служб безопасности объектов.

Она хорошо себя зарекомендовала в связи с высокой эффективностью дежурного контроля и мониторинга объектов, но практика показала, что в случае ЧС ключевые решения принимались "на местах", хотя и не всегда правильно. Большие перспективы сулит развитие Интернета вещей, который может взять на себя часть рутинных дежурных функций, при этом сдерживающим фактором выступает высокий уровень ответственности принимаемых по первичным данным ИСБ-решений. Готовы ли мы сделать этот процесс полностью автоматическим, пока до конца не ясно.
Поэтому в настоящее время оптимальным видится построение единого информационного пространства, позволяющего на базе облачных сервисов оперативно предоставлять пользователю любую запрашиваемую информацию, а также делать требуемые расчеты в пределах разрешенного ему подсистемой аутентификации доступа к данным и ресурсам (индивидуальное ранжирование).
В этом случае большое внимание следует уделять вопросу надежности и безопасности аутентификации пользователей для работы в системе, так как любая интеграционная платформа обладает возможностью контролировать, а также модифицировать и управлять работой всех интегрированных в ней ИСБ филиальной сети. Конечно же, во всех платформах предусмотрены системы ограничения доступа и разграничения полномочий, но гораздо надежнее попросту не допускать к работе с ИСБ нежелательных сотрудников и нарушителей, а у пользователей формировать ответственное отношение к работе с ИСБ.

Дмитрий Пехов:
Важно понимать, что единое информационное пространство объекта с сетью филиалов представляет собой не только совокупность ИТ-ресурсов и программно-технических средств, например серверов управления, баз данных, сетевых контроллеров и т.д., но также организационных структур, которые регулируют все информационные процессы, и организационно-нормативных документов. Вся система должна функционировать на базе единых принципов и по общим правилам.
В современном мире, когда общество становится все более информационным, интегрированная система безопасности компании уже не может эффективно работать в изоляции от других служб и информационных активов. Ее структура должна так же органично вписываться в общую ИТ-парадигму заказчика, как и остальные компоненты. При построении системы безопасности на распределенных объектах, как правило, используется принцип иерархичности, когда на уровне филиалов остаются механизмы оперативного контроля и администрирования, а центральный офис отвечает за систематизацию данных и общее управление.
Приведем несколько практических примеров такого подхода: небольшие филиалы, которые не подразумевают необходимость локального мониторинга службой безопасности, оснащаются только пожарной сигнализацией, системой оповещения, универсальными сетевыми контроллерами СКУД/СОТС и небольшими видеорегистраторами, обычно со встроенными PoE-коммутаторами. Мониторинг, управление и администрирование осуществляются из центрального офиса. При этом, когда канал связи с головным офисом практически не используется, осуществляется копирование видеоархива в СХД центрального офиса для долговременного хранения.
Крупные филиалы имеют свои локальные коммуникационные серверы и серверы баз данных регионального уровня для обеспечения автономной работы филиала при отсутствии связи с центральным сервером. Кроме этого, структура с локальными базами данных позволяет гибко настраивать передачу в центральную БД только событий с высоким уровнем приоритета, снижая при этом нагрузку на центральный сервер. Разделенные базы данных также могут быть настроены на работу только с конкретными подсистемами (АПС, СКУД, СОТС и т.д.), позволяя оптимально спланировать разделение ИТ-ресурсов.

Вячеслав Петин:
Для структурирования единого информационного пространства в современных ИСБ применяется сегментирование базы данных (мультисерверная архитектура), причем каждый сегмент – это отдельная региональная база данных, которая может работать автономно, а сегментирование может быть многоуровневым. Необходимое условие эффективной работы такой структуры – это синхронизация данных между множеством сегментов.
Благодаря такой архитектуре сотрудники службы безопасности и ИТ-менеджеры могут централизованно управлять всей интегрированной системой, но при этом каждое региональное отделение компании сохраняет возможность автономного контроля над своей подсистемой.

В каком случае интеграционная платформа обеспечивает максимально широкий перечень запросов заказчика?

Николай Татарченко:
Если платформа соединяет в себе зрелость с возможностью работы с периферийными устройствами различных вендоров, то она обеспечивает максимально широкий перечень запросов заказчика. Мультивендорность позволяет не только удовлетворить запросы заказчика, но и подобрать оборудование на любой вкус, обеспечить для него лучшее соотношение цены/качества.

Глеб Рыбаков:
Во-первых, интеграционная платформа должна быть исходно спроектирована и создана для комплексного решения задач безопасности – и видеонаблюдения, и контроля и управления доступом, и охранной сигнализации, и т.д. Выбор продукта, изначально специализированного в какой-то конкретной области, например видеонаблюдении (а именно таких продуктов на рынке большинство), существенно ограничивает заказчика в эксплуатационных возможностях создаваемого решения.
Во-вторых, платформа должна обеспечивать глубокую интеграцию широкого набора систем и средств с поддержкой максимума их функциональных возможностей. На практике многие продукты на рынке могут получить от интегрируемых средств только часть информации, не поддерживают управление такими средствами и т.д. Кроме того, платформа должна обеспечивать возможность интеграции со смежными системами, такими как системы автоматизации зданий и др. Только тогда на базе платформы можно будет автоматизировать действительно комплексные бизнес-процессы. Для обеспечения таких богатых интеграционных возможностей платформа должна реализовывать широкий набор стандартных протоколов и спецификаций – OPC, ONVIF и др.
Поддержка стандартов, модульная структура платформы, гибкая архитектура и наличие элементов "конструктора" (с возможностью конструировать из компонентов платформы различные конфигурации и автоматизировать работу с помощью скриптов поведения) делают решения на базе платформы устойчивыми к новым вызовам, изменениям со временем требований и бизнес-процессов.
Наконец, платформа должна позволять эффективно (в том числе по экономическим метрикам) решать задачи различного масштаба. Например, бизнес может со временем расти: на раннем этапе заказчик не хочет делать большие вложения в платформу, а на более поздних от платформы потребуется способность эффективно масштабироваться в соответствии с ростом бизнеса.

Иван Царев:
Интеграционная платформа обеспечивает максимально широкий перечень запросов в том случае, когда заказчик понимает, что он хочет получить в итоге, то есть точно ставит задачи и определяет необходимый функционал для интегрированной платформы систем безопасности. Наиболее эффективным решением является привлечение специалистов еще на этапе проработки вопросов внедрения интеграционной платформы. При таком подходе уже на этапе проектирования можно понять реальный спектр задач и возможные способы их реализации. Исходя из опыта многочисленных комплексных проектов, отмечу, что оптимальный выход – выбор одной компании, которая привлечет всех необходимых специалистов, разработает модель угроз, проведет анализ бизнес-процессов. Последнее необходимо для того, чтобы понять, какие из них могут быть оптимизированы с помощью внедрения интеграционной платформы и каким образом. Затем на основании проведенного аудита разработает техническое задание и согласно ему выполнит все необходимые работы по обеспечению безопасности территориального объекта и его интеграции в единый ситуационный центр средствами интеграционной платформы.

Марина Казарицкая:
Лучше отдать предпочтение той платформе, которая с наименьшими затратами позволит при необходимости масштабировать ИСБ, а также интегрировать новые виды оборудования, добавлять в систему новые логические модули. Важным плюсом может быть широкий перечень уже поддерживаемого оборудования, готовность поддержать новые типы и модификации устройств, а также возможность заказной разработки аппаратных и функциональных драйверов.

Максим Горяченков:
Можно попробовать представить себе универсальную интеграционную платформу, решающую все три описанные в п. 1 задачи. Однако почти сразу становится понятно, что возможность создания такой платформы – утопия. Главная проблема будет лежать не в технической, но организационной плоскости. Задачи относятся к компетенции различных структур и служб заказчика, редко глубоко связанных между собой на горизонтальном уровне. Только решения первой и второй задач могут как-то сочетаться. При этом вторая задача будет зачастую решаться на самом верхнем уровне такой системы.

Алексей Марков:
Вначале необходимо отметить, что переход к широкому применению интеграционных платформ был в первую очередь связан с острой необходимостью преодоления информационного разрыва между бизнес-подразделениями и ИТ-отделами компаний, который не давал возможности широкого внедрения интеграционных механизмов во всех сферах.
Сегодня в связи с бурным ростом вычислительных возможностей и применением их при создании ИСБ объектов происходит непрерывное усложнение процессов взаимодействия ИСБ объектов филиальной сети, однако именно это делает возможным реализацию качественно нового этапа развития интеграционных платформ в сторону применения машинного обучения и облачных сервисов.
Таким образом, масштабное усложнение самой интеграционной платформы должно привести к упрощению взаимодействия пользователей с интерфейсом системы и одновременному расширению функциональных возможностей ИСБ.

Дмитрий Пехов:
В случае, когда архитектура платформы может быть полностью адаптирована под ИТ-структуру клиента, при этом позволяя взаимодействовать с полным спектром технических средств безопасности и, кроме этого, имея возможности гибко взаимодействовать с системами верхнего уровня, например с ERP-системами.
Интеграционная система должна предоставлять заказчику все необходимое, чтобы обеспечить на разнородных объектах высокий уровень защищенности, оптимизировать управление всей системой, получить единый интерфейс для оперативного реагирования на нештатные ситуации. Именно такой подход к созданию единого аппаратно-программного комплекса позволяет системе эффективно и эргономично функционировать как единый организм.
Правильно выбранная платформа надежно защищена от компрометации и внутреннего саботажа. Как мы знаем, зачастую именно территориально распределенные объекты предъявляют повышенные требования к функционалу системы, будь то интеграция периметральной охраны, систем сканирования днищ автомобилей или получение информации о состоянии вентиляционных установок.
Платформа должна одинаково успешно работать как в условиях небольшого офиса, так и в условиях ситуационного и мониторингового центра вплоть до системы класса "Безопасный город". Важно помнить, что каждый объект имеет свой класс защиты в зависимости от модели угроз и возможных последствий, но все объекты холдинга должны быть защищены надежной безотказной системой, которая отвечает самым жестким корпоративным стандартам.

Вячеслав Петин:
Во-первых, я считаю, что для максимального удовлетворения потребностей клиента все его запросы необходимо отразить в техническом задании, а затем тщательно спланировать и спроектировать комплексную систему.
Во-вторых, со временем потребности заказчика могут измениться, поэтому предпочтение следует отдавать гибким ИСБ с возможностью наращивания функционала, например за счет приобретения дополнительных лицензий.
В-третьих, я бы отметил, что, кроме базовых возможностей, для кастомизации и расширения круга решаемых задач система должна иметь набор уже готовых интеграций со сторонним оборудованием и ПО. Такие интеграции помогут решить задачи, возникающие в ходе реализации и эксплуатации системы.

ОРГАНИЗАТОР

МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ARMY

МЕЖДУНАРОДНЫЙ ВОЕННО-ТЕХНИЧЕСКИЙ ФОРУМ «АРМИЯ-2018»

21–26 АВГУСТА
ПАТРИОТ ЭКСПО

WWW.RUSARMYEXPO.RU

ВЫСТАВОЧНЫЙ ОПЕРАТОР

МКВ

МЕЖДУНАРОДНЫЕ КОНГРЕССЫ И ВЫСТАВКИ

Генеральный партнер

ВЕРТОЛЕТЫ РОССИИ

Генеральный спонсор

РОСОБОРОНЭКСПОРТ

Официальный партнер

Концерн ВКО
Алмаз - Антей

Часто заказчику требуется разработка узкоспециализированного решения – некоего дополнительного функционала для платформы ИСБ, который вряд ли будет широко использован другими клиентами. Подобная работа стоит очень дорого. Какие альтернативные пути решения этого вопроса вы предлагаете заказчику в таком случае?

Николай Татарченко:
Альтернативой всегда являются ближайшие стандартные решения. Очень важно, чтобы продающие специалисты их знали. Счет стандартных решений, проверенных на практике в зрелой системе, идет не на десятки, а на сотни. Неплохая альтернатива разработке узкоспециализиронного решения (когда приходится создавать "железо" и софт) – использование настоящей платформы, то есть одного "железа" для решения разных задач. При этом в случае необходимости дополняются/исправляются только микропрограммы, программы или просто пишутся скрипты. В таком случае снижается стоимость разработки (в два и более раза), увеличивается надежность системы и снижаются сроки реализации проекта. Такой подход есть не у всех, однако количество правильных платформ растет. Их предлагают, например, "Семь печатей", Octagram, Appolo и др.

Глеб Рыбаков:
В такой ситуации мы вместе с заказчиком изучаем возникшую потребность, предпосылки и специфику задачи. На самом деле уникальных потребностей почти не бывает. Но понять, какая исходная проблема скрывается за узкоспециализированным запросом, бывает очень трудно. В процессе тесного взаимодействия с заказчиком чаще всего удается найти решение, не требующее специализированной разработки.
Для обеспечения быстрой и гибкой адаптации наших продуктов к требованиям заказчика мы реализуем в них принцип "конструктора": поведение или состав большей части платформы можно изменить с помощью скриптов-сценариев, шаблонов и ресурсов, для создания которых не требуется специальной квалификации. С одной стороны, специалисты заказчика могут внести соответствующие изменения самостоятельно. С другой – при заказе таких работ у нас их себестоимость (и, соответственно, стоимость для заказчика) оказывается значительно ниже.

Иван Царев:
На мой взгляд, здесь все обстоит с точностью до наоборот. На рынке в принципе не существует таких готовых универсальных интеграционных платформ, которые устроили бы любого заказчика. Для максимально эффективного использования системы, напротив, нужно дорабатывать базовый функционал под конкретные задачи конкретного заказчика. На это как раз будут влиять составленная модель угроз, требования по безопасности для определенных бизнес-процессов.
Кроме того, мне кажется, неверно говорить о дороговизне внедрения дополнительного функционала. На фоне стоимости внедрения интеграционной платформы для территориально распределенного многофилиального объекта стоимость адаптации под конкретные требования (если речь не идет о полном изменении конфигурации этой самой интеграционной платформы) не будет существенной.

Марина Казарицкая:
Используемая платформа должна быть открыта для интеграции, иметь доступный и качественный SDK для интеграции с каким-либо оборудованием или программными средствами силами сторонних разработчиков.
Платформа должна обладать богатыми возможностями автоматизации, позволяющими настроить связь между самыми разными (не только базовыми, но и сторонними) подсистемами.

Максим Горяченков:
Чудес не бывает. Любая серьезная интеграционная платформа для мониторинга большого количества распределенных объектов фактически создается индивидуально под конкретного заказчика, часто с привлечением к процессу его собственных ресурсов по разработке ПО. В качестве основы могут браться готовые продукты. Но обычно это бывают решения, позволяющие получать данные от систем различных производителей и выдавать их наверх в некоем унифицированном виде. Пользовательский интерфейс, отчеты и т.д. чаще создаются с нуля или сильно перестраиваются под существующие и работающие бизнес-процессы соответствующих служб заказчика.

Алексей Марков:
По моему мнению, внедрение современной ИСБ – это всегда разработка индивидуального (узкоспециализированного) решения даже для небольших, казалось бы, объектов.
В связи с этим выбор функционала ИСБ, который будет реализован, стоит перед заказчиком всегда, и это необязательно разработка чего-то дополнительного. В ряде случаев принимается решение о сокращении и уменьшении числа решаемых ИСБ задач для оптимизации работы системы безопасности и ее стоимости.
Если же заказчик требует от ИСБ выполнения специфических или "нестандартных" функций, то проводится анализ причин, которые формируют у заказчика такую позицию, затем в процессе дискуссии выбирается оптимальное решение и на этой основе корректируется функционал внедряемой ИСБ, при этом сначала предлагаются такие технические решения, где эти функции уже реализованы, с приоритетным использованием оборудования и программных комплексов вендоров из состава существующей ИСБ.
При необходимости разработки дополнительного функционала для платформы ИСБ заказчику предлагаются такие аппаратно-программные решения, которые содержат стандартные средства разработки, встроенные в ядро информационной платформы. Таким образом, стоимость этих работ для заказчика определяется стоимостью привлечения соответствующих специалистов или обучения собственных.

Дмитрий Пехов:
Прежде всего мы предлагаем нашим заказчикам использовать мощный механизм стандартизированных протоколов, например OPC и Onvif.
В случаях, когда средств стандартных протоколов недостаточно, используются SDK и API. Новый BIS Client SDK, который базируется на фреймворке WCF, предназначен в первую очередь именно для разработчиков, если требуется подключить программную платформу BIS к стороннему ПО или создать собственный BIS GUI.
Для обеспечения всесторонней поддержки партнеров в сложных проектах в Bosch Security создано особое подразделение инженерных решений (Engineered Solutions Business), которое помогает системным интеграторам эффективно решать нетиповые задачи от момента проектирования до этапа пусконаладки, обеспечивая максимальный уровень адаптации платформы под задачи конкретного клиента.

Вячеслав Петин:
Когда решается задача подобного рода, то первое, что, на мой взгляд, надо сделать, – это проанализировать интеграции, которые уже существуют для выбранной платформы ИСБ, возможно, среди них найдется решение под конкретные требования заказчика. Если таким способом не удается полностью реализовать необходимый функционал, то можно пойти путем модификации готовых интеграций и добиться соответствия системы поставленным задачам.
Кроме того, можно предоставить заказчику SDK или API для самостоятельной доработки системы, во многих случаях это обойдется дешевле, чем заказ реализации дополнительного функционала у стороннего исполнителя.

На что еще надо обратить внимание при выборе платформы крупной распределенной ИСБ с многофилиальной структурой?

Николай Татарченко:
Дополнительно к указанному в п. 1:
1. Существующую в филиалах профильную инфраструктуру (в связи с возможным использованием/заменой существующего оборудования).
2. Сложность оборудования и ПО. Стабильность/доступность вендора. Качество логистической, обучающей и сервисной структур вендора.
3. Предпочтения и знания персонала объектов.

Глеб Рыбаков:
В первую очередь следует ознакомиться с портфолио и реальным опытом (историями успеха) компании – производителя интеграционной платформы. Бывает так, что компания А громко заявляет о себе, участвует в выставках, "давит" маркетингом, но на практике оказывается, что на реальных объектах выбирают и устанавливают продукты компании Б, которая просто "хорошо делает свое дело".
Во-вторых, мы рекомендуем выбирать поставщика, который не только обеспечивает в своей платформе интеграцию широкого набора сторонних систем, но также предоставляет полный набор функциональных средств (СКУД, ОТС, ОПС, видеорегистраторов и др.) собственного производства. С одной стороны, это хорошо характеризует практические компетенции компании в соответствующих областях. С другой – выбор решения одного поставщика при прочих равных позволяет снизить как начальную стоимость системы, так и совокупную стоимость владения впоследствии.

Иван Царев:
Важно выбрать такую платформу, которая была бы открыта для масштабирования, добавления дополнительного функционала. Например, если заказчик планирует дальнейшее развитие предприятия, нужно понимать, что количество филиалов будет только увеличиваться. Таким образом, ему будет необходимо иметь возможность без особого труда добавлять объекты (без необходимости полной замены существующей инфраструктуры), наращивать как локальные системы, так и систему ситуационного центра. Если же заказчик не планирует расширение сети, то ему все равно необходимо понимать, что технологии меняются. В настоящее время активно происходит цифровая трансформация бизнеса, что позволяет решать новые дополнительные задачи и касается в том числе систем безопасности. Постоянно внедряются новые технологии, набирают обороты биометрия, видеоаналитика, появляются доступные системы позиционирования персонала, учета и контроля за перемещением материальных ценностей. Все это также может являться составным компонентом интеграционной платформы систем безопасности и эффективно решать широкий спектр бизнес-задач.

Марина Казарицкая:
Надо обратить внимание на надежность и мощность аппаратной части. Мощная программная платформа со слабеньким и ненадежным оборудованием – это колосс на глиняных ногах.

Максим Горяченков:
Немаловажным фактором в выборе базовой программной платформы для создания крупной распределенной системы мониторинга будет являться наличие у нее сертификатов соответствия различным требованиям по защите персональных данных пользователей, хранения ДСП и секретных данных (ФСТЭК), соответствия ведомственным и внутрикорпоративным нормативным документам

www.secuteck.ru февраль – март 2018

Иван Царев:
Важно выбрать такую платформу, которая была бы открыта для масштабирования, добавления дополнительного функционала. Например, если заказчик планирует дальнейшее развитие предприятия, нужно понимать, что количество филиалов будет только увеличиваться

Оборудование для систем серьезных масштабов следует подбирать с особой тщательностью. Особенно те его части, которые составляют костяк ИСБ. Рекомендуется внимательно изучить варианты, предлагаемые на рынке, и сделать выбор прежде всего в пользу качества, мощности и защищенности, так как скупой платит дважды.

Максим Горяченков:
Немаловажным фактором в выборе базовой программной платформы для создания крупной распределенной системы мониторинга будет являться наличие у нее сертификатов соответствия различным требованиям по защите персональных данных пользователей, хранения ДСП и секретных данных (ФСТЭК), соответствия ведомственным и внутрикорпоративным нормативным документам (постановление Правительства РФ о транспортной безопасности, перечни крупных госкорпораций и т.д.).

Алексей Марков:
Очень важным моментом является ресурсное обеспечение проектов по внедрению интеграционных платформ. Привлечение внешних специалистов – это практически обязательное условие, так как в интеграционный процесс вовлечены многие службы компании с различными внутренними установками, поэтому в проектной команде должны быть эксперты, находящиеся "вне схватки". Кроме того, технологически внедрение интеграционной платформы требует специалистов высокой квалификации по широкому спектру весьма специфических программных решений. Иметь их в штате компании невыгодно, а общей технической квалификации собственных сотрудников для этого, как правило, недостаточно, поэтому использование внешних высококлассных ресурсов более предпочтительно.

При внедрении единой интегрированной ИСБ необходимо также понимать принципы построения архитектур комплексных систем безопасности, основы бизнес-анализа, чтобы понять, как надо строить взаимодействие всех ИСБ филиальной сети. Такое понимание очень важно для достижения положительного результата.

Если говорить о проблемах интеграционных платформ, то следует в первую очередь отметить, что главной ахиллесовой пятой многих решений является наличие в их составе компонентов с различной историей развития, являющихся при этом продуктами разных компаний, когда-то приобретенных основным вендором. Часто новый хозяин решает обойтись "малой кровью" и вместо глубокой интеграции нового компонента ограничивается его подключением в качестве внешнего модуля, а это со временем приводит к резкому росту дополнительных вычислений со всеми вытекающими ресурсными издержками, включая увеличение стоимости серверного оборудования и т.д.

Дмитрий Пехов:
Выбор корпоративной платформы безопасности всегда является сложным вопросом, требующим тщательного всестороннего анализа и глубокого предварительного аудита. Важным фактором при выборе той или иной системы является точное понимание потребностей и задач большого количества подразделений заказчика. Для распределенных объектов не следует забывать про перечисленные ниже параметры.

1. Платформа должна быть максимально универсальной и иметь широкие возможности по интеграции с различными сторонними системами. С одной стороны, это позволяет осуществить плавный переход от существующего парка различных систем, установленных в филиалах организации, к единому аппаратно-программному комплексу. С другой – это позволит быстро обеспечить максимальный функционал при внедрении.
2. Для иностранных производителей платформ, на наш взгляд, очень важно иметь успешный практический опыт сотрудничества с локальными партнерами. С нашей стороны это конкретные кейсы с компаниями ISS, INSYRES и т.д.
3. Надежность и стабильность системы, которые подтверждены многолетним опытом применения на большом количестве распределенных объектов по всему миру. Часто работая в условиях нестабильных каналов связи, сетевые контроллеры должны обеспечивать надежную передачу накопленных событий в центральное ПО.
4. Срок жизни и поддержки, в том числе программного обеспечения, от производителя. Например, каждый релиз BIS в среднем поддерживается более пяти лет.
5. Гибкий принцип лицензирования платформы, который позволяет оптимально планировать бюджеты при расширении.
6. Единообразный подход к управлению "железом". Принцип "единого окна".
7. Полная поддержка ИТ-технологий при подключении аппаратных подсистем к интеграционной платформе.
8. Снижение требований к локальным АРМам – возможно использование технологий Web, HTML5 и CSS3 для формирования интерфейсов операторов.
9. Максимально гибкие отчеты, в том числе для внутреннего аудита (отчеты по действиям операторов и администраторов).

Вячеслав Петин:
Одна из важных рекомендаций при построении ИСБ – это использовать хорошо зарекомендовавшее себя оборудование и ПО от известных производителей, потому что реализация многофилиальной структуры требует немалых затрат и важно не ошибиться с выбором платформы. Лучше всего строить распределенную ИСБ на базе компонентов одного бренда, поскольку такой подход позволит получить на 100% рабочую систему, состоящую из полностью совместимых элементов. Моя рекомендация – это проверенные опытом инсталляторов во всем мире территориально распределенные ИСБ Bosch, Honeywell и Lenel.

Из конкретики при реализации ИСБ я бы рекомендовал обратить внимание на следующие свойства системы:

- возможность работы в различных часовых поясах одновременно;
- поддержка современных версий Windows и SQL;
- работа с протоколами IPv6 и OSDPv2;
- шифрование на всех уровнях передачи данных;
- реализация доступа по мобильным телефонам;
- возможность обмена данными с другими БД без привлечения дополнительных программных инструментов;
- модульное лицензирование, которое позволяет приобретать только необходимые лицензии и не переплачивать за ненужный функционал;
- сохранение инвестиций при расширении системы. ■

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

"Дальнобойная" парковочная СКУД: бюджетный комфорт

Изначально технология УВЧ-идентификации получила распространение в логистике, где она использовалась для учета движения больших объемов товаров. Затем это оборудование стало активно применяться в СКУД при дистанционной идентификации большого числа карт одновременно. Одним из самых успешных применений УВЧ-технологии распознавания меток стал контроль доступа автомобилей на парковки и на территории транспортных предприятий

Сфера применения УВЧ-идентификации (860–960 МГц) весьма обширна и, кроме систем безопасности и мониторинга грузов, включает в себя мониторинг положения шахтеров в шахте, защиту библиотечных фондов, отслеживание перемещений животных на фермах и многое другое. Существуют примеры нестандартного применения УВЧ-оборудования: радиочастотные метки используются при исследовании пещер, а также в музеях для автоматического предоставления посетителям информации об экспонате. За счет большого расстояния считывания ультравысокочастотных ридеров можно реализовать распознавание пользователей по методу Handsfree, когда персонал не должен совершать какие-либо действия при проходе через точку доступа.

Доступ на парковку в режиме "свободные руки"

УВЧ-оборудование удобно использовать при организации контроля доступа на парковку: на автомобиль устанавливается радиочастотная метка, считыватель настраивается на определенное расстояние идентификации и при приближении машины система автоматически срабатывает на разрешение/отказ в доступе. Вместо метки может использоваться пластиковая карта, которую водитель устанавливает под стекло автомобиля, а если карта комбинированная, использует ее для прохода через другие точки доступа. Принцип работы ультравысокочастотной СКУД такой же, как и у других RFID-систем с пассивными идентификаторами: когда метки или карты попадают в радиус действия электромагнитного поля считывателя, они получают от него энергию и генерируют ответный радиосигнал с кодом. Далее эта информация поступает на контроллер, который и принимает решение о доступе. Примечательно, что при этом система не требует, чтобы водитель остановил машину, открыл окно и потянулся к считывателю, поэтому ультравысокочастотные СКУД на парковках обеспечивают максимальный комфорт при повседневном использовании.

Считыватели Smartec с дальностью действия до 10 м

Для организации доступа на парковки Smartec предлагает использовать бюджетную новинку – "дальний" считыватель ST-LR320. Эта удачная модель совсем недавно появилась в продуктовом портфеле бренда, но уже успешно зарекомендовала себя в нескольких проектах. Считыватель обеспечивает дистанцию идентификации до 10 м и одновременное распознавание до 100 меток, а если требуется отстройка от сигналов автотранспорта, проезжающего вблизи точки доступа, радиус действия ST-LR320 можно уменьшить. Наличие Wiegand 26/34 гарантирует совместимость с любой системой контроля доступа, а встроенные интерфейсы RS-232 и RS-485 позволяют интегрировать данный считыватель в различные прикладные программы. Кроме этого устройства, в линейке Smartec представлен еще один УВЧ-считыватель с похожими характеристиками – ST-LR300. Его основное отличие от вышеописанной модели – наличие порта Ethernet, который позволяет подключиться к считывателю по сети с помощью ПК и вести сбор данных из различных приложений.

Комбинированные идентификаторы для доступа на парковки и в офисные СКУД

Для работы с УВЧ-считывателями Smartec производитель предлагает специальные пассивные карты и метки, работающие в ультравысокочастотном диапазоне. Память таких идентификаторов разделена на несколько пользовательских полей и одно заводское. Пользовательские поля предназначены для чтения и записи изменяемой информации. В заводское поле при производстве карт записывается уникальный для каждого чипа код, который можно считать, но нельзя изменить, поскольку эта область памяти не перепрограммируется.

Smartec ST-LC300 – стандартная пластиковая карта, оснащенная только УВЧ-чипом. В корпусе другой модели, ST-LC300EM, объединены сразу два чипа – УВЧ и EM, поэтому их можно одновременно использовать в парковочных СКУД с ультравысокочастотными считывателями и в офисных системах доступа с картридерами стандарта Em-Marine (125 КГц). Под маркой Smartec также выпускаются комбинированные карты ST-LC300MF, в которых совмещены чипы УВЧ и Mifare (3,56 МГц).

RFID-метки для крепления на автомобили и грузы

При доступе на парковку очень удобно использовать RFID-метки, которые позволяют автомобилисту не заботиться о том, взял ли он с собой пропуск, ведь метка всегда будет прикреплена к машине. В частности, метки ST-LT310, которые были разработаны специально для контроля проезда автотранспорта и перемещения грузов, можно крепить на металлическую поверхность – на номер автомобиля или на наружную часть грузового контейнера. В свою очередь, метки ST-LT320 изготавливаются из бумаги и имеют клейкий слой, что позволяет приклеивать их на стекло автомобиля с внутренней стороны.

Удобный ввод кодов в базу данных СКУД

Для регистрации идентификатора в базе данных системы контроля доступа достаточно поднести его к настольному считывателю ST-CE310LR, который автоматически введет его код в активное поле запущенного приложения. В отличие от ручного метода ввода кодов, такой считыватель позволяет исключить ошибки, связанные с человеческим фактором, и сократить время на регистрацию пропуска. Подключение ST-CE310LR к компьютеру выполняется с помощью стандартного USB-интерфейса, а для удобства оператора считыватель имеет световую и звуковую индикацию срабатывания. ■

УВЧ-карты и метки марки Smartec

УВЧ-считыватели Smartec: ST-LR300 и ST-LR320

USB-считыватель ST-CE310LR для ввода кодов идентификаторов в базу данных

КОЛОНКА РЕДАКТОРА

Осторожность не повредит

Для повышения надежности биометрической системы логично использовать мультимодальную аутентификацию. Методы объединения нескольких биометрических характеристик приведены в ГОСТ Р 54411–2011/ISO/IEC/TR 24722:2007 "Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии".

Использование нескольких биометрических модальностей, как показывают расчеты и здравый смысл, вроде бы должно повысить надежность определения личности человека и обеспечить защиту от различного рода подделок.

В статье "Особенности мультибиометрических технологий" показано, что к объединению мультибиометрических технологий необходимо подходить осторожно, поскольку в случае применения принципа объединения на уровне принятия решения ошибки распознавания могут не только не уменьшиться, но и увеличиться.

Повышение надежности и качества систем распознавания удается достичь при применении комбинированных (интегральных методов), например объединяя получаемые решения на уровне образцов или на уровне признаков и формируя в дальнейшем объединенный шаблон.

Система, построенная с использованием интегральных методов, потребует создания специализированной базы данных для проведения тестирования. Например, применение методов объединения по голосу и изображению лица потребует создания проверочной базы данных, содержащей изображения лиц и записи голосов. При этом следует обратить внимание на то, что в базе данных должны находиться только те субъекты, у которых были собраны обе биометрические характеристики.

Принципы проведения испытаний для различных модальностей приведены в следующих национальных стандартах:

- ГОСТ Р ИСО/МЭК 19795-1–2007 "Автоматическая идентификация... Часть 1";
- ГОСТ Р ИСО МЭК 19795-2–2008 "Автоматическая идентификация... Часть 2";
- ГОСТ Р ИСО/МЭК ТО 19795-3–2009 "Автоматическая идентификация... Часть 3".

Василий Мамаев
Редактор рубрики "Биометрические системы", заместитель директора некоммерческого партнерства "Русское биометрическое общество"

Особенности мультибиометрических технологий

Современные биометрические технологии распознавания личности за последнее десятилетие получили широкое развитие и распространение. Анализ результатов тестов NIST за все время проведения тестирования алгоритмов распознавания по изображению лица показывает огромный прогресс в их совершенствовании

Елена Кручинина
Независимый эксперт, к.т.н.

Данила Николаев
Директор НП "Русское биометрическое общество", председатель ТК 098 "Биометрия и биомониторинг"

Одним из вариантов защиты биометрических систем от подделки является многократное усложнение возможности создания поддельных образцов, а именно – применение двух и более биометрических характеристик (лицо, отпечатки пальцев, голос, радужная оболочка глаза), получение биометрических образцов с помощью различных методик (видимый диапазон и ИК-диапазон), регистрация нескольких экземпляров одной биометрической модальности (два ракурса лица). Выполнение таких "объединений" с целью улучшения качества автоматического распознавания личности и защиты биометрических систем от подделки представляет собой мультибиометрическую технологию распознавания.

Предпосылки развития мультибиометрической технологии

Данные, полученные в результате тестирования 2017 г., на некоторых базах демонстрируют, что при вероятности ошибки ложного совпадения FMR = 10^{-3} существуют алгоритмы, показывающие вероятность ошибки ложного несовпадения FNMR = 6×10^{-3} (рис. 1).

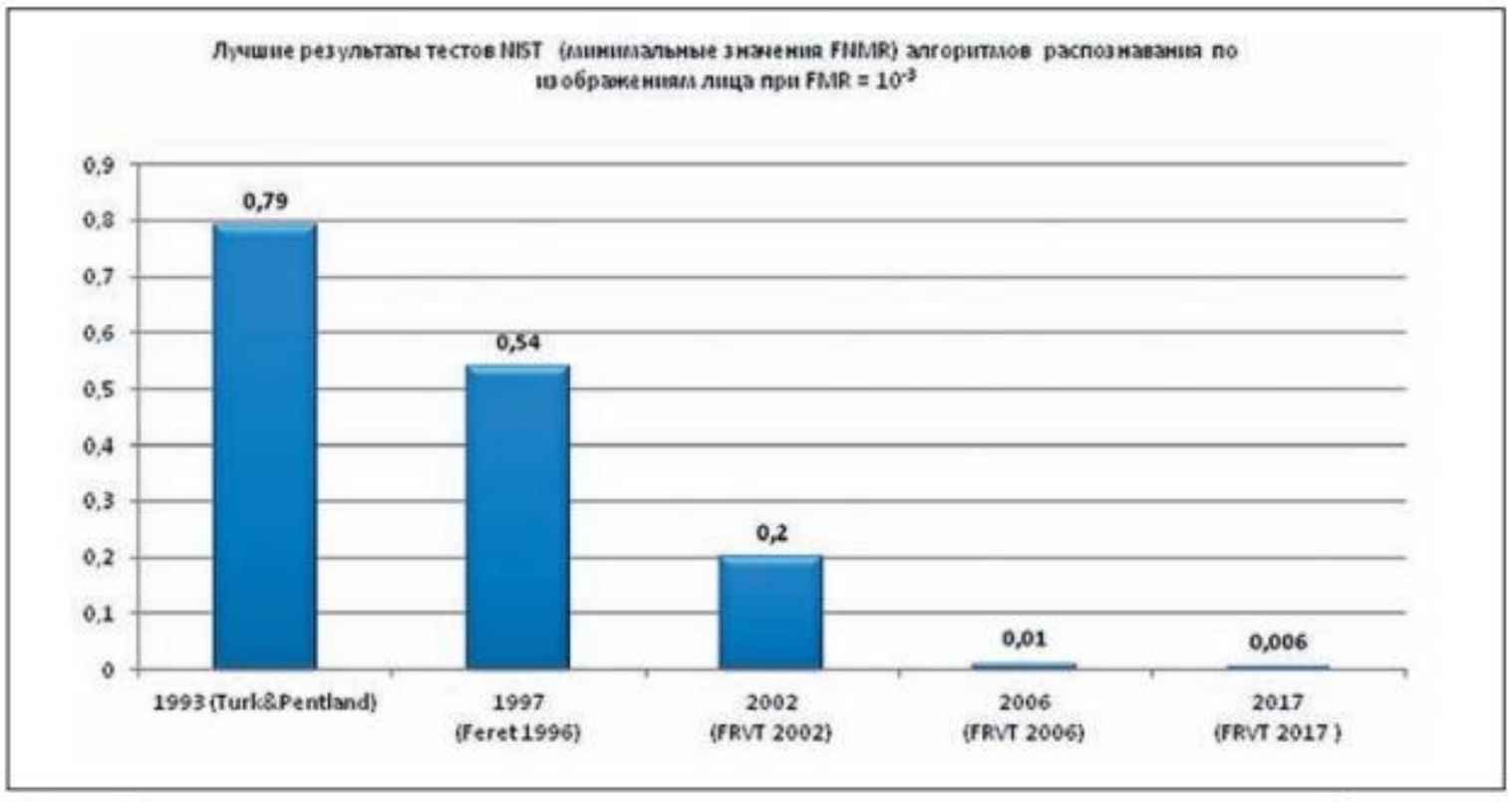


Рис. 1. Динамика совершенствования алгоритмов распознавания личности по изображению лица

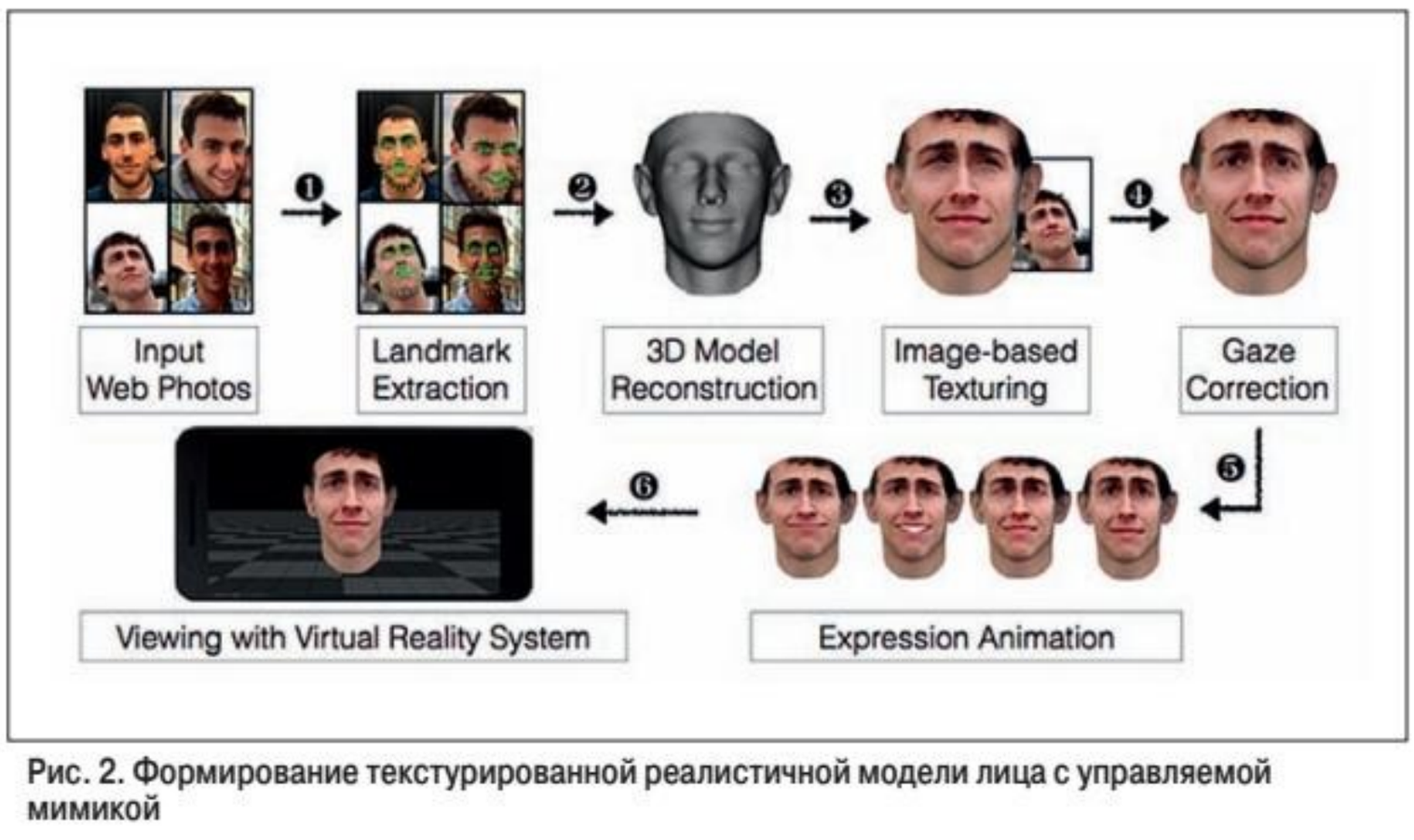


Рис. 2. Формирование текстурированной реалистичной модели лица с управляемой мимикой

Аналогичные улучшения вероятностных характеристик можно наблюдать и у других распространенных технологий распознавания личности: по отпечаткам пальцев, голосу, венам руки. Однако приведенные и рассчитываемые при тестировании вероятности учитывают только ошибки самих алгоритмов, когда их обман не был запланирован и целенаправленно осуществлен. Обзор источников показал, что наравне с развитием алгоритмов распознавания совершенствуются и способы подделки биометрических образцов для целенаправленного обмана систем.

Если первые системы лицевой биометрии можно было обмануть, предоставив фотографию или видеоролик с изображениями лица, то теперь большинство алгоритмов имеет встроенную защиту против такого способа подлога – методы оценки "живости" (Liveness Detection). Некоторые разработчики применяют алгоритмы оценки эмоций, отслеживание направления взгляда, подсчет количества морганий для выявления подлога с помощью фотографии или видеоролика.

Тем не менее современные возможности создания реалистических текстурированных трехмерных моделей позволяют перейти на новый уровень создания подделок для обмана систем безопасности на основе распознавания по лицу. В конце 2016 г. исследователи из университета Северной Каролины опубликовали статью с описанием метода формирования реалистичных моделей лиц на основе нескольких фотографий. Как показали авторы, исходным материалом для создания модели могут служить фотоизображения, опубликованные пользователем, например, в социальных сетях. Модель приводится в движение при помощи технологий виртуальной реальности, формируя узнаваемую мимику – поднятие бровей, улыбку и т.д. Проведенные эксперименты с несколькими ведущими разработчиками алгоритмов распознавания личности по изображениям лица подтвердили, что созданные трехмерные анимированные модели снижают вероятность правильной идентификации на 20–30%, а некоторые алгоритмы не могут отличить такую модель от живого лица.

В данном случае методом оценки "живости" и реальной "трехмерности" лица является использование ИК-датчиков и построение трехмерной модели лица перед проведением распознавания.

Задача выявления поддельных биометрических образцов особенно актуальна в случае удаленной идентификации и/или верификации личности пользователя (например, в банковском секторе), когда предоставить подделку проще, чем в общественном месте или при контакте с оператором или охранником.

Принципы объединения в мультибиометрической технологии

Суть применения мультибиометрической технологии заключается в том, что в ней удается получить большее количество информации об идентифицируемом субъекте. Обобщенно процесс обработки информации в биометрической системе может быть представлен в виде схемы (рис. 3).

Процесс объединения при создании мультибиометрической технологии может выполняться на любом из этапов обработки, поэтому традиционно выделяют следующие уровни объединения:

- уровень образцов. Выполняется регистрация различных биометрических образцов и формирование единого образца по специальному правилу, может использоваться одна модальность в разных представлениях (фото фас и профиль) или разные модальности (лицо, голос, отпечатки пальцев);
- уровень признаков. Выполняется обработка различных биометрических образцов и формирование отдельных векторов признаков, которые объединяются в один вектор признаков для дальнейшей классификации;
- уровень степеней схожести. В процессе параллельной обработки и классификации биометрических образцов формируется набор степеней схожести, которые объединяются в одну степень схожести или одно решение, в дальнейшем сопоставляемое с порогом принятия решения системы;
- уровень принятия решения. Каждая биометрическая технология формирует булев результат, которые объединяются с помощью комбинирующего правила.

При рассмотрении объединений на уровне регистрации и уровне извлечения признаков удается сформировать объединенный шаблон, который содержит большее количество идентифицирующих признаков, что может повышать вероятность правильной идентификации. В случае с объединением на уровне степеней схожести и принятия решений повышения надежности распознавания можно достичь за счет использования весовых коэффициентов для более "надежных" и "достоверных" результатов одной из технологий. Таким образом, можно сказать, что мультибиометрическая технология является более адаптивной к условиям применения и более информативной по объему обрабатываемой информации по сравнению с одномодальной биометрией.

Примеры и испытания лабораторных мультибиометрических систем с различными уровнями объединения показывают увеличение вероятностей идентификации на 5–15% (рис. 4).

Поскольку мультибиометрия преследует цель увеличения надежности системы за счет извлечения и обработки большего количества информации об объекте распознавания, то наилучшие результаты даст объединение отдельных параметров. В зависимости от уровня объединения могут возникать различные типы взаимодействия данных, например:

- взаимосвязь между модальностями. Имеет отношение к биометрическим образцам, которые физически связаны (например, речь и движение губ пользователя);
- взаимосвязь, возникающая вследствие идентичности биометрических образцов. Случай, когда один и тот же биометрический образец (изображение отпечатка пальца) или подмножества биометрического образца (голос, когда весь образец может быть использован одним алгоритмом и часть образца – другим) применяются разными алгоритмами извлечения признаков и алгоритмами сравнения (на основе контрольных точек и на основе текстуры);
- взаимосвязь значений признаков. Подмножество значений признаков, представляющих собой векторы признаков разных модальностей, могут быть взаимосвязаны, например

Рис. 3. Обобщенная схема обработки информации в биометрической системе

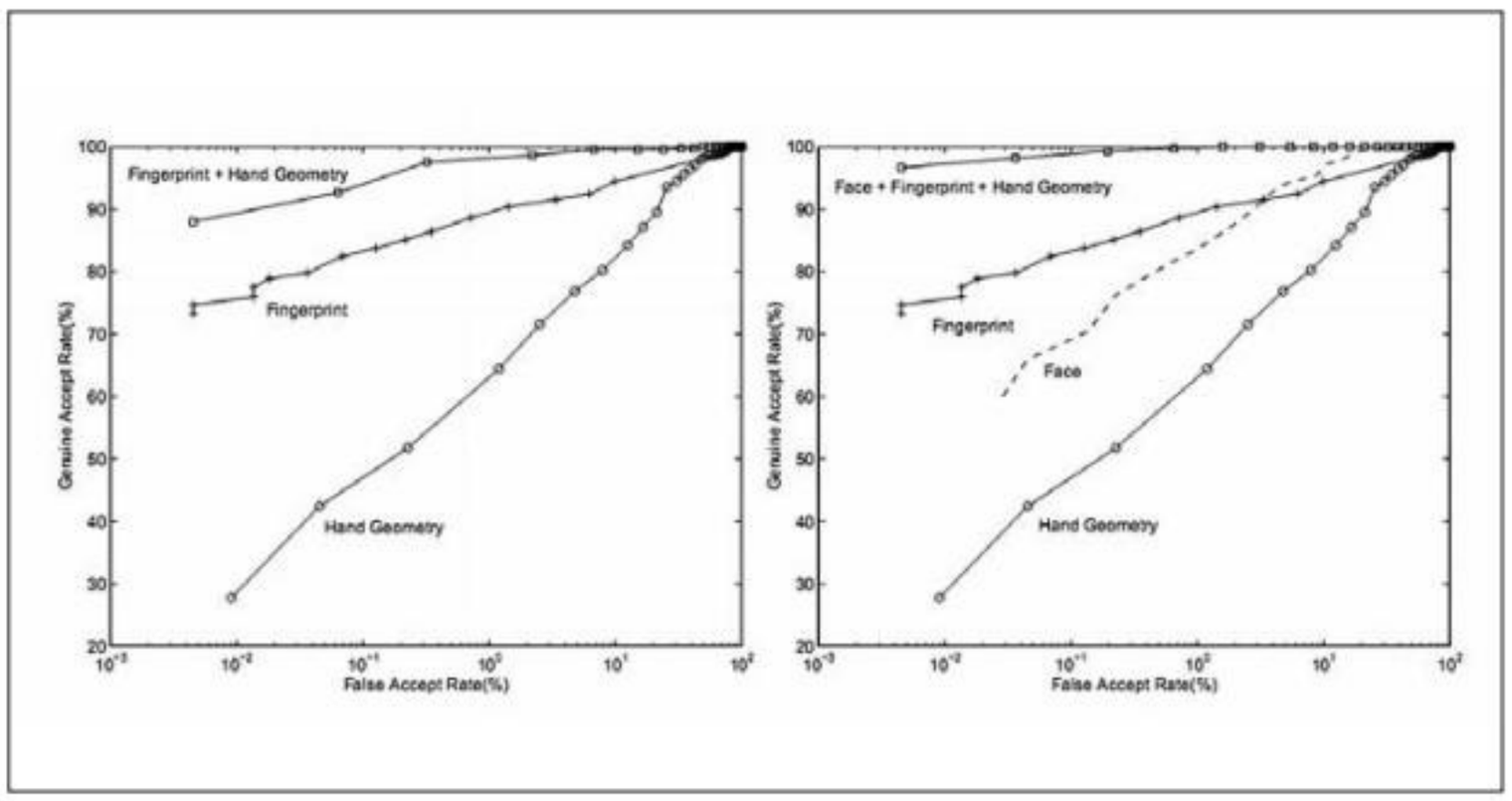


Рис. 4. Рабочие характеристики лабораторных мультибиометрических систем

площадь ладони пользователя (геометрия кисти руки) может быть связана с шириной лица;

- взаимосвязь экземпляров, возникающая при общей технике эксплуатации. Использование одного и того же устройства регистрации, один и тот же уровень подготовки оператора;
- взаимосвязь экземпляров, возникающая вследствие особенностей субъекта. К примеру, цветные контактные линзы на обоих глазах.

Для оценки взаимосвязи используют корреляционный коэффициент, который определяется по формуле:

$$p_{nC} = \frac{n \times N_C^f}{N - N_C^t - N_C^f - n \times N_C^f}$$

где n – общее число тестируемых классификаторов;

N – общее число входных данных;

N_C^f – число входных данных, ошибочно классифицируемых всеми классификаторами при использовании порога C;

N_C^t – число входных данных, правильно классифицируемых всеми классификаторами при использовании порога C.

Для получения наибольшего эффекта от объединения при формировании мультибиометрической технологии целесообразно применять параметры, коэффициент корреляции между которыми минимальный.

В настоящее время наибольшее практическое применение получили мультибиометрические системы, объединяющие две биометрические технологии на уровне принятия решений. Это обосновано относительной технологической простотой – отсутствием необходимости поиска способов объединения биометрических образцов или шаблонов, создания новых алгоритмов сравнения. Объединение на уровне принятия решения также позволяет использовать биометрические системы различных производителей, а в случае применения логического правила принятия окончательного решения – оценивать конечные вероятностные характеристики мультибиометрической системы на основе известных параметров объединяемых технологий.

Оценка вероятностных характеристик

Как уже было отмечено ранее, мультибиометрическая технология предусматривает объединение параметров, и это позволяет выдвинуть предположение, что об объекте "больше информации лучше, чем меньше информации", и, значит, технология должна быть надежнее. С другой стороны, интуитивно можно предположить, что если "надежная" технология сочетается с более "слабой", то результирующий метод принятия решений в некотором смысле усредняется и после объединения результирующие параметры будут находиться где-то между результатами исходных технологий.

Ключом к разрешению кажущегося парадокса является то, что когда две технологии объединяются, одна из результирующих ошибок первого или второго рода (FAR или FRR) становится ниже, чем у более надежной технологии, тогда как другая ошибка становится выше, чем у менее надежной технологии. Если две биометрические технологии существенно различаются по надежности ("мощности"), то объединение их может дать в некоторых случаях более высокие вероятности ошибок, чем исключительно более "надежная" и "сильная" биометрическая технология.

Рассмотрим объединение двух независимых биометрических технологий разных модальностей, например по изображению лица и по голосу. Каждая из них характеризуется собственной парой коэффициентов ошибок первого и второго рода в данной точке рабочей характеристики системы (ROC):

- p_1^{FAR} – вероятность ложного допуска первой биометрической технологии;
- p_1^{FRR} – вероятность ложного недопуска первой биометрической технологии;
- p_2^{FAR} – вероятность ложного допуска второй биометрической технологии;
- p_2^{FRR} – вероятность ложного недопуска второй биометрической технологии.

Предположим, что объединение технологий выполняется на уровне принятия решения. Рассмотрим два наиболее простых способа формирования совместного решения:

1. Правило конъюнкции (логическое "И"). Положительное совместное решение при требовании двух положительных решений от каждой из технологий.

2. Правило дизъюнкции (логическое "ИЛИ"). Положительное совместное решение при условии хотя бы одного положительного решения из двух технологий.

Теперь можно рассчитать коэффициенты ошибок первого и второго рода (FAR и FRR) для комбинаций двух технологий. Результирующие вероятности ошибок будут обозначаться: $p_{или}^{FAR}$, $p_{или}^{FRR}$, $p_{и}^{FAR}$ и $p_{и}^{FRR}$.

Если для объединения используется правило "ИЛИ", то ошибка ложного недопуска может возникать только в том случае, если обе технологии дали ошибочное решение ложного недопуска. Таким образом, вероятность ошибки ложного недопуска объединенной технологии определяется произведением двух вероятностей:

$$p_{или}^{FRR} = p_1^{FRR} \times p_2^{FRR}.$$

Вероятность этой ошибки будет меньше, чем у исходных технологий. Но вероятность ложного допуска FAR при использовании этого правила будет выше, чем у исходных технологий:

$$p_{или}^{FAR} = 1 - [1 - p_1^{FAR}] \times [1 - p_2^{FAR}] = p_1^{FAR} + p_2^{FAR} - p_1^{FAR} \times p_2^{FAR}.$$

При применении правила "И" для объединения двух технологий ошибка ложного доступа может возникать только в том случае, если обе технологии дали решение ложного доступа. Таким образом, объединенная вероятность ошибки ложного доступа является произведением вероятностей ошибок отдельных технологий:

$$p_{и}^{FAR} = p_1^{FAR} \times p_2^{FAR}.$$

Таким образом, ошибки ложного доступа при использовании данного правила будут меньше, чем ошибки исходных технологий, а объединение дает более надежную мультибиометрическую технологию. Но вероятность ложного недопуска при использовании этого правила, которая может быть выражена как дополнение к вероятности того, что ни первая, ни вторая технология не вызовет ложный отказ доступа, оказывается выше, чем для каждой технологии в отдельности:

$$p_{и}^{FRR} = 1 - [1 - p_1^{FRR}] \times [1 - p_2^{FRR}] = p_1^{FRR} + p_2^{FRR} - p_1^{FRR} \times p_2^{FRR}.$$

Приведенные расчеты справедливы при линейном логическом объединении двух технологий на уровне принятия решений, когда каждая из технологий дает логический (булев) результат сравнения (да/нет).

В общем случае в мультибиометрической технологии выполняется объединение разных параметров на различных уровнях, могут использоваться не только линейные, но и параллельные способы обработки данных и формирования решения. Поэтому рассчитать окончательные вероятностные характеристики системы на основе известных параметров исходных технологий в большинстве случаев не представляется весьма затруднительным.

secutech

The 21st International Security Expo

25 – 27 April 2018
Taipei Nangang Exhibition Center, Taiwan
www.secutech.com

Gathering leading brands to showcase security and AI innovations, Secutech will help you quickly build new partner networks and make your business thrive in the growing vertical markets.

Smart street lighting
Offering solutions in lighting and energy management, sensors and environmental monitoring, wireless transmission, real-time data processing and analytics.

Safe City
Converging AI, deep learning and big data to showcase the latest intelligent surveillance and video analytics systems.

Intelligent transportation
Demonstrating product and solutions for railway and highway monitoring, fleet management, 3G/4G telematics, smart parking and real-time traffic control.

Smart factory
Featuring video based analysis, machine vision, robotics, environmental monitoring system, big data analytics platform.

Smart retail
Showcasing retail solutions for consumer behavior analysis, warehouse management and operation management, displaying logistics platforms and more.

Smart living
Solutions for smart house, safe house and comfort house with smart security, software platform, mesh transmission, voice command, lighting control and intelligent video technologies.

Smart disaster prevention
Highlighting solutions in smart sensing, intelligent video surveillance, and disaster early warning.

Intelligent vertical solutions

For more information, please contact
Kirstin Wu
Kirstin.wu@newera.messefrankfurt.com

Concurrent with

Mobility Asia

SMhome powered by Secutech

fire&safety powered by Secutech

info security powered by Secutech

Register

В таком случае для достоверной оценки ошибок первого и второго рода мультибиометрической системы целесообразно выполнение полноценных испытаний. При этом необходимо использовать не синтезированные базы данных (искусственное случайное объединение различных баз данных, например разномодальных), а естественные. К примеру, для испытаний мультимодальной системы не должно допускаться объединение биометрических образцов разных людей, а необходимо формирование базы данных, в которой каждый человек представлен собственными биометрическими характеристиками. Данный подход позволяет учесть наличие взаимосвязи обрабатываемых параметров, которая в реальных условиях эксплуатации может повышать ошибки первого и второго рода.

Реализация на практике. Каковы перспективы?

Анализ литературных источников и принципов формирования мультибиометрической технологии показал, что при объединении двух и более технологий можно сформировать более надежную технологию с точки зрения как сложности создания поддельных образцов для обмана системы, так и более низких ошибок распознавания. На практике объединение желательно выполнять на уровне степеней схожести или принятия решения, такой подход позволяет минимизировать затраты на алгоритмическое обеспечение, но при этом использовать преимущество мультибиометрии.

В статье рассмотрены способы логического объединения двух технологий на уровне принятия решений, представлен математический аппарат для вычисления ошибок первого и второго рода мультибиометрической технологии на основе значений ошибок объединяемых технологий. Установлено, что логическое объединение "И" дает возможность сформировать более надежную технологию за счет уменьшения ошибки первого рода (ложного доступа). При логическом объединении "ИЛИ" удается снизить вероятность ошибки второго рода (ложного недопуска). Приведенный математический аппарат может применяться при создании мультибиометрических систем с указанными типами объединения для расчета ошибок первого и второго рода.

Объединение на уровне биометрических образцов и векторов признаков требует создания нового алгоритма сравнения и принятия решения, а в случае использования нейронных сетей – новой нейронной сети и обучения на базах данных объединенных образов/векторов признаков. Таким образом, подобное объединение требует существенных временных и финансовых вложений, а также не позволяет использовать наилучшие алгоритмы от ведущих разработчиков биометрических систем. Кроме того, данный подход хоть и имеет потенциальные преимущества в виде повышения надежности и устойчивости к подделкам, однако их достижимость зависит от качества разработки алгоритмов, баз данных для обучения и прочих условий. ■

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

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

securika Moscow

Москва

20–23 марта 2018

ЦВК «Экспоцентр»

Видеонаблюдение

Контроль доступа

Охрана периметра

Противопожарная защита

Сигнализация и оповещение

Автоматизация зданий

Организатор
Группа компаний ITE
+7 (499) 750-08-28
security@ite-expo.ru

Получите бесплатный электронный билет, указав промо-код

sec18iTKER

IdM-решения для автоматизации бизнес-процессов:
у любой монеты есть две стороны

Алексей Плешков
Редактор рубрики "Управление идентификацией"

Практически вся информация в любой организации, будь то детский сад с картами учащихся или ракетный завод с чертежами секретных разработок, оцифрована и обрабатывается с помощью вычислительных машин и программного обеспечения. Бизнес-процессы, разделенные на отдельные операции, выполняются сотрудниками организаций в специализированных (базовых или проприетарных) прикладных системах. Чем больше пользователей, тем сложнее предоставлять и контролировать доступ к прикладным системам и тем актуальнее и нужнее становится для организации внедрение системы управления учетными записями

IdM-решения как системы для идентификации пользователей и управления реквизитами доступа давно и успешно зарекомендовали себя в качестве основного инструмента администратора для автоматизации процедур предоставления и контроля доступа.

Практические выгоды IdM

В организации, где в повседневных бизнес-процессах участвуют одно и более структурных подразделений, функциональные роли неравномерно распределены между работниками, чьи рабочие места территориально разнесены, а степень их участия и полномочия регулярно меняются, система управления учетными записями и ролевая модель доступа являются единственным возможным вариантом автоматизации и сохранения тем самым таких дорогостоящих ресурсов, как время, рабочие места и деньги на оплату штата прикладных администраторов.

IdM не может существовать в вакууме – она требует интеграции и не работает сама по себе без настройки и сопровождения со стороны высококлассных ИТ-специалистов. Но даже это во многих случаях не мешает владельцам организации в долгосрочной перспективе, при быстром увеличении атомарных бизнес-операций и при желании так же быстро реагировать на эти изменения на рабочих местах сотрудников, оптимизировать свои затраты на ИТ и существенно экономить, по сравнению с ручным вводом и наделением работников правами по традиционной схеме.

Ограничение доступа

Для владельцев или руководителей бизнеса, которые на высоком уровне понимают схему работы своего персонала и не приземляют на прикладные системы основные функциональные роли, базовыми принципами с точки зрения информационной безопасности в любом случае остаются ограничение доступности обрабатываемой в системах чувствительной информации и организация непрерывного контроля за соблюдением выстроенных ограничительных мер. Ограничение доступности информации третьим лицам может быть реализовано:

- техническими средствами в рамках прикладного или системного программного обеспечения;
- наложенными (внешними) средствами контроля: служба каталогов, сетевые и локальные политики безопасности, средства шифрования и др.;
- организационно – путем выпуска соответствующих административно-распорядительных документов.

IdM на All-over-IP

При этом контроль за соблюдением выбранных мер чаще всего выполняется с помощью технических средств мониторинга событий и подсистемы уведомления о наступлении события с признаками инцидентов. Такие системы предполагают мониторинг действий пользователей в прикладных системах, мониторинг сетевой активности, мониторинг актуальных уязвимостей и другие виды мониторинга.

Цели и задачи

В качестве основных целей при внедрении автоматизированных средств управления учетными записями в любой компании чаще всего выбирается компиляция из нескольких пунктов, представленных ниже:

1. Автоматизация внутренних процессов предоставления и контроля доступа к автоматизированным системам.
2. Увеличение скорости внесения и качества отслеживания изменений прав доступа пользователей.
3. Снижение числа технических сбоев и ошибок в процессе эксплуатации и администрирования прикладного и системного программного обеспечения.
4. Построение централизованной и управляемой архитектуры для ИТ-подразделений в организации.
5. Унифицированный подход к предоставлению доступа в масштабах единой организации/группы компаний.
6. Существенная экономия ресурсов на эксплуатацию автоматизированных систем.
7. Проведение организационно-штатных и оптимизационных мероприятий в ИТ-подразделениях и сокращение внутренних финансовых расходов.

Мировой и российский рынок IDM

Рынок IdM-решений в мире с 2013 г. представляет собой ограниченное множество промышленно поддерживаемых, в большой степени интегрируемых между собой и дополняющих друг друга

Рис. 1. Рынок IdM/IAM(G) в мире

решений. По данным аналитических отчетов Gartner, 7–10 крупнейших игроков рынка ежегодно остаются в фокусе, несущественно меняясь местами и поглощая более мелкие компании.

Рынок IdM в России традиционно представлен не более чем дюжиной промышленных решений, некоторые из которых, что не может не радовать, являются высокотехнологическими разработками отечественных компаний. Эти разработчики в нише мирового рынка только начинают конкурировать с цифровыми гигантами класса IBM и Oracle, но в России они уже хорошо себя зарекомендовали и имеют широкую клиентскую базу из организаций, придерживающихся стратегии замещения импорта.

Успешные кейсы

Крупные компании сознательно идут на риск и внедряют у себя IdM, руководствуясь целями и задачами по автоматизации рутинных процедур. Одним из самых известных кейсов по внедрению IdM в кредитно-финансовых организациях последних лет является положительный опыт Банка Москвы. Бывший начальник управления информационной безопасности Банка Москвы Василий Окулесский в своих интервью неоднократно отмечал, что "появление системы управления доступом в Банке Москвы позволило поменять существующие на тот момент акценты. Те аспекты, на которые при обычных и привычных процессах в Банке вообще бы не обратили внимания, сейчас обрели большую значимость. Если раньше сама процедура управления заявками пугала своей сложностью и бесконтрольностью (напомню – бумага, скан, электронная версия, опять бумага), то сейчас она полностью автоматизирована. Проект по ходу своего выполнения потребовал усовершенствования бизнес-процессов, повысился уровень компетенций специалистов в части методики управления правами, а также произошло качественное изменение отношения к процессу управления доступом".

Подводные камни

Не все компании оптимистично настроены и тем более готовы тратить бюджет на внедрение систем управления учетными записями, а именно – компании и/или отдельные ИТ-руководители, имеющие негативный опыт внедрения IdM. К числу основных спорных моментов с точки зрения оптимизации и экономии чаще всего относят:

- непрогнозируемо растянутые по времени сроки ввода в эксплуатацию целевого решения внутри инфраструктуры заказчика при количестве подключаемых систем более 10;
- неоправданно высокая стоимость внедрения и владения решением класса IdM в перспективе 3–5 лет для небольшой организации;
- неготовность мировых и отечественных вендоров гибко реализовать интеграцию своих продуктов с проприетарными прикладными автоматизированными системами и вносить изменения в архитектуры решения в процессе нетипового внедрения;
- высокие трудозатраты на сопровождение и негибкость схемы работы IdM при условии изменения компонентов внешней по отношению к IdM инфраструктуры;
- статичность и/или прямая зависимость корректной работы IdM от стабильности и неизменности смежных систем;
- негибкость системы к жизненным ситуациям и/или невозможность заложения в алгоритм работы IdM всех вероятных сценариев, связанных с последствиями изменения реквизитов доступа пользователей;
- большое количество сбоев в результате реализации ошибок первого и второго рода и, как следствие, увеличение на первом этапе внедрения недовольства качеством ИТ-сопровождения со стороны бизнес-пользователей.

Рис. 2. Рынок IDM/IAM(G) в России

Внедрять или не внедрять?

Применять IdM в организации или нет – это сознательный выбор ИТ-руководителя, который видит и чувствует возможности и особенности автоматизации внутри подконтрольной ему инфраструктуры. Решения на отечественном рынке есть, они опробованы, многие имеют более чем десятилетнюю историю постоянного улучшения и интеграции. Но, как и в других сферах и областях ИТ-индустрии, не стоит забывать о том, что у любой монеты есть две стороны. ■

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

Итоги года в IdM. Мнения экспертов

Итоги года подводят по-разному: делают отчеты, графики, презентации. Подобрать количественный способ для фиксации и обсуждения достигнутых успехов и перспектив в такой специфической области, как информационная безопасность, довольно сложно, особенно в сфере управления правами и учетными записями в автоматизированных системах (далее – IdM от англ. Identity Management).
Оптимальным способом является диалог с экспертами-практиками. Мы попросили дать ответы на наши вопросы специалистов, которые имеют успешный опыт в проектах по развертыванию, сопровождению или модернизации IdM на площадках у заказчиков

Расскажите о наиболее интересном, на ваш взгляд, проекте по направлению IdM, в котором вам удалось принять участие в 2017 г.

Мария Ерохина:
Наиболее интересным мне кажется проект в одном коммерческом банке, включавший в себя нетривиальные задачи и требовавший комплексного решения. Наш IdM использовался в сочетании с модулем SSO и двухфакторной аутентификацией по смарт-картам. Сотрудники банка не знают своих паролей в целевых системах, аутентифицируются по карточкам, которые объединяют в себе множество функций. В частности, IdM был интегрирован со СКУД для автоматической блокировки доступа сотрудников к ИТ-системам при выходе из офиса и автоматической разблокировки при приходе на работу. Для компаний, которым важно ограничивать доступ к информации и данным своих клиентов, такое решение может быть очень актуальным.

Как чаще всего заказчик формулирует цели и задачи по проекту IdM и как удается скорректировать эти формулировки?

Мария Ерохина:
Чаще всего мы слышим: "Хочу управлять доступом", "Хочу контролировать ситуацию", "Нужна автоматизация предоставления доступа во всех системах" и мое самое любимое – "Мы хотим сделать ролевую модель, а потом внедрять IdM".
Каждый из этих запросов говорит о какой-то проблеме, и важно понять, о какой именно, так как под этими фразами каждый клиент имеет в виду что-то свое. Мы практикуем индивидуальный подход – разбираемся с тем положением вещей, которое имеет место в текущий момент, включая бизнес-процессы, состояние информационных систем, планы по их модернизации и замене, требования стандартов и регуляторов (состояние as is). После этого мы формируем конечную картинку – как все должно быть (состояние to be), с разбивкой по этапам достижения цели. При этом всегда учитываем рентабельность того или иного функционала, поскольку такие масштабные и ресурсозатратные проекты, как внедрение IdM-решения, в обязательном порядке проходят процедуру обоснования для бизнеса. В ходе согласования функционал может претерпеть значительные изменения и в отношении формулировок, и по существу.

С какими типовыми трудностями в рамках проектов по IdM сталкивается чаще всего ваша группа внедрения?

Мария Ерохина:
Я бы выделила два основных вида "осложнений" на проекте: организационные и технические.
Если говорить об организационных трудностях, то чаще всего мы имеем дело с несогласованностью действий служб компаний-заказчиков и непониманием сути процесса внедрения. К сожалению, далеко не все компании сталкивались с интеграционными проектами, а внедрение IdM предполагает интеграцию с различными бизнес-системами, которые подконтрольны разным службам заказчика. Из-за этого сроки реализации проекта могут существенно увеличиться.
К самым частым техническим трудностям можно отнести неготовность инфраструктуры к интеграции, существенную кастомизацию бизнес-систем, с которыми требуется интеграция, а то и просто работа с "древними" самописными системами, заменить которые заказчик по целому ряду причин не готов.
Тем не менее работать с такими трудностями можно и нужно. Мы консультируем заказчика, стараясь предусмотреть любые сложности на проекте и вырабатывая проектные решения для компенсации исторического разрыва в технологиях. Кроме того, в этом году мы решили организовать для наших потенциальных клиентов целый цикл обучающих мероприятий на тему того, как правильно подготовиться к внедрению IdM.

Роман Федосеев:
Есть несколько основных критериев успешности IdM-проекта:
- простые, понятные, достижимые цели проекта;
- квалифицированная проектная команда со стороны заказчика;
- наличие качественных сред разработки и тестирования.

Если что-то из вышеперечисленного отсутствует, то на проекте возникают сложности.

Алексей Лукацкий:
Я бы не назвал это трудностью, просто в контексте проектов нашей компании, а Cisco преимущественно концентрируется на сетевой безопасности, мы видим, что большинство проектов по IdM фокусируются на идентификациеи пользователей, забывая про идентификацию устройств, с которых пользователи заходят в корпоративную или ведомственную сеть. Такая "забывчивость" приводит к тому, что возникают ситуации, когда пользователь проходит все проверки, а его зараженный компьютер начинает жить своей жизнью и именно с него идет заражение внутренней сети. И это не говоря уже о том, что существует немало ситуаций, когда устройство подключается к сети вообще без пользователя на борту – принтеры, СКУД, видеокамеры, промышленные контроллеры и т.п.

Мария Ерохина
Менеджер по продвижению IGA-платформы Solar inRights компании Solar Security, CISM, CRISC

Роман Федосеев
Генеральный директор компании 1IDM

Алексей Лукацкий
Бизнес-консультант по безопасности компании Cisco

Каких побочных (помимо основных) результатов для заказчика удалось достичь вам на проектах по IdM в 2017 г.?

Мария Ерохина:
Смотря что называть "побочным" результатом, ведь цели внедрения IdM-решений могут кардинально различаться. Для одних побочным эффектом от внедрения IdM будет наведение порядка в информационных системах и снижение рисков за счет прозрачности процессов и инфраструктуры, для других – построение актуальной ролевой модели (да, ее лучше строить после внедрения, основываясь на фактическом состоянии дел), а кто-то снизит трудозатраты на предоставление доступа.
В 2017 г. мы помогли одному из заказчиков разобраться с инфраструктурой и установить зоны ответственности за процессы предоставления доступа, а для другой компании разработали отчеты для проведения аудита доступа сотрудников и выстраивания ролевой модели.

Роман Федосеев:
Как правило, в рамках IdM-проектов удается улучшить достоверность и актуальность кадровой информации. Информация о пользователях является исходной для IdM-систем, и от ее качества зависит качество всего процесса управления учетными записями и правами доступа.

Алексей Лукацкий:
Побочные результаты зависят от того, насколько их ждут и к ним готовы сами заказчики. Например, в одном из проектов "побочным", который на самом деле является основным, стала существенная финансовая экономия. Ведь обычно мы не задумываемся о том, сколько времени теряется на заведении учетных записей, на входе в различные системы, на разрешении проблем, на предоставлении доступа. Если сложить эти цифры вместе, то в большой компании экономия может составить огромную сумму. В одной из организаций, в которой трудилось 120 тыс. сотрудников, экономия от внедрения IdM составила более 20 млн долларов.

Что, на ваш взгляд, является правильным выбором заказчика: внедрение IdM от российского производителя или выбор и имплементация аналогичного иностранного решения?

Мария Ерохина:
На мой взгляд, заказчик сам может решить для себя этот вопрос.
Наша IGA-платформа Solar inRights успешно конкурирует на российском рынке как с российскими IdM-решениями, так и с западными. IdM выбирают не по принципу происхождения, хотя для ряда компаний это значимый критерий. Камнем преткновения становится выбор интегратора, у которого есть соответствующая экспертиза и который сможет выполнить проект. И, разумеется, заказчикам важен функционал, который реализован в том или ином IdM-решении, возможность обновления и масштабирования системы. Ценовая политика в последние годы также играет большую роль. Но, с учетом продолжения истории с санкциями, выбор западного решения становится все более рискованным.

Роман Федосеев:
Кому-то надо "шашечки", а кому-то – "ехать". Единого рецепта нет. Решение должно в первую очередь отвечать требованиям заказчика, и заказчик должен быть готов за него заплатить.

Алексей Лукацкий:
Я не сторонник национализма в ИБ. Качество продукта определяется не страной происхождения его разработчиков или владельца, а функциональностью и планами по развитию, в том числе и с учетом геополитических рисков. Кроме того, надо понимать, что иностранный сегмент рынка IdM появился гораздо раньше и он является более зрелым, чем российский. А в ряде ниш, например в решениях по контролю сетевого доступа и идентификации сетевых устройств, российских продуктов нет вообще и выбирать не приходится.

Расскажите о курьезном случае, если такой имел место в проектах по IdM в прошлом году.

Мария Ерохина:
К нам обратился заказчик из крупного концерна. На их предприятии на тот момент уже более полутора лет шло внедрение IdM другого российского производителя, позиционирующего себя технологическим лидером в сегменте Identity Management. Но никаких значимых результатов заказчик так и не получил: то система "не взлетала"; то работала, но не так, как надо; то разваливалась после установки патча, которого ждали полгода. Наши инженеры выполнили весь объем задач по проекту за девять недель. Для IdM это практически нереальный срок. Вот такие курьезы отечественного рынка!

Какие заказчики в 2017 г. чаще обращались к вам с задачами, связанными с работой IdM?

Мария Ерохина:
К нам приходят заказчики практически из всех отраслей, кроме малого бизнеса. Наибольший спрос наблюдается со стороны крупных компаний, которым очень не хватает упорядоченности в предоставлении доступа и автоматизации, а также со стороны банков, которые подчинены строгому регулятору в лице ЦБ.

Роман Федосеев:
Чаще всего к нам обращаются компании из реального сектора экономики – предприятия среднего и крупного бизнеса. Именно коммерческие предприятия находятся в жесткой конкурентной среде и вынуждены выбирать лучшие решения по параметру "цена/качество".

Алексей Лукацкий:
Наверное, наиболее прогрессивными в части проектов по сетевому IdM являются финансовые структуры, которые чаще других сталкивались с реальными атаками, наносящими измеримый деньгами ущерб. Они понимают, что защиты периметра уже недостаточно и надо четко фиксировать, кто или что, откуда, куда, когда и как подключается к корпоративной сети. Отсюда и необходимость проектов IdM, которые позволяют в любой момент отследить все попытки доступа пользователей и устройств, что и является залогом успеха если не в предотвращении инцидентов, то в их оперативном расследовании.

Если заказчик не хочет внедрять IdM, что в этом случае можно ему посоветовать в качестве альтернативы или компенсационных мер?

Мария Ерохина:
Организационные меры – выстраивание процессов управления доступом без технических средств, обучение персонала работе по заданной схеме. Однако стоит помнить, что это возможно лишь при высоком уровне зрелости компании.
Нередко до внедрения IdM используют таблицы Excel и скрипты – например, настраивают ежедневную/еженедельную выгрузку из кадровой системы, выгрузки из критичных целевых систем и сводят это в ручном режиме для осуществления контроля прав.

Алексей Лукацкий:
Любому проекту, в названии которого встречается слово Management, альтернативой можно назвать ручные операции, которые являются вполне нормальной практикой в небольших организациях, где просто нет потребности в централизации. Например, в небольшом офисе на 3–7 коммутаторов и маршрутизаторов не всегда необходимо внедрять системы управления сетевой идентификацией, можно ограничиться "поднятием" протокола 802.1x на сетевых устройствах. Например, в сети Cisco только маршрутизаторов 40 тыс. Понятно, что в ручном режиме настраивать на них правила идентификации пользователей и устройств – задача неподъемная. Поэтому я бы не стал говорить о какой-либо альтернативе или компенсации. Скорее речь может идти о том, что IdM – это осознанная необходимость организации, которая уже неспособна управлять своими пользователями и устройствами в ручном режиме.

Чего не хватает современным технологическим решения класса IdM, чтобы они получили массовое распространение?

Мария Ерохина:
В идеальном мире IdM-решения внедрялись бы быстрее, а стоили бы дешевле. Но вопрос тут скорее не в IdM-решениях как таковых, а в особенностях самой технологии. Разнообразие информационных систем, которые требуется интегрировать, сложность бизнес-процессов, которые требуется автоматизировать, организационные проблемы, которые требуется решить, – это те вещи, которые делают внедрение IdM сложным, а следовательно не столь массовым, как, скажем, DLP. Поэтому для перехода в сторону более массового распространения нужны изменения среды, в которой функционирует IdM.

Роман Федосеев:
Большинство современных IdM-решений очень сложные во внедрении и поддержке. Заказчики ждут простых и удобных решений с минимальной стоимостью владения.

Алексей Лукацкий:
Основная проблема любых сложных проектов – отсутствие стандартизации и унификации, позволяющей интегрировать решение в существующую инфраструктуру. Это напрямую касается и IdM, основное препятствие на пути массового распространения которых – сложность интеграции с существующими приложениями, в том числе и так называемыми legacy-приложениями, разработанными по заказу много лет назад и по которым в компании отсутствует экспертиза и документация, чтобы доработать их до интеграции с IdM.

Что бы вы посоветовали заказчикам, которые задумываются о внедрении IdM?

Мария Ерохина:
В первую очередь нужно четко сформулировать, зачем нужен IdM, осознавая все плюсы и минусы внедрения, а также возможные выгоды (снижение рисков, автоматизация рутинных операций и высвобождение ресурсов ИТ для более значимых задач, снижение затрат на операционную деятельность и т.д.).
Вторым шагом будет формирование внутри компании группы, которая будет заниматься внедрением IdM (подготовка инфраструктуры и целевых систем к интеграции, взятие под контроль процедур предоставления доступа, формирование требований к функционалу системы и т.д.).

Роман Федосеев:
Выявить потребность (не надо гнаться за модой), определить цели проекта, оценить собственные ресурсы (IdM-проект требует серьезного вовлечения сотрудников заказчика), оценить расходы на систему в перспективе пяти лет, выработать критерии оценки решений.

Алексей Лукацкий:
Так сложилось, что под IdM-проектами обычно понимают только управление идентификационной информацией пользователей, напрочь забывая про идентификацию устройств, которые могут сами по себе стать мишенью для злоумышленников или плацдармом для незаметного развития атаки по внутренней сети. Поэтому я бы посоветовал посмотреть и в сторону систем контроля сетевого доступа или сетевой идентификации, которые позволят проверять права на доступ не только пользователей, но и устройств.

Какие изменения в законодательстве в 2017 г. поспособствовали более глубокому проникновению IdM-решений на отечественный рынок?

Мария Ерохина:
IdM, на мой взгляд, – это история не про законодательство, хотя требования по управлению доступом есть и в новом ГОСТе, и в требованиях ЦБ. Управление доступом – один из базовых принципов информационной безопасности, соблюдение которого позволяет избежать массы неприятных историй. По сути, управлять доступом просто разумно.

Алексей Лукацкий:
2017 год был достаточно спокойным с точки зрения законодательных новелл – ни одного нового нормативного акта, упоминающего IdM, не появилось. Скорее, наконец-то пришло осознание у организаций, попадающих под действие 17, 21, 31-го приказов ФСТЭК, а также нормативных документов Банка России, например 382-П. А вот в следующем году у многих начнет "болеть голова" по поводу нового ГОСТ 57580.1 Банка России и законодательства по безопасности критической информационной инфраструктуры.

Как менялось осознание проблематики IdM у ваших заказчиков до проекта, в процессе внедрения и по его завершении?

Мария Ерохина:
Часто на начальном этапе есть непонимание реальных процессов в организации, какую работу по их оптимизации придется провести, а также насколько важны те или иные проектные решения. Многие особенности процессов (например, наличие специальных типов сотрудников) могут выясняться только при опытной эксплуатации. Нередко процессы приходится менять по ходу внедрения, например что-то сделать с тем, что приказы о приеме сотрудников на работу могут вводится в кадровую систему с задержкой в пять дней. Многие вещи поначалу кажутся клиентам незначительными, а при переводе системы в эксплуатацию такие "мелочи" могут стать ключевыми для правильной автоматизации бизнес-процессов, и клиенты удивляются, почему раньше им об этом не сказали. Таким образом, по ходу внедрения осознание сильно меняется, но, к сожалению, происходит это только опытным путем.

Роман Федосеев:
Уровень зрелости заказчиков может быть разным. Зрелые заказчики больше ориентированы на основные цели проекта, точнее выражают свои требования и имеют более реалистичные ожидания от проекта.

Назовите основные технологические недостатки IdM-решений и способы их компенсации.

Мария Ерохина:
Системе IdM на вход нужны чистые кадровые данные в определенном формате. Практически всегда возникают проблемы с качеством данных (повторения, ошибки последовательности, несвязанность и т.п.) и с предоставлением их в нужном формате. В данном случае решение – это специальные скрипты для очистки данных.
Кроме того, с каждой целевой системой IdM работает на определенном уровне абстракции, например на уровне групп или ролей. А клиенты нередко хотят видеть более глубокий срез – не просто группы или роли, которые назначены пользователю в определенной целевой системе, но и полномочия, которыми обладают эти группы. Это ограничение преодолевается переработкой коннектора, но оно не всегда реализуемо в рамках имеющейся структуры данных.

Роман Федосеев:
Большинство IdM-решений построены с использованием особенных технологий разработки, поэтому на российском рынке мало квалифицированных специалистов. В этой ситуации советую заказчикам обращать внимание на решения с открытым исходным кодом и достаточной доступностью специалистов на рынке.

Как изменилась за последний год относительная стоимость проектов по внедрению IdM?

Мария Ерохина:
Думаю, она не изменилась. Проекты IdM запускаются в среднем 1,5–2 года. Для изменений это слишком короткий срок.

Роман Федосеев:
По нашим наблюдениям, стоимость IdM-проектов не изменилась за последний год. Но существенно увеличилось само количество запросов на проекты.

Алексей Лукацкий:
Относительная стоимость любого проекта по ИБ – понятие такое же относительное, как и средняя зарплата. Все очень сильно зависит от типа организации, ее масштаба, количества пользователей и устройств, зрелости и т.п. Но чаще всего мы видим, что ввиду немалых затрат ресурсов (не только финансовых, но преимущественно временных) заказчики предпочитают поэтапное внедрение IdM-решений, начиная с отдельных подсистем или сегментов, постепенно расширяя внедрение на всю организацию.

Приведите пример сценария атаки на инфраструктуру типовой организации, эффект воздействия которой можно минимизировать за счет наличия внедренного IdM-решения.

Мария Ерохина:
Самое типовое – незаблокированный доступ уволенного сотрудника к корпоративным системам. Для ряда организаций, особенно банковского сектора, ограничения доступа являются требованием регулятора. Незаблокированный доступ чреват утечкой значимой для организации информации, данных клиентов и партнеров, информации о проектах. При этом не стоит забывать о принципе Defense in Depth, то есть безопасность не может обеспечиваться только одним средством, всегда нужна многослойная защита.

Алексей Лукацкий:
Если рассматривать сетевые IdM-решения, то они помогают бороться с практически любой внутренней угрозой. Например, подмена устройства, подключающегося к коммутатору, взлом Wi-Fi, компрометация внутреннего компьютера вредоносным кодом. Во всех этих случаях идентификация устройств позволяет локализовать атаку и не дать ей распространяться по сети. ■

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

ВИДЕОНАБЛЮДЕНИЕ

Автоматизированная система круглосуточного тепловизионного контроля электротехнического оборудования АСТРОН-ТА

Производитель: АО "ОКБ "АСТРОН"
Сертификат: информация не предоставлена
Назначение: круглосуточное видеонаблюдение и диагностика состояния электротехнического оборудования, узлов и агрегатов различных установок, производственных линий и технологических процессов
Особенности: возможность совмещения в одной системе функций охранного видеонаблюдения и контроля и диагностики оборудования
Возможности:
- круглосуточное видеонаблюдение, определение широкого набора дефектов и неисправностей электрического оборудования и различных механизмов по степени нагрева
- встроенная аналитика с функцией автоматического определения дефектов, выдача оповещения оператору о возникновении опасной ситуации

Характеристики:
- условия эксплуатации: УХЛ1 или ЭХЛ1, ГОСТ 15150
- питание 220/24 В (AC)
- частота сети 50 Гц
- спектральный диапазон 7–14 мкм
- степень защиты IP67
- потребляемая мощность макс. 30 Вт
- типичная с термостабилизацией 12 Вт
- изоляция по входу 3000 В
- импульсный ток до 20 кА
- диапазон рабочих температур от -60 до + 60 °С
- размер 330x300x180 мм
- масса не более 25 кг

Ориентировочная цена: 1 000 000 руб.
Время появления на российском рынке: декабрь 2017 г.
Подробная информация: www.astrohn.com
Фирма, предоставившая информацию:
АСТРОН, ОКБ, АО

DH-IPC-HFW4431TP-ASE-0360B

Производитель: Dahua Technology
Сертификат: RUC-CN.MO10.B.02006, выдан ЦЕНТР-СТАНДАРТ
Назначение:
- поддержка видеоаналитики
- запись видеоизображения
- возможность подключения внешнего микрофона

Особенности:
- 1/3" 4 Мпкс CMOS
- поддержка H.265/H.264 до 3 потоков
- 25 кадр/с при разрешении 4 Мпкс (2688x1520)
- широкий динамический диапазон
- объектив 3,6 мм
- дальность инфракрасной подсветки до 60 м
- слот карты памяти, IP67, IK10, ePoE

Возможности:
- поддержка технологии ePoE
- поддержка WDR
- поддержка видеоаналитики: пересечение линии (Tripwire); контроль области/вторжение в область (Intrusion); пропавшие и оставленные предметы (Object Abandoned/Missing); детекция лиц (Face Detection); поддержка кодека Smart H.265+

Характеристики:
- матрица 1/3" CMOS
- разрешение 4 Мпкс
- чувствительность: 0,06 лк @ F1.6 (цв., 1/3с); 0,4 лк @ F1.6 (цв., 1/30с); 0 лк @ F1.6 (ИК вкл.)
- дальность ИК-подсветки до 60 м
- фокусное расстояние 3,6 мм
- угол обзора: 83 град. (по горизонтали); 45 град. (по вертикали)
- питание 12 В (DC), PoE (802.3af) (класс 0), до 11 Вт
- класс защиты IP67, IK10

Время появления на российском рынке: 2018 г.
Фирма, предоставившая информацию:
DAHUA TECHNOLOGY RUS LLC

Интегрированные уличные PTZ-камеры Pelco Esprit Enhanced с бортовой видеоаналитикой

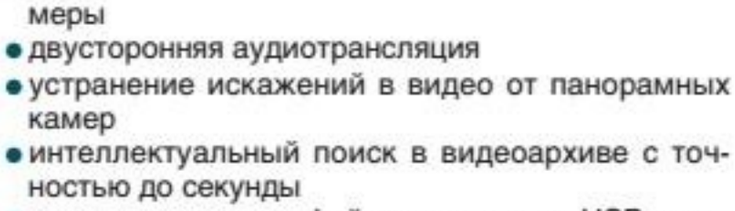
Производитель: Schneider Electric
Сертификат: RU C-FR.АИ96.В.00568, выдан ООО Сертификации продукции "ЭнергоСертСервис"
Назначение: круглосуточная видеосъемка с разрешением 2 Мпкс в системах охраны периметра аэропортов, морских портов, НПЗ и др.
Особенности:
- два типа оптических блоков для модификации в стандартном либо герметичном исполнении
- поддержка технологии SureVision 3.0
- предустановленная 9-модульная видеоаналитика, включающая AutoTracker, Abandoned Object и т.д.
- поддержка модулей SFP
- WDR 130 дБ
- 2-потоковая передача видео в H.264/MJPEG с разрешением до Full HD и фреймрейтом до 60 кадр/с
- функция "Антитуман" (3 уровня)

Возможности:
- 30-кратный трансфокатор (4,3–129 мм)
- стабильная работа при температурах от -45 до +60 °С
- "холодный старт" при -40 °С
- встроенный стеклоочиститель (модели ES6230-1xx)
- ИК-прожектор (850 нм) с дальностью подсветки до 200 м (модификации с индексом R)
- точность позиционирования ±0,1 град.
- локальное хранение видео на сменных картах памяти SDXC до 2 Тбайт
- совместимость с ПО Digital Sentry, Endura, VideoXpert
- соответствие ONVIF S/G/Q

Характеристики:
- светочувствительность до 0,008/0,001 лк
- панорамирование и наклон со скоростью до 140 град/с
- 1/2,8" КМОП-сенсор Exmor
- электронная стабилизация изображения (EIS)
- Anti-Bloom для компенсации "расплывания" картинки
- 3D-шумоподавление
- 256 предустановок
- маскирование до 32 зон
- солнцезащитный козырек
- 4 входа, 2 выхода тревоги
- питание по технологии HPoE, от источников 24 В (AC), 48 В (DC) или 100–240 В (AC)
- защита по классам IP66 и NEMA 4X

Ориентировочная цена: от 5494 долл.
Время появления на российском рынке: январь 2018 г.
Подробная информация: www.armosystems.ru
Фирма, предоставившая информацию:
АРМО-СИСТЕМЫ

32-канальный IP-видеорегистратор Honeywell HEN32304



Производитель: Honeywell Security and Fire
Сертификат: изделие сертифицируется
Назначение: запись, хранение, воспроизведение и передача по сети видео и аудио от IP-камер с разрешением до 12 Мпкс
Особенности:
- разрешение записи до 4K (12 Мпкс) при 15 кадр/с
- поддержка форматов H.265, H.264, MJPEG и MPEG-4
- 4-ядерный процессор
- встроенная ОС LINUX
- 8 слотов для установки HDD с суммарной емкостью до 64 Тбайт
- встроенный 16-портовый коммутатор PoE
- детектор движения с 396 зонами
- ONVIF-совместимость
- поддержка мобильных платформ Android и iOS

Возможности:
- запись видео с суммарным фреймрейтом до 960 кадр/с
- режимы записи: непрерывный, по сигналу тревоги, по расписанию, по движению, по активации вручную
- детекция потери видеосигнала и закрытия камеры
- двусторонняя аудиотрансляция
- устранение искажений в видео от панорамных камер
- интеллектуальный поиск в видеоархиве с точностью до секунды
- копирование видеофайлов по сети, на USB-накопитель, внутренний HDD или устройство eSATA
- гигабитное Ethernet-соединение

Характеристики:
- входящий/исходящий битрейт до 320 Мбит/с
- продолжительность видеозаписи от 1 до 120 мин.
- пред-/посттревожная запись: 1–30/10–300 с
- выходы мониторов: 2 HDMI (1-й с поддержкой разрешения 8 Мпкс, 2-й программируемый), 1 VGA
- синхронное воспроизведение до 16 каналов
- мультиэкранный режим
- 16 входов и 6 выходов тревоги
- порты 2 USB 2.0 и 2 USB 3.0
- RAID 0/1/5/6/10
- до 128 удаленных пользователей
- парольная защита доступа
- габаритные размеры 440x454x95 мм
- потребляемая мощность 17,5 Вт

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 151–152 "Ньюсмейкеры"

Ориентировочная цена: 85 500 руб.
Время появления на российском рынке: январь 2018 г.
Подробная информация: www.armosystems.ru
Фирма, предоставившая информацию:
АРМО-СИСТЕМЫ

IBS-3MS-2812AF

Производитель: INFINITY
Сертификат: информация не предоставлена
Назначение: уличная видеокамера с технологией STARLIGHT и моторизированным объективом
Особенности: высокочувствительная 3-мегапиксельная уличная видеокамера с моторизированным ZOOM-объективом 2,8–12 мм и ИК-подсветкой для работы в условиях сложной неравномерной освещенности
Возможности: высокая чувствительность и качественное изображение в условиях низкой освещенности, аппаратная система WDR двойного сканирования, всепогодное исполнение IP67, -40 °C
Характеристики: разрешение 3 Мпкс 1/2.8" Sony STARVIS IMX123 CMOS 3M + HiSilicon 3516D, моторизированный объектив 2,8–12 мм с удаленным управлением, 3DNR, D/N, True WDR, BLC, ROI, детектор движения, приватные зоны, защита от саботажа, базовые функции видеоаналитики, поддержка ONVIF, тревожный вход и выход, аудиовход/выход
Ориентировочная цена: 13 590 руб.
Время появления на российском рынке: I квартал 2018 г.
Подробная информация: http://r1.infinity-cctv.ru/
Фирма, предоставившая информацию:
СТА ПЛЮС, ООО

IDM-4M-28

Производитель: INFINITY
Сертификат: информация не предоставлена
Назначение: компактная антивандальная сетевая уличная видеокамера
Особенности: 4-мегапиксельная видеокамера с фиксированным широкоугольным объективом 2,8 мм и встроенной ИК-подсветкой для установки в помещениях или на улице
Возможности: универсальный вандалозащищенный уличный корпус размером 120x60 мм, быстрая установка при помощи специальной монтажной пластины, IP67, -40 °C, IK10
Характеристики: разрешение 4 Мпкс, 1/3" OmniVision OV4689 CMOS + HiSilicon 3516D, фиксированный объектив 2,8 мм, угол обзора 90 град., 3DNR, D/N, D-WDR, BLC, ROI, детектор движения, приватные зоны, защита от саботажа, базовые функции видеоаналитики, поддержка ONVIF
Ориентировочная цена: 9990 руб.
Время появления на российском рынке: I квартал 2018 г.
Подробная информация: http://r1.infinity-cctv.ru/
Фирма, предоставившая информацию:
СТА ПЛЮС, ООО

VRF-IP3286PE

Производитель: INFINITY
Сертификат: информация не предоставлена
Назначение: 32-канальный IP-видеорегистратор
Особенности: 32 канала видео с разрешением до 8 Мпкс, питание 16 IP-камер по PoE, 8 жестких дисков объемом до 6 Тбайт
Возможности: профессиональный видеорегистратор для записи 32 сетевых видеокамер, 16 из которых могут быть напрямую подключены к регистратору и получать от него питание по PoE; возможность установки сразу восьми жестких дисков позволяет формировать объемный 48-террабайтный архив
Характеристики: 32 канала видео, макс. разрешение камер 8 Мпкс, 8 HDD x 6 Тбайт, H.265/H.264, ONVIF 2.6, видеовыходы HDMI и VGA, аудиовход/выход, 16 тревожных входов и 1 выход, выход eSATA, порт RS485, 3 порта USB, 1 порт управления 1000 Мбит/с Ethernet, 16 портов 10/100 Мбит/с Ethernet с поддержкой PoE для подключения камер, мощность PoE 7 Вт на порт, базовые функции видеоаналитики, детектор движения по каждому каналу
Ориентировочная цена: 53 990 руб.
Время появления на российском рынке: I квартал 2018 г.
Подробная информация: http://r1.infinity-cctv.ru/
Фирма, предоставившая информацию:
СТА ПЛЮС, ООО

Уличная 8 Мпкс IP-камера ActiveCam AC-D2183WDZIR5

Производитель: DSSL
Сертификат: ТС № RU Д-RU.МЛ66.В.00488, выдан испытательной лабораторией "Контроль-тест", ООО "НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ЦЕНТР"
Назначение: организация IP-видеонаблюдения внутри и снаружи помещений на объектах различного профиля
Особенности: моторизированный объектив; кодек H.265; Smart IR, Real WDR; высокое разрешение 8 Мпкс (3840x2160), ИК-подсветка до 50 м, степени защиты IP67, IK10
Возможности:
- автофокус
- внутренний видеоархив
- двусторонний аудиоканал
- ПО Trassir в комплекте

Характеристики:
- матрица 1/2.5" CMOS Sony STARVIS 8 Мпкс
- чувствительность: 0,002 лк (F1.4), 0 лк (F1.4, ИК вкл.)
- режим "день/ночь"
- механический ИК-фильтр (ICR)
- моторизованный объектив 2,7–12 мм, автофокус
- Real WDR 120 дБ
- шумоподавление 3D DNR
- компенсация засветки BLC/HLC
- функция "Антитуман" (Defog)
- ROI до 4 зон
- аппаратная видеоаналитика
- детектор лиц, обнаружение пересечения линии, вторжения в зону, оставленных/пропавших предметов, аудиодетекция
- стандарт сжатия H.265/H.264

Ориентировочная цена: 35 900 руб.
Время появления на российском рынке: ноябрь 2017 г.
Подробная информация: http://www.dssl.ru/products/ac-d2183wdzir5/
Фирма, предоставившая информацию:
ДССЛ, ООО

Вандалостойкая 6 Мпкс IP-камера ActiveCam AC-D3163WDZIR5

Производитель: DSSL
Сертификат: ТС № RU Д-RU.МЛ66.В.00488, выдан испытательной лабораторией "Контроль-тест", ООО "НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ЦЕНТР"
Назначение: организация IP-видеонаблюдения внутри и снаружи помещений на объектах различного профиля
Особенности: моторизированный объектив; кодек H.265; Smart IR, Real WDR; высокое разрешение 6 Мпкс (3072x2048), ИК-подсветка до 50 м, степени защиты IP67, IK10
Возможности:
- автофокус
- внутренний видеоархив
- двусторонний аудиоканал
- ПО Trassir в комплекте

Характеристики:
- матрица 1/2.9" CMOS Sony STARVIS 6 Мпкс
- чувствительность: 0,002 лк (F1.4), 0 лк (F1.4, ИК вкл.)
- режим "день/ночь"
- механический ИК-фильтр (ICR)
- моторизованный объектив 2,7–13,5 мм, автофокус
- Real WDR 120 дБ
- шумоподавление 3D DNR
- компенсация засветки BLC/HLC
- функция "Антитуман" (Defog)
- ROI до 4 зон
- аппаратная видеоаналитика
- детектор лиц, обнаружение пересечения линии, вторжения в зону, оставленных/пропавших предметов, аудиодетекция
- стандарт сжатия H.265/H.264

Ориентировочная цена: 27 900 руб.
Время появления на российском рынке: ноябрь 2017 г.
Подробная информация: http://www.dssl.ru/products/ac-d3163wdzir5/
Фирма, предоставившая информацию:
ДССЛ, ООО

Неуправляемый PoE-коммутатор TRASSIR TR-NS1010-96-8POE

Производитель: DSSL
Сертификат: ТС № RU Д-RU.МЛ66.В.00488, выдан испытательной лабораторией "Контроль-тест", ООО "НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ЦЕНТР"
Назначение: организация и построение локальных сетей на объектах с системой видеонаблюдения
Особенности: грозозащита; стандарты IEEE802.3, IEEE802.3u и IEEE802.3X., самонастройка MDI/MDIX, металлический корпус
Возможности: 8 PoE-портов 802.3af/802.3at, 2 порта Uplink, режим PoE до 250 м, Hi-PoE
Характеристики:
- порт Ethernet 2 Uplink-порта 10/100/1000 Мбит/с, 8 портов PoE 10/100 Мбит/с

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 151–152 "Ньюсмейкеры"

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 151–152 "Ньюсмейкеры"

- потребляемая мощность: 30 Вт (PoE-порты 2–8), 60 Вт (порт 1), 96 Вт (общая)
- протоколы PoE IEEE802.3af, IEEE802.3at, Hi-PoE
- коммутационная способность 5,6 Гбит/с
- скорость пересылки 4.17 млн пакетов в секунду
- буферная память для хранения пакетов 4 Мбайт
- размер таблицы MAC-адресов 16 000
- управление потоком – включено по умолчанию
- допустимая влажность 10–90%
- питание – адаптер питания 48–57 В (DC)
- грозозащита: 2 кВ (стандартный режим), 0,5 кВ (дифференциальный режим)
- рабочая температура от- 10 до +55 °С
- масса 0,49 кг
- размеры 190x100x30 мм

Ориентировочная цена: 8990 руб.
Время появления на российском рынке: январь 2018 г.
Подробная информация: http://www.dssl.ru/products/tr-ns1010-96-8poe/

Фирма, предоставившая информацию:
ДССЛ, ООО

Видеокамера сетевая BOLID VCI 320

Производитель: ЗАО НВП "Болид"
Сертификат: № RU C-RU.ME61.B.01256, выдан МНИТИ-СЕРТИФИКА
Назначение: для работы в составе комплекса видеонаблюдения и непрерывной трансляции видеоизображения с охраняемой зоны на системы отображения, записи, хранения и воспроизведения видеоизображения
Особенности:
- корпусная камера
- все современные функциональные опции на борту
- большой набор внутренней аналитики

Возможности: камера для решения нестандартных задач:
- где требуется качественная оптика, нестандартные телеобъективы, чувствительная матрица – например, протяженные периметры
- где требуется нестандартная защита корпуса камеры от внешних воздействий – от температуры (как низкой, так и высокой – например, в производственных цехах), от агрессивных сред (производства, морские порты, уличная дорожная сеть и т.п.), от радиации и т.п.
- где требуется наличие стеклоочистителя, стеклоомывателя для камеры
- это решается подбором объектива и кожуха под конкретную нестандартную задачу

Характеристики:
- цветная
- 2 Мпкс
- microSD
- аудиовход
- микрофон
- 12/24 В (DC/AC)
- PoE
- от -30 до +60 °С

Время появления на российском рынке: март 2017 г.
Подробная информация: https://bolid.ru/production/cctv/network_camera/case/vci_320.html

Фирма, предоставившая информацию:
БОЛИД, НВП, ЗАО

Видеокамера сетевая BOLID VCI 529

Производитель: ЗАО НВП "Болид"
Сертификат: № RU C-RU.ME61.B.01257, выдан МНИТИ-СЕРТИФИКА
Назначение: для работы в составе комплекса видеонаблюдения и непрерывной трансляции видеоизображения с охраняемой зоны на системы отображения, записи, хранения и воспроизведения видеоизображения
Особенности: высокоскоростная купольная антивандальная камера
Возможности: детальный обзор больших открытых территорий – площади, ангары, склады, периметр
Характеристики:
- цветная
- 2 Мпкс
- объектив 6–180 мм (x30 оптический zoom)
- ИК-подсветка (до 200 м)
- microSD
- аудиовход
- 24 В (AC), 3 А
- PoE
- IP67
- IK10
- от -50 до +70 °С

Время появления на российском рынке: апрель 2017 г.
Подробная информация: https://bolid.ru/production/cctv/network_camera/rotation/vci_529.html

Фирма, предоставившая информацию:
БОЛИД, НВП, ЗАО

Видеокамера сетевая BOLID VCI 722

Производитель: ЗАО НВП "Болид"
Сертификат: № RU C-RU.ME61.B.01256, выдан МНИТИ-СЕРТИФИКА
Назначение: для работы в составе комплекса видеонаблюдения и непрерывной трансляции видеоизображения с охраняемой зоны на системы отображения, записи, хранения и воспроизведения видеоизображения
Особенности:
- мини-купольная камера со встроенным микрофоном
- разрешение 2 Мпкс, фиксированный объектив

Возможности: камера предназначена для решения задач, при которых требуется малая заметность наблюдения, вандалостойкость, малые габариты оборудования, например подвалы, лестничные площадки, чердаки, вестибюли и т.п.
Характеристики:
- цветная
- 2 Мпкс
- объектив 2,8 мм
- ИК-подсветка (до 20 м)
- microSD
- микрофон
- 12 В (DC)
- PoE
- IP67
- от -30 до +60 °С

Время появления на российском рынке: март 2017 г.
Подробная информация: https://bolid.ru/production/cctv/network_camera/dome/vci_722.html

Фирма, предоставившая информацию:
БОЛИД, НВП, ЗАО

KEDACOM IPC2453-HNB-PIR30-L0360 (-L0600)

Производитель: KEDACOM (Китай)
Сертификат: KZ7500361.21.01.25617 серия KZ0013601, выдан испытательным центром ТОО "Казэкспоаудит"
Назначение: IP-видеокамера с ИК-подсветкой
Особенности: высокое разрешение (до 4 Мпкс) и четкая картинка; формат сжатия H265; высокая чувствительность, 0,03 лк (цв.), WDR/HLC/3D-шумоподавление
Возможности: компактный размер, интеллектуальные функции, встроенная высокоэффективная ИК-подсветка, поддержка карт microSD до 128 Гбайт и функции автоматического восстановления соединения (ANR), двойной поток (1080p + D1), специальное покрытие стекла для предотвращения запотевания, температурный режим от -40 до +70 °С, PoE, IP67
Характеристики:
- матрица 1/3" КМОП
- 4 Мпкс
- чувствительность: 0,03 лк (цв.), 0 лк (ч.-б. с ИК) 1–1/30 000 с
- автоматический режим "день/ночь"
- цифровой WDR (DWDR)
- сигнал/шум >50 дБ
- баланс белого авто/ручной
- улучшение изображения выкл./WDR/BLC/HLC
- крепление объектива M12
- фокусное расстояние 3,6 мм (6 мм)
- угол обзора 78,6/53,2 град.
- дальность ИК-подсветки 30 м
- тип ИК-подсветки Smart IR
- формат сжатия H265/H264/MJPEG
- питание 12 В (DC) ± 10%/PoE (IEEE802.3af)
- потребляемая мощность до 7 Вт
- масса 0,6 кг
- размеры 161,5x62x57 мм
- кронштейн в комплекте

Ориентировочная цена: 9000 руб.(рекомендованная розничная)
Время появления на российском рынке: ноябрь 2017 г.
Подробная информация: http://ru.kedacom.com/products/ip-camery/%D1%86%D0%B8%D0%BB%D0%B8%D0%BD%D0%B4%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5/%D1%84%D0%B8%D0%BA%D1%81%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5/ipc2453-hnb-pir30-l0600-detail.html

Фирма, предоставившая информацию:
ВИДЕОКОНТРОЛЬ, ООО

SkyHawk AI

Производитель: Seagate Technology
Сертификат: информация не предоставлена
Назначение: жесткий диск для систем видеонаблюдения с искусственным интеллектом
Особенности: диск разработан специально для систем видеонаблюдения с технологией искусственного интеллекта, работающей на периферии и внутри сети
Возможности: накопитель обеспечивает мгновенный отклик и превосходную скорость произвольного чтения, необходимую для быстрого поиска и анализа видеозаписей. Оснащен микропрограммой Seagate ImagePerfect AI, записывает высококачественное видео высокого разрешения без пропуска кадров
Характеристики:
- оптимизация под системы видеонаблюдения с искусственным интеллектом
- обслуживание до 64 камер высокого разрешения
- макс. скорость передачи данных 214 Мбит/с
- емкость до 10 Тбайт

Ориентировочная цена: 25 000 руб.
Время появления на российском рынке: август 2016 г.
Подробная информация: https://www.seagate.com/gb/en/internal-hard-drives/hdd/skyhawk/
Фирма, предоставившая информацию:
SEAGATE TECHNOLOGY

CD310-4G

Производитель: "НПП "Бевард"
Сертификат: сертификат отсутствует
Назначение: обеспечение беспроводного облачного видеонаблюдения
Особенности: передача видео по сетям 4G, датчик движения, с отправкой сообщений при активации по SMS или e-mail
Возможности: съемка в полной темноте: встроенный PIR-датчик и ИК-подсветка; встроенный активный микрофон дальностью до 10 м, объектив 2,5/2,8/3,6/8/12/16 мм на выбор
Характеристики:
- 1 Мпкс, КМОП 1/4"
- чувствительность 0,3 лк (день)/0,1 лк (ночь)
- 1280x720 (HD) @ 2 5 кадр/с
- проводное питание 5 В

Время появления на российском рынке: I квартал 2018 г.
Подробная информация: https://www.beward.ru/katalog
Фирма, предоставившая информацию:
БЕВАРД, НПП, ООО

CD330

Производитель: "НПП "Бевард"
Сертификат: сертификат отсутствует
Назначение: облачная Wi-Fi-камера
Особенности:
- передача видео по Wi-Fi
- встроенный PIR-датчик, с отправкой сообщений при активации по SMS или e-mail

Возможности: съемка в полной темноте: встроенный PIR-датчик и ИК-подсветка; встроенный активный микрофон дальностью до 10 м, объектив 2,5/2,8/3,6/8/12/16 мм на выбор
Характеристики:
- 1 Мпкс, КМОП 1/4"
- чувствительность 0,3 лк (день)/0,1 лк (ночь)
- 1280x720 (HD) @ 25 кадр/с
- проводное питание 5 В

Время появления на российском рынке: I квартал 2018 г.
Подробная информация: https://www.beward.ru/katalog
Фирма, предоставившая информацию:
БЕВАРД, НПП, ООО

DS06M

Производитель: "НПП "Бевард"
Сертификат: сертификат отсутствует
Назначение: SIP-домофон с встроенным распознаванием лиц
Особенности: распознавание лиц доступно без приобретения серверов, установки дополнительного ПО и покупки лицензий; эта функция будет бесплатно доступна на ранее приобретенных домофонах DS06M после установки соответствующего обновления
Возможности:
- встроенная база на 30 фотографий
- антивандальное исполнение
- качественная двухстороння аудиосвязь
- ИК-подсветка до 10 м

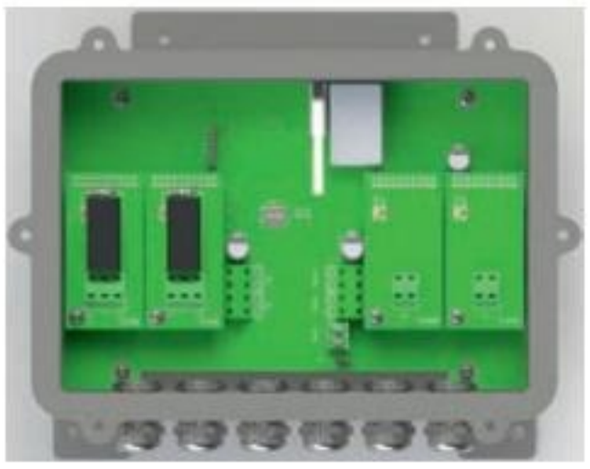
Характеристики:
- 1,3 Мпкс, 1/3" SONY Exmor
- чувствительность 0,01 лк (день)/0,003 лк (ночь)
- 1280x960 @ 25 кадр/с
- питание 12 В (DC)
- антивандальный

Ориентировочная цена: 14 300 руб.
Время появления на российском рынке: I квартал 2018 г.
Подробная информация: https://www.beward.ru/katalog/ip-videodomofony/vyzyvnye-paneli/vyzyvnaya-panel-ds06m/
Фирма, предоставившая информацию:
БЕВАРД, НПП, ООО

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 151–152 "Ньюсмейкеры"

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ. ПЕРИМЕТРОВЫЕ СИСТЕМЫ

Блок линейный периметровый ТРЕЗОР-БЛ



Производитель: ООО "Научно-производственный центр "Трезор"
Сертификат: изделие подлежит сертификации
Назначение: для работы в составе системы охранной сигнализации периметра
Особенности:
- модульная конструкция
- уличное исполнение
- возможность автономной работы
- настройка при помощи программного обеспечения

Возможности:
- работает в составе системы охранной сигнализации периметра ТРЕЗОР
- подключение сторонних периметровых извещателей с выходом типа "сухой контакт" (плата входа)
- управление охранным освещением и исполнительными устройствами (плата выхода)
- полноценная интеграция по RS-485 (открытый протокол) для работы в составе интегрированной системы безопасности объекта

Характеристики:
- до 4 плат входа и выхода (250 В (AC), 3 А)
- интерфейс RS-485
- выходы для питания сторонних извещателей 12 В (100 мА) и 24 В (50 мА)
- уличное исполнение IP65
- диапазон рабочих температур от -60 до +60 °С
- напряжение питания от 10 до 30 В (DC)
- потребляемый ток не более 50 мА, 24 В (без учета плат входа и выхода)

Ориентировочная цена: 25 000 руб.
Время появления на российском рынке: март 2018 г.
Подробная информация: http://trezorrussia.ru/каталог/
Фирма, предоставившая информацию:
ТРЕЗОР, НПЦ, ООО

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Адреса и телефоны фирм, предоставивших информацию, см. на стр. 151–152 "Ньюсмейкеры"

DHI-VTO9231D

Производитель: Dahua Technology
Сертификат: RU C-CN.ИМ43.В.00437, выдан "ТехИмпорт"
Назначение:
- открытие замка паролем, картой, отпечатком пальца или дистанционно
- запись журналов вызовов, тревог, открываний дверей
- вызов домофона, вызов на пульт консьержа

Особенности:
- 10" IPS-дисплей
- 2 Мпкс CMOS-видеокамера
- алюминиевый сплав, класс защиты IP54
- подсветка в ночное время
- врезной монтаж
- поддержка SIP-протокола

Возможности:
- работа с несколькими видеодомофонами
- возможность подключения IP-видеокамер
- возможность интеграции с охранной сигнализацией

Характеристики:
- дисплей 10" TFT 800x1280
- видео: сжатие H.264; матрица 1/3" 2 Мпкс CMOS; фокусное расстояние объектива 3,6 мм; угол обзора 135 град. (по диагонали), 115 град. (по горизонтали); режим "день/ночь", цветное изображение
- аудио: сжатие G.711; всенаправленный микрофон, встроенный динамик
- сенсорные кнопки
- считыватель карт Mifare, отпечатков пальцев; дистанция распознавания 1 м
- тревожные входы/выходы 2/2
- входы/выходы Wiegand 1/1
- питание 12 В (DC)
- потребление: до 8 Вт (в режиме ожидания); до 30 Вт (в режиме работы)
- диапазон рабочих температур от -20 до +60 °C
- класс защиты IP54
- материал алюминий; закаленное стекло; врезной монтаж
- размеры 475x174x58 мм
- масса 2 кг

Время появления на российском рынке: 2018 г.

Фирма, предоставившая информацию:
DAHUA TECHNOLOGY RUS LLC

ST-NC441

Производитель: Smartec
Сертификат: ТС № RU Д-GB.АЛ16.В.47523, выдан испытательной лабораторией "ЛСМ" ООО "Трансконсалтинг"
Назначение: сетевой контроллер СКУД
Особенности:
- 2 Ethernet-порта, работающих в качестве повторителя
- свободно программируемые входы/выходы
- 12 контролируемых входов
- 6 релейных выходов

Возможности:
- поддержка до 4 дверей или 2 турникетов
- поддержка считывателей Wiegand 26 и Wiegand 34
- виды идентификации: карта, код, карта и код, карта или код
- автономный режим работы

Характеристики:
- пользователей: 100 000
- событий: 100 000
- временных зон: 256
- уровней доступа: 5000
- пункты доступа: до 4 дверей или 2 турникетов
- считыватели: 4
- входы/выходы: 12/6, свободно программируемые
- интерфейсы связи: 2 порта TCP/IP (режим повторителя)
- вход считывателя: Wiegand 26, Wiegand 34, ПИН 8 бит
- релейные выходы: НЗ/НР; 36 В (DC), 5А/30 В (AC), 8 А
- питание 9–14 В (DC), не более 650 мА (без учета считывателей)
- диапазон рабочих температур от 0 до +55 °C без конденсации
- диапазон рабочей влажности 10–80%
- габариты 180x120x21 мм
- опции: ST-AC001BX – монтажный бокс

Ориентировочная цена: 240 долл.
Время появления на российском рынке: ноябрь 2017 г.
Подробная информация:
www.smartec-security.ru

Фирма, предоставившая информацию:
АРМО-СИСТЕМЫ

А

ААМ СИСТЕМЗ

111250, Москва, Е-250,
ул. Красноказарменная, 14
Тел.: +7 (495) 921-2227
(многоканальный)
Факс: +7 (495) 362-7262
E-mail: aam@aamsystems.ru
www.aamsystems.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 20

АРГУС-СПЕКТР, ООО

197342, Санкт-Петербург,
ул. Сердобольская, 65, лит. А
Тел.: +7 (812) 703-7500
Факс: +7 (812) 703-7501
E-mail: mail@argus-spectr.ru
www.argus-spectr.ru, стрелец.рф
См. стр. 114, 115

АРМО-СИСТЕМЫ

125167, Москва,
Ленинградский просп., 37А, корп. 14
Тел.: +7 (495) 787-3342
Факс: +7 (495) 937-9055
E-mail: armosystems@armo.ru
www.armosystems.ru
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 41
См. ст. "Дальнобойная" парковочная СКУД: бюджетный комфорт" на стр. 133
См. 4-ю обл.

АСТРОН, ОКБ, АО

140080, г. Лыткарино Московской обл.,
ул. Парковая, 1
Тел/факс: +7 (495) 374-5388
E-mail: sales@astrohn.ru
www.astrohn.ru
См. стр. 61

Б

БЕВАРД, НПП, ООО

117198, Москва,
ул. Миклухо-Маклая, влад. 8, стр. 3
Тел.: +7 (495) 505-6341,
+7 (391) 278-9200
Факс: +7 (391) 278-9202
E-mail: moscow@beward.ru
www.beward.ru
См. клапан на 1-й обл.
См. стр. 69
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 42

БИК-ИНФОРМ, ООО

190020, Санкт-Петербург,
ул.Бумажная, 9, корп. 1
Тел.: +7 (812) 447-9555
Факс: +7 (812) 447-9556
E-mail: bic@bic-inform.ru
www.bic-inform.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 22

БОЛИД, НВП, ЗАО

141070, г. Королев Московской обл.,
ул. Пионерская, 4
Тел/факс: +7 (495) 775-7155
E-mail: info@bolid.ru
www.bolid.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 23
См. ст. "Расширение линейки видеонаблюдения компании BOLID: что нового?" на стр. 82, 83

В

ВИДЕОКОНТРОЛЬ, ООО

121170, Москва,
Кутузовский просп., 36, стр. 8
Тел/факс: +7 (499) 130-0115
E-mail: zakaz@video-control.pro
www.video-control.pro
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 40

Д

ДИСТРИБЬЮТОРСКИЙ ЦЕНТР СТА, ООО

Тел.: +7 (495) 221-0821
Факс: +7 (495) 221-0820
E-mail: info@sta.ru
www.sta.ru
www.infinity-cctv.ru
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 41
См. стр. 87
См. стр. 101

дормакаба Евразия, ООО

117036, Москва,
ул. Дмитрия Ульянова, 7а
Тел.: +7 (495) 966-2050
E-mail: russia@dormakaba.com
www.dorma.ru
См. ст. "Решения dormakaba для спортивных объектов: высочайший уровень безопасности и комфорта" на стр. 119
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. 11
См. анонс на стр. 17
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 42
См. стр. 53
См. стр. 81

И

ИНТЕГРА-С, КОНСОРЦИУМ

115230, Москва, Варшавское ш., 46
Тел.: +7 (495) 730-6252,
(846) 951-9601
Факс: +7 (495) 730-6252
E-mail: zaovolga@integra-s.com
www.integra-s.com/
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 19

НЬЮСМЕЙКЕРЫ

П

ПРОСОФТ-БИОМЕТРИКС, ООО

620149, Екатеринбург,
ул. Зоологическая, 9
Тел.: (800) 770-0246,
+7 (343) 270-2333
E-mail: sale@bio-smart.ru
www.bio-smart.ru
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 38

Р

РОСТЕВРОСТРОЙ, ПК, ООО

344111, Ростов-на-Дону,
просп. 40-летия Победы, 306А
Тел.: +7 (863) 206-1686, 269-9938
Факс: +7 (863) 206-1686, 269-9937
E-mail: 2699935@rostovturniket.ru
www.rostovturniket.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 22

Т

ТРЕЗОР, НПЦ, ООО

105318, Москва,
ул. Ибрагимова, 31, корп. 47
Тел.: +7 (495) 663-9596,
+7 (929) 663-9596
Факс: +7 (495) 663-9596 #102
E-mail info@trezorrussia.ru
http://trezorrussia.ru
См. анонс на стр. 15

Ц

ЦЕСИС НИКИРЭТ, ЗАО (ЦЕНТР СПЕЦИАЛЬНЫХ ИНЖЕНЕРНЫХ СООРУЖЕНИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО И КОНСТРУКТОРСКОГО ИНСТИТУТА РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ)

440013, Пенза, ул. Чаадаева, 62
Тел.: +7 (8412) 37-4048
(служба продаж)
Тел/факс: +7 (8412) 37-4050
(секретарь)
E-mail: info@cesis.ru,
snabsbit@cesis.ru
www.cesis.ru
www.cesis-proekt.ru
См. стр. 97

A

AHI CARRIER FZC

121059 Москва,
ул. Киевская, 7, вход 7, этаж 2
Тел.: +7 (495) 937-4241, доб. 272
Факс: +7 (495) 937-1890
E-mail: alexander.barsukov@ahi-carrier.ru
www.utcfssecurityproducts.eu,
www.ahi-carrier.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 20
См. стр. 107

AXIS COMMUNICATIONS, ООО

125284, Москва, Ленинградский
просп., 31А, стр. 1, этаж 16
Тел/факс: (495) 940-6682
www.axis.com
См. 2-ю обл.

D

DAHUA TECHNOLOGY RUS LLC

115280, Москва,
ул. Ленинская Слобода, 19, этаж 5,
комната 21
Тел.: +7 (499) 682-6000
E-mail: info@dahuasecurity.pro
http://dahuasecurity.pro/
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 40
См. стр. 65

P

PANASONIC

115191, Москва,
ул. Большая Тульская, 11
Тел.: +7 (495) 665-4205
Факс: +7 (495) 665-4224
E-mail: info@ru.panasonic.com
panasonic.com
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 39

PERCO

194021, Санкт-Петербург,
ул. Политехническая, 4,
корп. 2, стр. 1
Тел.: 8 (800) 333-5253,
+7 (812) 247-0457
E-mail: market@perco.ru
www.perco.ru
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 21
См. СПЕЦПРОЕКТ ТРАНСПОРТ на стр. 39

S

SEAGATE TECHNOLOGY

125284, Москва,
ул. Беговая, 3, стр. 1
(филиал частной компании
с ограниченной ответственностью
"Сигейт Текнолоджи Ю-Кей ЛТД.",
Великобритания)
E-mail: Pr.emea@seagate.com
www.seagate.com/ru/ru/
См. СПЕЦПРОЕКТ ЛУЧШИЕ ПРОДУКТЫ 2018 на стр. 19

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. стр. 89, 90

СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Мы предлагаем комплексные решения контроля и управления доступом.
От одного поставщика.

Ключи и цилиндры

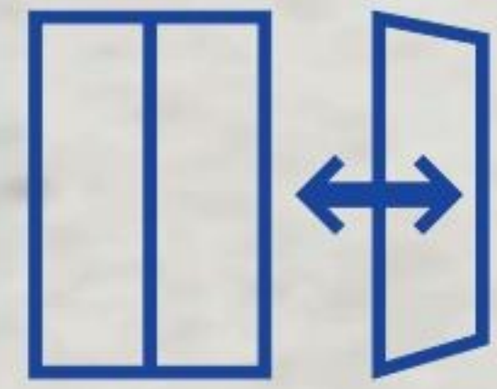
Дверная техника
и фурнитура

Системы крепления
стекла

Автоматические двери
и турникеты

Отельные системы

Системы контроля
доступа



Мобильные стены

Сервис

Консалтинг

01 июля 2016 года компании DORMA и KABA объединились в компанию dormakaba.
Мы разрабатываем, производим и поставляем комплексные дверные решения, интеллектуальные системы контроля доступа и эвакуации.
Проектируем, обеспечиваем монтаж и сервис.
dormakaba - сохраняем жизни

www.dormakaba.com
8-800-250-15-76

dormakaba

Надежный поставщик оборудования и решений по безопасности

20%
ежегодный прирост клиентов

20 лет
на рынке систем безопасности

гарантии
от 50
вендоров

ОПЫТ УНИКАЛЬНЫХ ПРОЕКТОВ
для многопрофильных предприятий, нефтегазовых комплексов и транспортных узлов

армо-системы

- видеонаблюдение
- охранно-пожарная сигнализация
- контроль доступа
- системы оповещения

Москва
+7 (495) 787-33-42
Санкт-Петербург
+7 (812) 303-53-53
Екатеринбург
+7 (343) 372-72-27

E-mail:
armosystems@armo.ru

armosystems.ru