

Журнал для руководителей предприятий и специалистов отрасли безопасности

№5(32)
сентябрь-октябрь
2013

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ



Основные вопросы и порядок подтверждения соответствия продукции требованиям технических регламентов Таможенного союза

Технический регламент Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения»

Нормативное обеспечение создания и применения систем видеонаблюдения

Проектирование, монтаж, наладка средств и систем пожарной автоматики и охранной сигнализации. Вопрос-ответ

Банковская безопасность

Системы контроля управления доступом

Нормативное регулирование

Безопасность банковско-финансовой сферы: актуальные вопросы, проблематика в сегменте

СКУД в Республике Беларусь: новинки, обзор систем, проекты

Системы видеонаблюдения

Пожарная безопасность

Обеспечение комплексной информационной безопасности АСУ ТП: опыт российских компаний



LG SECURITY SYSTEM



ул. Машиностроителей,
29-117 (5-й этаж),
г. Минск, 220118,
Беларусь

tel.: +375 (17) 341 50 50
MTS: +375 (29) 541 50 50
Vel.: +375 (29) 641 50 50

info@secur.by
www.secur.by

официальный дистрибутор LG Electronics в РБ по направлению
ПРОФЕССИОНАЛЬНЫЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

ОДО «СФЕРАТРЭЙД»
группа компаний «Сфера»

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, № 5 (32)–2013
В НОМЕРЕ:

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

Подтверждение соответствия требованиям технических регламентов Таможенного союза 4
Гальперина Евгения, заместитель главного редактора журнала «Технологии безопасности»

Технический регламент Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» 7
Шатило Эдуард Эдуардович, начальник учреждения «Республиканский центр сертификации и экспертизы лицензируемых видов деятельности» МЧС Республики Беларусь, полковник внутренней службы

Нормативное обеспечение создания и применения систем видеонаблюдения 9

Проектирование, монтаж, наладка средств и систем пожарной автоматики и охранной сигнализации (вопрос-ответ) 11
Вопросы по ТКП 472-2013(02010) «Правила технического обслуживания технических систем охраны», ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений»

БЕЗОПАСНОСТЬ БАНКОВСКО-ФИНАНСОВОЙ СФЕРЫ

Безопасность банковско-финансовой сферы 13
Дубков Сергей Витальевич, заместитель председателя правления Национального банка Республики Беларусь

Актуальность выработки методик и ознакомления с технологиями расследования инцидентов в системах электронных платежей 16
Денисов Денис Валерьевич, Главное управление единого расчетного и информационного пространства. Эксперт по информационной безопасности, защите информации в банковской сфере, противодействию мошенничеству в области электронных платежей

Индикаторы несанкционированного доступа 20
ООО «Смарт Бизнес Технолоджи»

СКУД ЭКСПЕРТЫ

Рынок СКУД в РБ – экспертные комментарии 22

НОВОСТИ

Изменения в лицензионных правах на использование авторского программного продукта «ВОРОН-НЕЙРО» 27
ООО «Прикладная радиофизика»

СКУД

Шлюзовая кабина рентгеновского досмотра – инновационная технология контроля доступа посетителей 28
УП «АДАНИ»

СКУД на базе оборудования «Болид»: сегодня и завтра ... 29
ЗАО НВП «Болид»

Построение распределенной СКУД для офисов крупной компании 32
Парсиев Дмитрий, директор ООО «Видео-СКУД»

«WEB-офис» – новое поколение IP-СКУД 34
ООО «Видео-СКУД»

Развитие САП 777 «КомплексПаркинг» 35
Петлицкий Александр, заместитель директора по технике ООО «РОВАЛЭНТКОМПЛЕКС»

СКУД без проводов: идеи, реализации, перспективы 38
ООО «Легион безопасности»

Система контроля и управления доступом в зданиях Банка 43
ООО «Совершенные системы»

Построение СКУД распределенных объектов на базе оборудования GeoVision 48
ООО «Спецэлектро Лтд»

Интеллектуальные решения безопасности CEM Systems . 50
СП ООО «Унибелус»

Системы контроля и управления доступом, представленные на рынке Беларуси, 2013 (сводная таблица) 52

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Мегапиксельное качество аналогового видео. Технология 960H от HIKVISION 58
ОДО «АВАНТ-ТЕХНО»

ПОЖАРНАЯ БЕЗОПАСНОСТЬ

Опыт применения оборудования системы «ИНТЕГРАЛ» (практика применения в Республике Беларусь) 61
НПО «КЛАСКОМ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Обеспечение комплексной информационной безопасности АСУ ТП: опыт российских компаний 65
Тимошенко Андрей Борисович, начальник отдела консалтинга департамента консалтинга и аудита компании «Информзащита»

СПРАВОЧНАЯ ИНФОРМАЦИЯ

Новинки рынка 69
Информация о компаниях 74



ОФИСТЕХНИКА

Уничтожители документов HSM®
made in GERMANY гарантия 2 года

www.officetehnika.by

Минск: (017) 289-78-54

(029) 193-23-24 (моб)

Витебск: (0212) 36-27-35, 36-27-65

Гродно: (0152) 54-25-99

On-line (ICQ) консультац.: 260821693



Уничтожаем

бумажные документы
карточки
диски
флэшки
жесткие диски



Мы научили документы молчать

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»

Производственно-практический журнал
№ 5 (32), октябрь-ноябрь, 2013

Периодичность выхода: 1 раз в 2 месяца

Учредитель и издатель:

ООО «АэркомБел»

Главный редактор:

Сергей Адамович Драгун

Над номером работали:

Лисенкова Анна

Карпук Мария

Журнал зарегистрирован
в Министерстве информации
Республики Беларусь
Свидетельство о регистрации
№ 846 от 10.12.2009

Адрес редакции:

220073, г. Минск, ул. Гусовского, 6,
оф. 2.15.2
Тел./факс: (017) 290-84-05

Отдел рекламы:

Тел./факс: (017) 290-84-05,
256-10-35, 256-10-47
e-mail: info@aercom.by
www.aercom.by

Отдел подписки:

Тел./факс: (017) 290-84-05
e-mail: podpiska@aercom.by

Подписка через РУП «Белпочта»:

01248 — для индивидуальных
подписчиков;

012482 — для предприятий и организаций.

Цена 77500 бел. руб. без НДС,
на основании п. 3.12 ст. 286
Особенной части Налогового Кодекса
Республики Беларусь

Подписано в печать — 19.12.2013 г.

Формат: 60х90 1/8

Бумага офсетная

Гарнитура Myriad Pro. Печать офсетная

Усл. печ. л. 10; Уч.-издл. 10,8

Тираж: 800 экз.

Заказ _____

Отпечатано в типографии
ООО «Юстмаж»

Адрес типографии: г. Минск,
ул. Калиновского, д.6, Г 4/К, комн. 201
Лиц. ЛП № 02330/0552734 от 31.12.2009,
Министерство информации РБ

Издатель не несет ответственности за
достоверность рекламных материалов.

*Воспроизведение материалов, опубликованных
в журнале «Технологии безопасности»,
допускается только с письменного разреше-
ния редакции. При использовании ссылка на
журнал обязательна.*

*Мнение редакции не всегда совпадает с мнени-
ем авторов статей.*

*Материалы, опубликованные со значком R,
являются рекламными.*

ISSN 2221-8661



СЛОВО РЕДАКТОРА



В 2014 году банковский сегмент Беларуси будет одним из самых крупных потребителей средств и систем безопасности, причем как информационной, так и инженерно-технической. Главные стимулы – развитие системы безналичных платежей и филиальных сетей. Важный момент – понимание руководством Национального банка проблематики и защита собственных корпоративных интересов перед структурами, обеспечивающими безопасность банковского сегмента. Можно констатировать, что банковская безопасность одна из первых подошла к решению и пониманию проблем безопасности как к комплексному подходу.

В этом номере представляем обзор рынка СКУД в нашей стране. Потенциальный заказчик может ознакомиться с новыми разработками и спектром предложений на рынке.

Ключевые моменты развития СКУД Беларуси:

- Стабильный, сформировавшийся рынок с устоявшимися игроками. Представлены системы как международных ТМ, так и местных производителей. Рынок характеризуется малым присутствием азиатских производителей;

- Основа рынка – государственный сектор 70% запросов, 30% – коммерческие предприятия;

- Происходит активное внедрение СКУД в системы жизнедеятельности предприятия. Заказчиком все больше предъявляются требования к интеграции СКУД с СВН, ПС, ОС и пр. системами;

- Переход СКУД на IP-технологии, интерес заказчика и готовность белорусских интеграторов к созданию сетевых распределенных СКУД (пока единичные проекты);

- Технологии идентификации. Пока самой распространенной на рынке остается пластиковая карта с чипом EM-Marip. Рост в 2013 году количества проектов с использованием систем биометрической идентификации;

- С точки зрения коммерческого интереса и бюджетов на 2014 год, сегмент СКУД перспективен для монтажных компаний и интеграторов при условии грамотных предложений по интеграции и глубокому внедрению СКУД в процессы предприятий.

Благодарим участников номера за профессиональное содействие в подготовке материалов.

Готовится новый номер журнала: «Итоги отрасли безопасности». В номере:

- Обзор, перспективы развития отрасли безопасности в 2014 году. Тенденции, участники рынка, технические решения.

- Техническое регулирование в рамках Таможенного союза.

Нормативное регулирование сегмента пожарной безопасности в 2014 году.

- Тактика и стратегия развития Департамента охраны МВД Республики Беларусь.

- Нормативное регулирование сегмента систем видеонаблюдения в Республике Беларусь.

- Обзор знаковых проектов за 2013 год.

Приглашаем к участию компании и специалистов.

**С уважением, Драгун Сергей Адамович,
главный редактор журнала.**

20-я международная выставка и конференция

ОХРАНА, БЕЗОПАСНОСТЬ И ПРОТИВОПОЖАРНАЯ ЗАЩИТА



Mips

OSCOV

14–17 АПРЕЛЯ 2014 ГОДА
МОСКВА, ВВЦ, ПАВИЛЬОН 75



01010010111110101010010101010
0111111010101001010101010101001010010111110101010010101010
11101010100100010101010101010101010010000010111110101010010101001011110101010010010101010
0001011111101010100101010101010100101010010111110101010010101010
001110101001000101010100101010100100100000101111101010100101010101001010111101010100101010



Охранное
телевидение
и наблюдение



Технические
средства
обеспечения
безопасности



Системы
защиты
периметра.
Ограждения



Пожарная
безопасность.
Аварийно-
спасательная
техника.
Охрана труда



Смарт карты



Организатор:



Тел.: +7 (495) 935 7350
Факс: +7 (495) 935 7351
security@ite-expo.ru

При поддержке:



МВД России

www.mips.ru



ЕАС Подтверждение соответствия требованиям технических регламентов Таможенного Союза

Принятие технических регламентов Таможенного Союза (далее – ТР ТС) в области электротехники и радиоэлектроники поставило перед импортерами и производителями таких изделий новую задачу – подтверждение соответствия обязательным требованиям ТР ТС для легального размещения продукции на рынке Республики Беларусь, Казахстана и Российской Федерации. Существенные трудности при решении этих задач возникли у субъектов хозяйствования, чьи изделия ранее не подлежали обязательному подтверждению соответствия на национальном уровне.



Евгения Гальперина,
заместитель главного
редактора журнала
«Технологии безопасности»

Справка ТБ

Евгения Гальперина, образование высшее, в 2006 году окончила Минский институт управления, факультет правоведения. С 2006 по 2008 год работала в юридической компании, специализировалась на регистрации субъектов хозяйствования, лицензировании, сертификации. С 2008 г. работает в компании «АэркомБел», основная специализация – нормативное обеспечение отрасли безопасности.

Электротехника и радиоэлектроника частично или полностью являются объектом регулирования следующих технических регламентов Таможенного Союза:

- ТР ТС 004/2011 «О безопасности низковольтного оборудования»;
- ТР ТС 010/2011 «О безопасности машин и оборудования»;
- ТР ТС 012/2011 «О безопасности оборудования для работы во взрывоопасных средах»;
- ТР ТС 016/2011 «О безопасности аппаратов, работающих на газообразном топливе»;

- ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

В целях детального рассмотрения области применения ТР ТС и возможных процедур подтверждения соответствия, компания ООО «АэркомБел» в ноябре текущего года организовала информационно-практический семинар «Основные вопросы и порядок подтверждения соответствия продукции требованиям ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и ТР ТС 004/2011 «О безопасности низковольтного оборудования». В семинаре приняли участие: начальник отдела технического нормирования и стандартизации в электротехнике и радиоэлектронике БелГИСС, начальник отдела сертификации БелГИМ, начальник отдела государственного надзора и контроля Госстандарта, инспекторы отдела организации таможенного регулирования Минской региональной таможни.

В данной статье будут изложены основные тезисы семинара, основанные на выступлениях должностных лиц, для формирования общего понимания вопросов при легализации товара на рынке Беларуси и возможной ответственности за нарушение предусмотренного порядка обращения товара.

Действие ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и ТР ТС 004/2011 «О безопасности низковольтного оборудования».

Оба регламента вступили в силу с 15.02.2013 г. С этой даты выдача или принятие документов об оценке (подтверждении) соответствия товара обязательным требованиям, ранее установленным национальным законодательством государств-членов Таможенного союза или нормативными правовыми актами Таможенного союза, не допускается. Документы об оценке (подтверждении) соответствия обязательным требованиям,



установленным национальным законодательством государств-членов Таможенного союза или нормативными правовыми актами Таможенного союза, выданные на продукцию до 15.02.2013 г. действительны до окончания срока их действия, но не позднее 15.03.2015 г.

Согласно Решению Коллегии ЕЭК №247 от 04.12.2012 г. до 15.11.2013 г. допускалось производство и выпуск в обращение на таможенной территории Таможенного союза продукции, не подлежавшей до дня вступления в силу рассматриваемых ТР ТС обязательной оценке (подтверждению) соответствия обязательным требованиям, установленным нормативными правовыми актами Таможенного союза или законодательством государства – члена Таможенного союза, без документов об обязательной оценке (подтверждении) соответствия и без маркировки национальным знаком соответствия (знаком обращения на рынке).

Область применения ТР ТС 004/2011 и ТР ТС 020/2011 подробно изложена в статье 1 каждого регламента.

Перечни объектов технического регулирования, подлежащих подтверждению соответствия требованиям ТР ТС, в форме **сертификации** указаны соответственно в Приложении к ТР ТС 004/2011 и в Приложении №3 к ТР ТС 020/2011. Продукция, не перечисленная в указанных приложениях, но входящая в область применения ТР ТС, подлежат подтверждению соответствия в форме **декларирования соответствия**.

Перечни стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований ТР ТС, утверждены решениями Комиссии Таможенного союза от 25 декабря 2012 г. № 292 (ТР ТС 004/2011) и от 9 декабря 2011 г. №879 (ТР ТС 020/2011).

Выбор схемы декларирования соответствия товара осуществляется изготовителем (уполномоченным изготовителем лицом), импортером. По решению изготовителя (уполномоченного изготовителем лица), импортера подтверждение соответствия товара, подлежащего декларированию, может осуществляться в форме сертификации. В случае неприменения стандартов, указанных в Перечне стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований ТР ТС 004/2011 и 020/2011, или при их отсутствии, подтверждение

Решением Коллегии ЕЭК №91 от 24.04.2013 г. установлен перечень продукции, в отношении которой подача таможенной декларации сопровождается представлением таможенному органу документа об оценке (подтверждении) соответствия требованиям ТР ТС 004/2011. В настоящее время ведется работа по актуализации данного перечня и подготовке аналогичного перечня для ТР ТС 020/2011. Планируется расширить данные перечни за счёт включения не только изделий, подлежащих сертификации (в этом случае приводится исчерпывающая номенклатура продукции, входящей в область применения ТР ТС), но и наиболее важных и массовых изделий, подлежащих подтверждению соответствия требованиям ТР ТС в форме декларирования (ограниченный перечень). Утверждение данных Коллегией Евразийской экономической комиссии (далее – ЕЭК) ожидается в январе-феврале 2014 года.

соответствия изделия осуществляется в форме **сертификации**.

На момент публикации материала БелГИСС подготовлены методические рекомендации по применению технического регламента Таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования». В настоящее время этот документ одобрен Госстандартом Республики Беларусь и направлен на рассмотрение в ЕЭК, Россию и Казахстан.

Порядок подтверждения соответствия требованиям ТР ТС

После определения формы и выбора схемы подтверждения соответствия рассмотрим основные моменты в процедуре (порядке) подтверждения соответствия. Работы по подтверждению соответствия проводят органы по сертификации, аккредитованные в ТС на проведение таких работ по конкретным видам продукции (наименование, код ТН ВЭД).

Единый реестр органов по сертификации и испытательных лабораторий (центров) Таможенного союза приведен на сайте <http://www.gosstandart.gov.by> (раздел «Таможенный союз»).

Сам порядок подтверждения соответствия продукции требованиям ТР ТС 004/2011 и ТР ТС 020/2011 подробно изложен в статье 7 каждого регламента.

Описание типовых схем подтверждения соответствия, включая процедуры и пакеты документов, изложены в Положении о порядке применения типовых схем оценки (подтверждения) соответствия требованиям тех-

нических регламентов Таможенного союза, утвержденном Решением Комиссии Таможенного союза от 7 апреля 2011 года №621.

В отличие от процедур сертификации, осуществляемых аккредитованным органом по сертификации, декларирование соответствия осуществляется непосредственно заявителем. Единая форма декларации о соответствии требованиям технического регламента Таможенного союза и правила ее оформления утверждены Решением Коллегии Евразийской экономической комиссии от 25 декабря 2012 г. №293. Порядок регистрации декларации определен Положением о регистрации деклараций о соответствии продукции требованиям технических регламентов Таможенного союза (Реш. Коллегии ЕЭК от 9 апреля 2013 г. №76). Указанные документы находятся в свободном доступе на сайте <http://www.gosstandart.gov.by> (раздел «Таможенный союз»).

При декларировании соответствия, заявителем могут выступать зарегистрированные на территории государства-члена ТС (в соответствии с законодательством этого государства) юридическое лицо или физическое лицо в качестве индивидуального предпринимателя, являющиеся изготовителем или продавцом, либо выполняющие функции иностранного изготовителя на основании договора с ним (далее – заявитель).

В орган по сертификации к самостоятельному заполненной и подписанной декларации заявитель прилагает следующие документы:

а) заявление о регистрации декларации о соответствии, подписанное заявителем (форма заявления утверждается органом по сертификации);

б) копии документов, подтверждающих государственную регистрацию юридического лица или государственную регистрацию физического лица в качестве индивидуального предпринимателя в соответствии с законодательством государств-членов (Свидетельство о гос. регистрации);

в) копия договора с иностранным изготовителем, предусматривающего обеспечение соответствия поставляемой продукции требованиям ТР ТС и ответственность за несоответствие поставляемой на таможенную территорию Таможенного союза продукции указанным требованиям (для лица, выполняющего функции иностранного изготовителя). Стороны самостоятельно по своему усмотрению определяют в договоре форму ответственности и порядок ее наступления. Также в договоре следует предусмотреть право субъекта хозяйствования – резидента ТС – представлять интересы иностранного производителя при подтверждении соответствия серии товара, (принимать) регистрировать декларации, выпускать в обращение задекларированную на территории ТС, продукцию.

После завершения работ по подтверждению соответствия заявитель формирует комплект документов, который в общем случае включает:

- технические условия (при наличии);
- эксплуатационные документы;
- **перечень стандартов**, требованиям которых должна соответствовать данная продукция из Перечня взаимосвязанных стандартов;
- контракт (договор на поставку) или товаросопроводительную документацию (для партии продукции (единичного изделия) (схемы 3с, 4с, 3д, 4д);
- сертификат соответствия (копия сертификата) на систему менеджмента качества производства или разработки и производства продукции (схема бд);
- **протокол (протоколы) испытаний;**
- результаты анализа состояния производства (акт);
- сертификат соответствия (при форме подтверждения соответствия – сертификация);

- декларацию о соответствии (при форме подтверждения соответствия – декларирование).

Срок хранения комплекта документов: на серийное производство – у изготовителя (уполномоченного изготовителем лица) в течение не менее 10 лет со дня снятия (прекращения) с производства продукции; на партию низковольтного оборудования – у импортера или уполномоченного изготовителем лица в течение не менее 10 лет со дня реализации последнего изделия из партии.

Маркировка единым знаком обращения продукции на рынке государств-членов Таможенного союза

Продукция выпускается в обращение на рынке при ее соответствии всем ТР ТС, действие которых на нее распространяется и при условии, что она прошла процедуры подтверждения соответствия, установленные всеми ТР ТС, действие которых на нее распространяется. Продукция, не маркированная единым знаком обращения на рынке государств-членов Таможенного союза, не допускается к выпуску в обращение на рынке.

Нанесение единого знака осуществляется после завершения процедуры подтверждения соответствия. Допускается маркировать товар на складе поставщика перед выпуском товара в обращение. Следует обратить внимание на правила изображения единого знака, выбор места и способа его нанесения. Подробно с порядком маркировки можно ознакомиться в статьях 8 ТР ТС 004/2011 и ТР ТС 020/2011 и в Положении о едином знаке обращения продукции на рынке государств-членов Таможенного союза (Реш. КТС от 15 июля 2011 г. №711, документ размещен на сайте <http://www.gosstandart.gov.by>).

Базовый размер единого знака (рис. 1) должен быть не менее 5 мм.

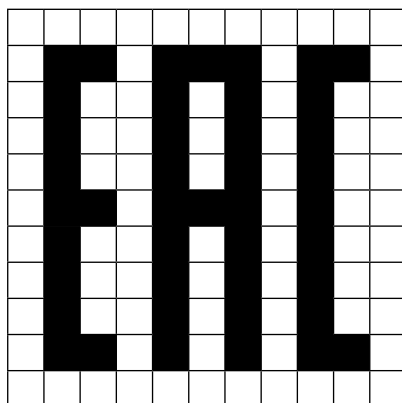


Рис. 1

Увеличение размера графического изображения единого знака обращения должно быть пропорционально базовому размеру.

Формы и виды ответственности за нарушение (несоблюдение) требований ТР ТС

Государственный надзор за соблюдением технических регламентов осуществляется Государственным комитетом по стандартизации Республики Беларусь и иными республиканскими органами государственного управления, уполномоченными на проведение государственного надзора в Республике Беларусь. Ответственность за нарушение требований стандартов предусмотрена как для субъектов хозяйствования (административные штрафы; оперативные санкции (запреты реализации, предписания о возврате продукции от потребителя); санкции по гражданскому праву), так и персональная ответственность должностных лиц (уголовная, административная, дисциплинарная, материальная).

Согласно Кодексу об Административных правонарушениях Республики Беларусь, **нарушение требований обязательного подтверждения соответствия продукции (работ, услуг) требованиям технических нормативных правовых актов в области технического нормирования и стандартизации предусматривает следующую ответственность (статья 23.11):**

- Реализацию продукции (выполнение работ, оказание услуг), в том числе импортируемой, подлежащей обязательному подтверждению соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации, без наличия сертификата соответствия и (или) **декларации о соответствии** и (или) с неправомерным использованием знаков соответствия Национальной системы подтверждения соответствия Республики Беларусь –

влечет наложение штрафа в размере от двух до пятнадцати базовых величин, а на индивидуального предпринимателя или юридическое лицо – до двукратной стоимости реализованной продукции (выполненных работ, оказанных услуг).

- Реализацию продукции (выполнение работ, оказание услуг) без наличия требуемых, в предусмотренных законодательством случаях, документов, подтверждающих качество

Продолжение на стр. 10 →



Технический регламент Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения»



Шатило Эдуард Эдуардович,
начальник учреждения
«Республиканский центр
сертификации и экспертизы
лицензируемых видов
деятельности» МЧС
Республики Беларусь,
полковник внутренней
службы

В соответствии с Соглашением о единых принципах и правилах технического регулирования в Республике Беларусь, Республике Казахстан и Российской Федерации от 18 ноября 2012 года, решением Совета Евразийской экономической комиссии от 20 ноября 2012 г. №232 «Об утверждении Плана разработки технических регламентов Таможенного союза на 2012–2013 годы» в настоящее время ведется работа над Техническим регламентом Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения».

Руководство, в лице начальника учреждения Шатило Эдуарда Эдуардовича, поделилось информацией о ходе работы над Техническим регламентом Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения».

Предпосылки к созданию Технического регламента Таможенного

союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения».

В настоящее время у стран-участниц Таможенного союза существует единое экономическое пространство, благодаря чему подразумевается свободное перемещение товаров между этими странами. Единое экономическое пространство предполагает идентичность требований безопасности к продукции, выпускаемой в каждой стране Таможенного союза, одинаковые процедуры подтверждения (оценки) соответствия, взаимное признание компетентности органов по сертификации продукции и испытательных лабораторий.

Обеспечение защиты населения и территорий от чрезвычайных ситуаций является важнейшей задачей как в Республике Беларусь, так в Российской Федерации и Республике Казахстан. Решение указанной задачи обеспечивается, в том числе, установлением обязательных для исполнения требований к продукции, предназначенной для обеспечения пожарной безопасности.

В соответствии с Решением Комиссии Таможенного союза от 28 января 2011 г. №526 в Единый перечень продукции, в отношении которой устанавливаются обязательные требования в рамках Таможенного союза, вошли средства обеспечения пожарной безопасности, средства пожаротушения, средства индивидуальной защиты. В целях установления единых требований к указанной продукции со стороны МЧС Российской Федерации в 2011 году было выдвинуто предложение о необходимости разработки соответствующего Технического регламента Таможенного союза, которое было поддержано МЧС Республики Беларусь, МЧС Республики Казахстан.

В октябре текущего года в Казах-

стане было проведено очередное совещание рабочей группы по разработке Технического регламента Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения», по результатам которого принято решение о доработке документа и вынесении его на **публичное** обсуждение.

Основная задача разработки данного Технического регламента – это установление на таможенной территории Таможенного союза единых для применения и исполнения требований к средствам обеспечения пожарной безопасности и пожаротушения.

Принципиальные отличия в требованиях к средствам обеспечения пожарной безопасности и пожаротушения, заложенные в Техническом регламенте Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» по сравнению с национальными требованиями.

Говорить о принципиальных отличиях в требованиях к средствам обеспечения пожарной безопасности и средствам пожаротушения, установленных в Техническом регламенте, от национальных требований до определения перечня стандартов, в результате применения которых обеспечивается соблюдение требований Технического регламента, пока преждевременно. Дело в том, что в Техническом регламенте установлены общие требования к средствам обеспечения пожарной безопасности и средствам пожаротушения, а их конкретизация и методы оценки определяются во взаимосвязанных с техническим регламентом стандартами. Следует отметить, что аналогичный подход существует и Республике Беларусь (ТР

2009/013/ВУ «Здания и сооружения, строительные материалы и изделия. Безопасность»). В настоящее время ведутся работы по гармонизации стандартов стран Таможенного союза, анализируются требования, заложенные в национальных стандартах к продукции. На основании данного анализа будет принято окончательное решение по выбору основополагающих стандартов, которые будут устанавливать общие требования к качеству и безопасности продукции на территории Таможенного союза.

При этом следует отметить, что в Республике Беларусь, как и в странах участницах Таможенного союза уже на протяжении ряда лет ведется работа по гармонизации национальных документов в области стандартизации, содержащих требования безопасности и методам их оценки, с международными стандартами. И это является одним из приоритетных направлений по совершенствованию технического регулирования и развитию национальной системы стандартизации в области пожарной безопасности Республики Беларусь. Актуальность указанной задачи обусловлена необходимостью создания благоприятного инвестиционного климата, обеспечения соответствия отечественной продукции международным требованиям и повышения ее конкурентоспособности, устранения технических барьеров в международной торговле, а также использования зарубежных научно-технических достижений в целях повышения уровня обеспечения пожарной безопасности в республике.

В соответствии с Положением о порядке разработки и утверждения перечней международных и региональных стандартов, а в случае их отсутствия – национальных (государственных) стандартов государств – членов Таможенного союза, обеспечивающих соблюдение требований технического регламента Таможенного союза и необходимых для осуществления оценки (подтверждения) соответствия, утвержденного Коллегией Евразийской экономической комиссии от 25 декабря 2012 г. №306 при формировании проектов перечней стандартов приоритет, прежде всего, отдается межгосударственным стандартам, принятым на основе международных стандартов и национальным (государственным) стандартам государств – членов, принятых на осно-

ве международных стандартов.

Поэтому я бы хотел обратиться к нашим производителям средств обеспечения пожарной безопасности и пожаротушения – «Уже сейчас (а не после его принятия и введения в действие) надо активно включаться в обсуждение проекта Технического регламента и принимать необходимые меры по его реализации в дальнейшем».

Проблематика, принципиальные отличия в порядке подтверждения соответствия предусмотренном проектом Технического регламента и действующим порядком подтверждения соответствия в Республике Беларусь средств обеспечения пожарной безопасности и пожаротушения.

Изменений в порядке подтверждения соответствия проектом Технического регламента не предусмотрено. В настоящее время схемы, применяемые для подтверждения соответствия в Национальной системе Республики Беларусь, полностью соответствуют схемам, применяемым в Таможенном союзе.

Практически по всей продукции, подпадающей под действие Технического регламента, предусматривается подтверждение соответствия в форме сертификации. Лишь незначительная группа продукции будет подлежать декларированию соответствия.

О планах по введению дополнительных условий обращения (реализации, инсталляции) средств обеспечения пожарной безопасности и пожаротушения на национальном уровне после принятия Технического регламента в целях защиты национального рынка.

В условиях создания Единого экономического пространства, перехода на единые разрешительные документы, выдаваемые государствами-членами Таможенного союза, при росте импорта продукции появляется опасность проявления недобросовестности со стороны отдельных представителей бизнеса. Одной из основных причин обращения на рынке республики недоброкачественных опасных товаров является низкий уровень административной ответственности за ее поставку и реализацию.

В связи с этим, для защиты внутреннего отечественного рынка в условиях Таможенного союза, необходимо усиление мер ответ-

ственности за выпуск (реализацию) продукции, не соответствующей обязательным требованиям технических регламентов Таможенного союза, необоснованного принятия документов об оценке соответствия, как минимум не ниже, чем в Российской Федерации и Республике Казахстан, создание эффективной системы надзора за рынком, как на национальном, так и межгосударственном уровне.

В целях обеспечения эффективности надзора за безопасностью и качеством продукции, размещаемой на рынке Республики Беларусь, в настоящее время Госстандартом ведется работа по подготовке соответствующего нормативного правового акта.

Прогнозы по изменению белорусского рынка средств обеспечения пожарной безопасности и пожаротушения после принятия ТР ТС, более свободный доступ на рынок продуктов из Российской Федерации, Казахстана.

По всем видам средств и систем пожарной безопасности в республике присутствуют отечественные производители, за исключением специфических позиций, например извещателей пламени, которые применяются на единичных объектах. Так, например, в настоящее время средства для огнезащитной обработки сертифицированы 22 производителями, из них 15 – это отечественные производители, на противопожарные двери, окна, люки – 35 производителями, из них отечественных – 32, на извещатели пожарные – 10 производителей, из них отечественных – 8, приборы приемно-контрольные пожарные, приборы управления – 7 производителями, из них отечественных – 5. При этом в страны Таможенного союза свою продукцию поставляют лишь единичные отечественные производители.

Поэтому здесь скорее нужно говорить о преимуществах для отечественных производителей в части открытия для них рынков стран Таможенного союза, без получения дополнительных разрешительных документов. Ну, а конкуренция между белорусскими и зарубежными производителями была и будет. Главное, чтобы она носила добросовестный характер.

**Подготовила,
Гальперина Евгения**

EXPERIENCE THE NEXT®



СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ
НОВОГО ПОКОЛЕНИЯ

axxonnext.ru



Скачайте бесплатную версию:

1 сервер

16 камер

1 Тб видеоархива

Неограниченное количество клиентов

Видеоаналитика

Биометрические системы контроля доступа
и учёта рабочего времени

ANVIZ[®]
Intelligent . Security



УНП: 192102396



Биометрик Солюшнс,ООО (Biometric Solutions, LLC)
Минск, пр. Партизанский 8, к. 28, каб.6
Тел./факс: (017) 389-72-12, (044) 466-36-36, (033) 366-36-36
www.bio-system.by info@bio-system.by


LLC BIOMETRIC SOLUTIONS
WWW.BIO-SYSTEM.BY



Нормативное обеспечение создания и применения систем видеонаблюдения

Нарушения и ответственность в рамках Постановления СМ от 11.12.2012 №1135

Продолжаем рассматривать практику применения норм Положения о применении систем безопасности и телевизионных систем видеонаблюдения, утвержденного Постановлением СМ от 11.12.2012 №1135 (далее – Положение).

Справка ТБ:

«Положение о применении систем безопасности и телевизионных систем видеонаблюдения» утверждено Постановлением №1135 от 11.12.2012 г. Советом Министров Республики Беларусь. Документ является одним из первых нормативных актов, принятых как попытка осуществить регулирование сегмента СВН в стране. По оценкам специалистов, актуальность данного НА высока, но вместе с тем, документ имеет ряд недостатков (см. разбор НА в №1, 2013 год, журнала «Технологии безопасности»). В целом можно говорить, что принятый НА является прообразом будущих документов, касающихся регламентации СВН.

Сегодня, при сдаче в эксплуатацию многофункциональных объектов с массовым пребыванием людей, сотрудники МВД (управления охраны правопорядка) требуют соблюдения норм Постановления №1135.

В целях предупреждения нарушения законодательства в сфере создания и модернизации СВН на объектах с единовременным массовым пребыванием граждан, редакция журнала обратилась в МВД Республики Беларусь за разъяснением следующих вопросов:

1. Какие основные нарушения норм Положения выявлены за время действия нормативного акта? На каких объектах чаще других выявляется несоблюдение норм Положения?

2. К какой ответственности привлечены нарушители?

3. Каковы планы по дальнейшему совершенствованию нормативной базы в части применения СВН?

На поставленные вопросы специалисты главного управления охраны правопорядка и профилактики Министерства внутренних дел Республики Беларусь пояснили следующее. Сотрудники органов внутренних дел при согласовании режима работы торговых объектов, торговых объектов общественного питания, объектов бытового обслуживания населения, рынков и торговых центров, а также в ходе мониторинга систем безопасности объектов с единовременным массовым пребыванием граждан, информируют руководителей юридических лиц о необходимости соблюдения требований Положения.

Однако имеются факты нарушения требований Положения. Так, за 9 месяцев 2013 года сотрудниками органов внутренних дел выявлено более 2000 указанных нарушений. К наиболее распространенным следует отнести – несоблюдение руководителями торговых объектов и объектов общественного питания с правом торговли алкогольными напитками требований к телевизионным системам видеонаблюдения и средствам, используемым для их создания.

За допущенные нарушения Положения и в соответствии со ст.21 Закона Республики Беларусь от 10.11.2008 г. «Об основах деятельности по профилактике нарушений» сотрудниками органов внутренних дел внесено в организации более 400 **представлений об устранении причин и условий, способствующих совершению правонарушений**, направлено 26 информации в районные исполнительные комитеты, привлечено к административной ответственности более 200 должностных лиц организаций **за неприятие мер по представлениям** (ст.24.3 Кодекса Республики Беларусь об административных правонарушениях).

В целях принятия дополнительных мер по обеспечению общественного порядка 28 ноября 2013 года принят

Указ Президента Республики Беларусь №527 «О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка» (далее – Указ).

Подводя итог выше сказанному, а также проанализировав нормы Положения, редакция журнала обращает внимание на следующие моменты:

- должностные лица организаций привлекались к административной ответственности не за невыполнение норм Положения, а за непринятие мер по представлениям;

- согласно пунктам 2 и 5 Положения, система безопасности представляет собой совокупность взаимосвязанных технических средств, информационных и аналитических систем, основанных на применении телевизионных систем видеонаблюдения и специальных детекторов, используемых, в том числе, на объектах с массовым пребыванием граждан (общественные, административные здания и сооружения), решающих задачи по обеспечению общественной безопасности и общественного порядка. Таким образом, требовать выполнение норм Положения законно только в отношении систем безопасности и телевизионных систем видеонаблюдения, обладающих одновременно следующими критериями:

- а) эксплуатируются или создаются (модернизируются) государственными органами (организациями);

- б) предназначены для обеспечения общественной безопасности и общественного порядка (на основе разъяснений, первого заместителя начальника Главного управления охраны правопорядка и профилактики милиции общественной безопасности). На объектах, не обладающих в совокупности вышеуказанными критериями, выполнение норм Положения может носить рекомендательный порядок;

- требования Положения **не распространяются** на системы безопасности, создаваемые организациями

В целях принятия дополнительных мер по обеспечению общественного порядка 28 ноября 2013 года принят **Указ Президента Республики Беларусь №527 «О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка»**.

для собственных целей и не направленные на обеспечение общественной безопасности и общественного порядка (например, системы, созданные для обеспечения сохранности имущества организации; контроля за соблюдением сотрудниками правил внутреннего распорядка; пропускного режима в организации и т.д.).

На момент подготовки материалов к публикации разработаны и

проходят согласования изменения и дополнения в Постановление СМ от 11.12.2012 г. №1135, что предусмотрено Указом. В готовящихся изменениях планируется утвердить перечень средств системы видеонаблюдения и технические требования к ним, утвердить перечень мест массового пребывания граждан в г.Минске, подлежащих обязательному оборудованию средствами систе-

мы видеонаблюдения, а также утвердить критерии отнесения объектов к числу, подлежащих обязательному оборудованию средствами системы видеонаблюдения.

До внесения указанных изменений, руководствуясь нормами Положения, следует учитывать область применения последнего, а также своевременно и аргументированно реагировать на представления органов внутренних дел.

В следующих номерах журнала запланировано детальное рассмотрение Указа и нормативных документов, принимаемых для его исполнения.

**Материал подготовила
Евгения Гальперина.**

← Начало на стр. 6

Подтверждение соответствия требованиям технических регламентов Таможенного Союза

товаров, или при наличии несоответствующих действительности документов, за исключением совершения нарушений, предусмотренных частями 1 и 2 настоящей статьи, –

влечет наложение штрафа в размере от двух до восьми базовых величин, а на индивидуального предпринимателя или юридическое лицо – до ста процентов стоимости реализованной продукции (выполненных работ, оказанных услуг), а при невозможности ее установления – до трехсот базовых величин.

Нарушение требований законодательства о техническом нормировании и стандартизации (ст. 23.12)

- Выпуск, в том числе в продажу и после ремонта, либо поставка (реализация) продукции, не соответствующей обязательным для соблюдения требованиям технических нормативных правовых актов в области технического нормирования и стандартизации и образцов (эталонов) по качеству, маркировке, комплектности, упаковке и другим требованиям, установленным законодательством Республики Беларусь, –

влекут наложение штрафа в размере от десяти до сорока базовых величин, на индивидуального предпринимателя или юридическое лицо – до ста процентов от стоимости реализованной продукции (выполненных

работ, оказанных услуг), а при невозможности ее установления – до пяти-сот базовых величин.

Нарушение запрета органов государственного надзора за соблюдением технических регламентов и средствами измерений (ст. 23.67)

Нарушение запрета органов государственного надзора за соблюдением технических регламентов и средствами измерений на выпуск, реализацию продукции (выполнение работ, оказание услуг) –

влечет наложение штрафа на индивидуального предпринимателя или юридическое лицо в размере стоимости реализованной продукции (выполненных работ, оказанных услуг).

В материале приведен неполный перечень оснований для наступления ответственности за нарушения в области технического нормирования. Как было отмечено в ходе семинара, сейчас ведется работа по усилению мер ответственности в области технического нормирования.

В итоге:

1. Не допускаются к обращению на рынке изделия, входящие в область применения ТР ТС, без соответствующего документа о подтверждении соответствия требованиям ТР ТС и маркировки единым знаком обращения продукции на рынке государств-

членов Таможенного союза. Нарушение данного запрета влечет наступление административной, а в некоторых случаях, и уголовной ответственности.

2. Несмотря на достаточно простую процедуру принятия декларации, руководителям субъектов хозяйствования следует понимать, что вся полнота ответственности за заявление о соответствии товара требованиям ТР ТС лежит на них. Минимальный пакет документов, требуемый при подаче на регистрацию декларации, не означает поверхностного отношения к перечню документов, которые должны быть у заявителя в соответствии с выбранной схемой подтверждения соответствия.

3. Определяя декларирование, как форму подтверждения соответствия, законодатель предлагает европейский подход к гарантии качества и безопасности продукта, при котором ответственность возлагается на заявителя, а не на государственные органы.

В следующих номерах мы продолжим освещать актуальные вопросы подтверждения соответствия технических регламентов Таможенного Союза. Планируется семинар по данной тематике. Актуальные вопросы отправляйте на ящик: eg@aercom.by ■

Проектирование, монтаж, наладка средств и систем пожарной автоматики и охранной сигнализации (вопрос-ответ)

В случае необходимости получения официального ответа, следует направить запрос регулятору сегмента

Вопросы по ТКП 472-2013(02010) «Правила технического обслуживания технических систем охраны».

**Ответ: Департамент охраны МВД
Республики Беларусь.**

Вопрос:

На основании **п.5.6.2.2 ТКП 472-2013** юридические лица, занимающиеся техническим обслуживанием систем охраны по специальным разрешениям (лицензиям), должны иметь обменный фонд технических средств охраны для оперативной замены технических средств охраны, вышедших из строя, на период нахождения их в ремонте. В большинстве случаев организации, эксплуатирующие технические системы охраны, каждый год проводят тендера на закупку услуг по техническому обслуживанию указанных систем. И довольно часто поставщиком данных услуг на следующий год становятся другие организации. Исходя из вышесказанного, встает ряд вопросов:

- Что делать с оставшимся на складе подменным фондом предыдущей организации? Особенно это актуально, если объект большой и на нем установлено много специфического оборудования, которое можно использовать только на этом объекте;

- Что делать в случае, если тендер на поставку услуг по техническому обслуживанию технических систем охраны выиграла другая организация, и на объекте, принимаемом ею на техническое обслуживание в установленном порядке, были ранее смонтированы технические средства, которые не поставляются в Республику Беларусь. Соответственно, данных технических средств нет в продаже (или истек срок действия сертификата соответствия), при этом срок службы установленной на объекте системы охраны не превышает нормативный? При этом у предыдущей организации был обменный фонд необходимых наименований технических средств охраны для данного объекта.

На основании вышеизложенного, можно сделать вывод о необходимости наличия подменного фонда у Заказчика (лица, осуществляющего эксплуатацию технической системы охраны), а не у Исполнителя (организации, осуществляющей техническое обслуживание). Данный подменный фонд целесообразно формировать одновременно со сдачей системы охраны в эксплуатацию (при этом в большинстве случаев оборудование данного наименования имеется в продаже и на него действует сертификат соответствия). В этом случае перечисленные выше вопросы потеряли бы свою актуальность.

Ответ:

В соответствии с **п.5.6.2.2 ТКП 472-2013(02010)** «Правила технического обслуживания технических систем

охраны» организации, занимающиеся техническим обслуживанием систем охраны по специальным разрешениям (лицензиям), должны иметь обменный фонд технических средств охраны для оперативной замены технических средств охраны, вышедших из строя, на период нахождения их в ремонте. Обменный фонд технических средств охраны исполнителей должен быть в количестве, достаточном для восстановления работоспособности обслуживаемых систем охраны в течение 12 часов после поступления заявок от пользователей, если иной срок не установлен в договорах на техническое обслуживание, но не менее одной единицы каждого наименования технического средства, находящегося на техническом обслуживании.

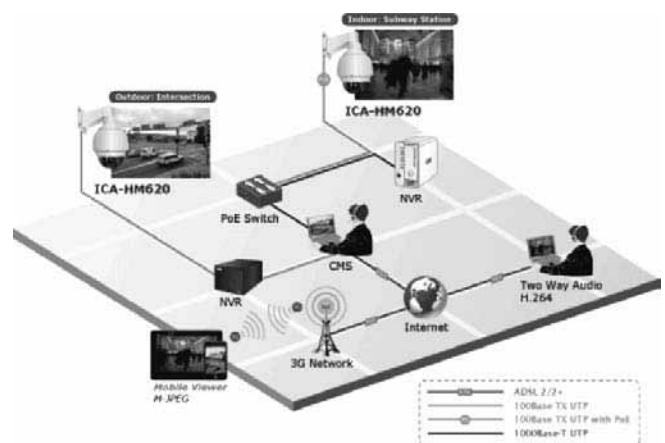
В связи с тем, что оборудование, входящее в обменный фонд, является собственностью организации, сформировавшей обменный фонд, следовательно, по-



УП «Рамок»
г. Минск, ул. Лермонтова, 29
8 (017) 213-67-00
8 (029) 613-67-00 velcom
8 (033) 313-67-00 mts

Комплексные системы безопасности:

- IP камеры видеонаблюдения Planet
- Сетевое оборудование Planet
- Аналоговые камеры видеонаблюдения Vangold
- Охранная сигнализация
- Пожарная сигнализация
- Озвучивание помещений



www.Ramok.by

сле окончания договорных обязательств эта организация вправе использовать это оборудование на других объектах, либо продать его иным организациям.

В случае если на объекте смонтированы технические средства сигнализации, которые в настоящее время по каким-либо причинам не представляется возможным приобрести, допускается использовать аналогичное по своим техническим характеристикам сертифицированное в Республике Беларусь оборудование. Порядок формирования, учета и использования технических средств охраны обменного фонда определяется ведомственными инструкциями юридических лиц, занимающихся техническим обслуживанием систем охраны. Техническое обслуживание систем охраны юридическими лицами, не имеющими обменного фонда технических средств охраны, запрещается.

Вопросы по ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений».

**Отвечает Пукач Анатолий Анатольевич,
главный специалист по пожарной
безопасности РУП «МБИ».**

Вопрос:

Согласно п. 16.2 ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений», шлейфы и другие соединительные линии пожарной автоматики необходимо выполнять с условием обеспечения автоматического контроля их целостности по всей длине. Необходимо ли, на основании данного пункта, обеспечивать автоматический контроль линии между приемно-контрольным прибором, пожарным и промежуточным реле, управляющим исполнительными механизмами (например, отключением вентиляции и кондиционирование воздуха при пожаре электромеханическими замками для открытия дверей и т.п.)?

Уточнение: Имеется в виду не только отключение вентиляции, но и управление с помощью промежуточного реле другими исполнительными механизмами, например, электромеханическими замками для открытия дверей, включение эвакуационного освещения, отключение иного технологического оборудования.

Ответ:

Требование п.16.2 ТКП 45-2.02-190 не распространяется на линии отключения систем вентиляции и кондиционирования воздуха при пожаре электромеханическими замками для открытия дверей (реле отключения вентиляции не является компонентом СПС по СТБ 11.16.01-98).

Вопрос:

Согласно п. 13.5 ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений» приборы пожарной автоматики следует устанавливать на стенах, перегородках и конструкциях, изготовленных из негорючих материалов. В пособии к ВСН 25-09.68-85 «Правила производства и приемки работ. Установки охранной, пожарной и охранно-пожарной сигнализации» (отменен с 01.01.2008 г.) в п. 10.3 сказано: «при монтаже ПКП, ПКУ на горючих основаниях (деревянные стены, монтажный щит из дерева или ДСП, толщиной не менее 10 мм) необходимо применять огнезащитный листовый материал...». Какой документ на настоящий момент дает

определение, что необходимо понимать под «горючим основанием»?

Ответ:

Определение параметров горючести строительных материалов приведено в ТКП 45-2.02-142-2011.

Вопрос:

Согласно п. 13.6 ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений» расстояние от верхнего края прибора до перекрытия (покрытия) потолка, выполненного из горючих материалов, должно быть не менее 1 м. Допускается ли, при невозможности монтажа прибора на расстояние не менее 1 м до перекрытия, уменьшить данное значение, при условии монтажа над прибором на перекрытии потолка стального листа толщиной не менее 1 мм, или другого листового негорючего материала толщиной не менее 10 мм, при условии, что листовый материал будет выступать за контур устанавливаемого оборудования, при проецировании его на горизонтальную плоскость не менее чем на 100 мм?

Ответ:

Считаю, что такое решение возможно. Чтобы не было проблем при сдаче в эксплуатацию, данное решение необходимо согласовать с органами государственного пожарного надзора. ■

ЧУП "Завод СВТ"

**Металлодетекторы
арочные и досмотровые**

Видеомониторы, ПЗВМ, тонкие клиенты

Радиоизмерительная аппаратура

Тел: 8 (017) 297-93-92 ZSVT.BY

УНП 190737825



Безопасность банковско-финансовой сферы

В рамках разработки тематики банковской безопасности мы провели ряд интервью с представителями Национального банка Республики Беларусь как одного из регуляторов, курирующего этот сегмент. Ставилась задача выявить актуальные вопросы, обеспечить понимание проблематики в сегменте банковской безопасности как информационной, так и инженерно-технической.

Данная тематика становится актуальной. Согласно планов по развитию в Республике Беларусь системы безналичных расчетов по розничным платежам с использованием современных электронных платежных инструментов и средств платежа на 2013–2015 годы, предполагается увеличение доли безналичного денежного оборота к 1 января 2016 года до 50%, что примерно в четыре раза больше текущей доли. Активное развитие системы безналичных расчетов повлечет за собой развитие мер по обеспечению безопасности. Насколько готова система, обеспечивающая безопасность в нашей стране к такому росту? Дать оценку внешних структур, обеспечивающих безопасность банковского сегмента, мы попросили Дубкова Сергея Витальевича, заместителя Председателя Правления Национального банка Республики Беларусь.

Каковы основные вопросы взаимодействия банковской системы, как потребителя услуг по безопасности, с ведомствами, осуществляющими услуги и регулирование сегмента безопасности. Ваше видение как участника такой работы?

Национальный банк сотрудничает с ОАЦ (ранее – ГЦБИ), МВД и другими правоохранительными органами в течение многих лет. С ОАЦ это совместное участие в разработке законов «Об электронном документе», «Об электронном документе и электронной цифровой подписи», создании Государственной системы управления открытыми ключами, стандартов, регламентирующих использование средств криптозащиты информации, с МВД – разработка нормативных актов



Дубков Сергей Витальевич, заместитель Председателя Правления Национального банка Республики Беларусь, член программного комитета выставки-форума «Центр безопасности».

по технической укрепленности объектов банков. Как координатор, Национальный банк уделяет первостепенное внимание вопросам обеспечения безопасности банковской сферы.

В соответствии с Законом Республики Беларусь от 13 июля 2012 года «О внесении дополнений и изменений в Банковский кодекс Республики Беларусь» статья 26 Банковского кодекса Республики Беларусь дополнена рядом функций Национального банка, направленных непосредственно на усиление его организующей роли в обеспечении безопасности объектов банковской деятельности, в частности по:

- установлению для банков и небанковских кредитно-финансовых организаций обязательных требований к безопасному функционированию объектов и безопасности оказания банковских услуг, защите информационных ресурсов и информации, распространение и (или) предоставление которых ограничено, если иное не предусмотрено законодательными актами Республики Беларусь;
- осуществлению контроля за обеспечением безопасности и защиты информационных ресурсов в банках и небанковских кредитно-финансовых организациях;

- установлению требований к техническим возможностям банков, небанковских кредитно-финансовых организаций, их филиалов, структурных подразделений и удаленных рабочих мест для проведения банковских операций, осуществлению технического нормирования и стандартизации в области банковской деятельности.

Банковская система в целом не имеет проблем при взаимодействии с регуляторами сегментов обеспечения безопасности.



По линии МЧС Республики Беларусь с банками организовано взаимодействие по следующим направлениям:

- защита зданий и сооружений, имущества, ценностей, жизни персонала и клиентов банков от пожара посредством системы мониторинга техническими средствами обнаружения и передачи информации на пульт мониторинга МЧС;
- контроль за соблюдением лицензионных требований и условий при осуществлении банком деятельности по обеспечению пожарной безопасности;
- приемка систем пожарной автоматики и оповещения о пожаре;
- защита зданий и сооружений, имущества, ценностей, жизни персонала и клиентов банков в других чрезвычайных ситуациях, носящих природный или техногенный характер;
- банками обеспечивается выполнение предписаний территориальных подразделений МЧС по результатам плановых обследований обеспечения пожарной безопасности, создаются добровольные пожарные дружины, утверждаются внутренние акты, регламентирующие порядок действий в

чрезвычайных ситуациях, проводятся внутренние, а также совместные с МЧС учения в целях готовности персонала к четкой и слаженной работе при возникновении чрезвычайных ситуаций.

По линии МВД Республики Беларусь с банками организовано взаимодействие по следующим направлениям:

- Расчетный центр Национального Банка предоставляет доступ банкам к информационным ресурсам МВД в ограниченном объеме, информацию из которого банки используют для оценки рисков при принятии решений о выдаче кредитов, проверки деловой репутации контрагентов, проверки кандидатов на работу в банках;
- банки и Национальный банк предоставляют МВД всю необходимую и имеющуюся в банках информацию по совершаемым преступлениям;
- проведение совместных мероприятий с целью профилактики и раскрытия преступлений в банковской сфере;
- МВД оперативно реагирует на инциденты, связанные с преступлениями против банков, а также клиентов банков.

По линии Департамента охраны МВД Республики Беларусь с банками организовано взаимодействие по следующим направлениям:

- защита зданий и сооружений, имущества, ценностей, жизни персонала и клиентов банков от противоправных посягательств;
- контроль и выработка мероприятий по оборудованию объектов банков инженерно-техническими средствами защиты;
- мониторинг и реагирование на сигналы от технических средств охраны и тревожной сигнализации посредством пульта централизованного наблюдения Департамента охраны, выезд оперативных сотрудников Департамента охраны в случае инцидентов, обслуживание инженерно-технических средств защиты и сигнализации;
- физическая охрана банковских объектов;
- контроль за соблюдением лицензионных требований и условий при осуществлении охранной деятельности.

По линии Оперативно-аналитического центра при Президенте Республики Беларусь с банками организовано взаимодействие по следующим направлениям:

- контроль использования программно-аппаратных средств защиты информации, в том числе криптографических;

Справка ТБ:

По информации, полученной журналом, Департаментом охраны МВД Республики Беларусь совместно с Национальным банком Республики Беларусь подготовлен проект инструкции «О порядке и условиях оборудования объектов Национального банка Республики Беларусь, банков, подлежащих обязательной охране Департаментом охраны Министерства внутренних дел Республики Беларусь, и небанковских кредитно-финансовых организаций, средствами и системами охраны». Данный проект инструкции проходит согласование в заинтересованных организациях, стадия согласования – заключительная.

- аттестация систем защиты информации банков, либо отдельных информационных систем;
- контроль за соблюдением лицензионных требований и условий при осуществлении деятельности по технической защите информации, в том числе криптографическими методами.

Вместе с тем, по результатам проведенного опроса банков по заданной тематике, в банках существуют предложения по совершенствованию взаимодействия с государственными регуляторами. Для удовлетворения потребностей банковской системы Национальный банк прорабатывает с соответствующими ведомствами вопросы дальнейшего развития сотрудничества. Национальный банк организует площадки для обсуждения экспертами текущей проблематики и дальнейшего совершенствования взаимодействия участников, заинтересованных в защите банковско-финансовой сферы. Функционируют рабочие группы, комитеты, а также проводятся специализированные мероприятия, форумы, семинары, круглые столы.

Какова роль Национального банка в разработке нормативных актов, регулирующих сегмент безопасности? Планируется ли активное участие Национального банка (в частности подразделения Управления безопасности и защиты информации) в разработке нормативных актов?

В части нормативных актов по инженерно-технической безопасности Национальным банком разработаны и сопровождаются стандарты Республики Беларусь, устанавливающие технические требования и методы испытаний для:

- банковских хранилищ ценностей;
- сейфов;
- пунктов обмена валют;
- защитного остекления;

- противовзломных дверей хранилищ;
- замков для бронедверей и банковских сейфов;
- бронеавтомобилей для перевозки ценностей;
- передвижных обменных пунктов на базе бронеавтомобилей.

Разработан и сопровождается Технический кодекс установившейся практики по проектированию зданий банков. Совместно с Департаментом охраны МВД разработаны нормативные документы, устанавливающие требования по:

- оборудованию банков техническими средствами охраны;
- организации охраны банков;
- технической укреплённости пунктов обмена валют;
- технической защите банкоматов.

В части нормативных актов по информационной безопасности Управлением безопасности и защиты информации организована разработка стандартов:

- СТБ 34.101.41 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения»;
- СТБ 34.101.42 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности»;
- СТБ 34.101.62 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41»;
- СТБ 34.101.60 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41»;
- СТБ 34.101.61 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности».

Указанные СТБ предполагается издать в 2014 году.

Какая работа ведется для обеспечения безопасности системы безналичных расчетов?

Практика развития рынка безналичных розничных платежей свидетельствует о том, что с расширением ко-

личества операций с использованием современных электронных платежных инструментов возрастает уровень мошенничества в данной сфере. Данный вывод подтверждает увеличивающееся количество поступающих в Национальный банк обращений граждан – держателей банковских платежных карточек (далее – карточки).

Одним из существенных факторов снижения роста мошеннических транзакций является выпуск в обращение карточек с микропроцессором (чипом) стандарта EMV, разработанного международными платежными системами. По сравнению с карточками с магнитной полосой чиповые карточки предоставляют возможность не только расширения функционала таких продуктов, но и более высокого уровня безопасности совершения операций, поскольку правомерность использования карточки подтверждается ПИН-кодом, а не подписью держателя. При этом, как правило, выпускаются в обращение комбинированные продукты, сочетающие в себе магнитную полосу и чип. Сохранение магнитной полосы позволит рассчитаться карточкой также в инфраструктуре, не предназначенной для приема чиповых продуктов.



В рамках перехода к микропроцессорным карточкам следует учитывать не только общемировые тенденции, но и обстоятельства, складывающиеся на рынках сопредельных стран. В частности, в Российской Федерации в целях сокращения роста мошенничества Центральным банком подготовлено решение, согласно которому все вновь эмитируемые карточки с 1 января 2015 года должны будут оснащаться микропроцессором стандарта EMV. Фактор отсутствия границ между странами в рамках Таможенного союза в данной ситуации создаст угрозу роста мошеннических операций в Республике Беларусь при сохранении на внутреннем рынке большой доли карточек с магнитной полосой.

Следует отметить, что банки Республики Беларусь уже выпускают в об-

ращение карточки стандарта EMV и 96% функционирующих в Республике Беларусь объектов программно-технической инфраструктуры адаптированы к приему чиповых карточек. Международные платежные системы MasterCard и VISA также заявили о готовности на паритетных началах перейти на эмиссию в Республике Беларусь исключительно чиповых карточек.

С учетом изложенного, в целях предотвращения мошенничества с использованием карточек, в рамках заседания Комитета по безналичным расчетам Ассоциации белорусских банков проработан со специалистами банков вопрос об обязательном выпуске с 1 января 2015 года в обращение карточек с микропроцессором. Также предложено банкам и ОАО «Банковский процессинговый центр» принять меры по повышению качества обучения сотрудников организаций торговли (сервиса), принимающих карточки к оплате за товары (услуги), и минимизации фактов мошенничества при осуществлении таких операций.

Отмечаем, что указанному вопросу Национальный банк, МВД, Следственный комитет и Прокуратура уделяют очень большое внимание. Проводится постоянная и эффективная слаженная работа. В рамках проведения 1-й Национальной выставки-форума «Информационная безопасность. Телекоммуникации» представитель Национального банка выступил с отдельным докладом по данной тематике.

Мировой опыт. Есть ли зарубежные примеры, когда Национальный банк осуществляет/координирует работу по разработке нормативных актов для банков?

В большей части стран имеется понимание о необходимости создания двухуровневой банковской системы: центральный банк страны, регулирующий банковскую сферу, и банки, осуществляющие банковскую деятельность. Центральный банк (ЦБ) страны устанавливает правила функционирования банковской системы страны и контролирует банковскую систему, осуществляя необходимое регулирование процессов.

Различные ЦБ в разных странах имеют разные перечни регулируемых направлений банковско-финансового сектора страны. Процесс появления новых функций ЦБ не статичен. Некоторые направления признаются функциями, не свойственными ЦБ, но появляются и новые функции по регулированию банковской или финансовой деятельностью страны.

Регулирующие органы, коими являются ЦБ, разрабатывают и формируют правила работы банковской системы, которые утверждаются нормативными актами, государственными стандартами. Так, например, по направлению информационной безопасности Банком России была разработана серия стандартов ИББС (Информационная безопасность банковской системы).

Согласно новой редакции Банковского кодекса Республики Беларусь, вступившей в силу 22.01.2013 г., в функции Национального банка Республики Беларусь добавлено регулирование обеспечения безопасности банковской системы Республики Беларусь.

Сегодня ряд банков заявляют о возможности и желании осуществлять охранный мониторинг и охрану силами собственных служб безопасности. Например, ОАО «АСБ Беларусбанк» осуществляет такую деятельность. Каково Ваше видение в части демополизации рынка охранных услуг для банковских объектов? Каковы перспективы, тенденции и актуальность такой политики?

Демополизация рынка охранных услуг требует кардинального изменения законодательства Республики Беларусь, но позволит обеспечить конкуренцию по предоставлению охранных услуг, которая может повысить качество и разнообразие предоставляемых услуг, внедрение новых научно-технических разработок, обеспечит обоснованность ценообразования.

Необходимо отметить, что крупные банки Республики Беларусь работают на массового клиента, они имеют свои службы безопасности и инкассаторские службы. Эти банки способны осуществлять большие капиталовложения на развитие указанных служб, их техническое оснащение, подготовку кадров, оплату труда сотрудников, отчисления на нужды обязательного социального страхования, ГСМ и т.п. Для малых и средних банков, ориентированных на оказание банковских услуг узкому сегменту населения, полный переход на выполнение охраны банковских объектов своими силами не реален ввиду недостаточности сил и средств, неготовности осуществления ими больших материальных вложений в развитие служб безопасности.

Также, по мнению банков, полный отказ от услуг Департамента охраны нецелесообразен и не рассматривается. В частности, охрана оружия должна в любом случае производиться Департаментом охраны МВД. ■



Актуальность выработки методик и ознакомления с технологиями расследования инцидентов в системах электронных платежей



Денисов Денис Валерьевич. Главное управление единого расчетного и информационного пространства. Эксперт по информационной безопасности, защите информации в банковской сфере, противодействию мошенничеству в области электронных платежей.

Как в Беларуси происходит развитие регулирования указанного сегмента?

Пожалуй, отправной точкой нововитка развития направления обеспечения банковской безопасности можно считать разбойное нападение 10.12.2009 г. на обменный пункт ЗАО «Абсолютбанк» в Минске. Убита 21-летняя кассир. После этого инцидента 24.12.2009 г. в Национальном банке Республики Беларусь с участием представителей органов государственного управления и руководителей банков состоялось совещание, на котором были приняты достаточно серьезные решения. По результатам совещания был составлен план мероприятий. В

дальнейшем в целях комплексного подхода к борьбе с преступностью Указом Президента от 23.09.2010 г. №485 утверждена Государственная программа по борьбе с преступностью и коррупцией на 2010–2012 годы, в которой уже были учтены и мероприятия по результатам совещания в Национальном банке. Во исполнение решений п. 2.3 Плана мероприятий совещания в Национальном банке Республики Беларусь и п. 3.1.1.4 Государственной программы, распоряжением Председателя Правления Национального банка Республики Беларусь от 31.12.2010 года № 1056 была создана межведомственная рабочая группа по противодействию мошенничеству в области электронных платежей. В состав рабочей группы вошли представители Национального банка Республики Беларусь, крупнейших банков Республики Беларусь, Министерства внутренних дел Республики Беларусь, Следственного комитета Республики Беларусь, ОАО «Банковский процессинговый центр», ООО «VISA Украина», ООО «Мастеркард» (г. Москва). Результатом работы группы стал Свод рекомендаций, включивший в себя:

- рекомендации по организации взаимодействия между банками, процессинговыми центрами и органами Министерства внутренних дел, в случае выявления мошенничества с банковскими платежными карточками;
- рекомендации по обеспечению безопасного функционирования программно-технической инфраструктуры банков, ОАО «Банковский процессинговый центр», ООО «Веб Пэй» и аналогичных организаций, участвующих в обработке интернет-транзакций с использованием банковских платежных карточек;
- рекомендации для оценки надежности интернет-магазинов, под-

ключаемых белорусскими банками-эквайерами;

- рекомендации по противодействию мошенничеству при совершении расчетов в сети Интернет по банковским платежным карточкам;
- рекомендации банкам по оформлению документов, позволяющих подтверждать ущерб, причиненный резидентам иностранных государств в результате мошенничества в области интернет-эквайринга на территории Республики Беларусь.

В дальнейшем по распоряжению Первого заместителя Председателя Правления Национального банка Республики Беларусь Лузгина Н.В. от 13.11.2012 г. №484 были продолжены мероприятия по функционированию рабочей группы по противодействию мошенничеству в области электронных платежей с целью дальнейшего анализа состояния и потребностей в данном направлении. Также была дана оценка эффективности применения разработанного в 2011 году свода рекомендаций по противодействию мошенничеству в области электронных платежей и определены новые векторы работы группы.

Какие организационно-технические меры принимаются участниками рынка для обеспечения безопасности платежей?

По информации банков, некоторые из них внедрили механизмы микроплатежей. При совершении оплаты с использованием иностранной банковской платежной карточки платежный сервер осуществляет online авторизацию с использованием данной карты на случайную сумму от 0,5 до 2 USD. Держатель карты должен узнать сумму микроплатежа в банке-эмитенте платежной карты и ввести сумму микроплатежа для подтверж-

noVus®

Профессиональные решения для систем безопасности

КАМЕРЫ ЗМП

Инновационные функции, Широкий спектр применения!



- Матрица 1/2.8" CMOS, 3 мп (2048 x 1536)
- Объектив с переменными фокусными расстояниями, обеспечивающий горизонтальный угол обзора 90° ~ 28°
- Широкий динамический диапазон (WDR)
- Повышение чувствительности за счет

- уменьшения скорости затвора (DSS)
- Цифровое шумоподавление (DNR)
- Механический ИК-фильтр
- ИК-подсветка до 40 метров
- 6 ненаблюдаемых зон
- H.264, MPEG4 и M-JPEG

- До 20 кадров/сек для 2048 x 1536
- До 30 кадров/сек для 1920 x 1080
- Запись видео в формате AVI
- Обнаружение движения
- Поддержка диапазона температур -40°C ~ 50°C
- IP 66

Программное обеспечение для мониторинга в комплекте!



Full HD



Поддержка мобильных устройств

Высокая чувствительность
0,001 лк/Ф = 1.2 (ч/б, DSS)



Коммутатор/маршрутизатор

Операция потока

Дистрибьюторы оборудования NOVUS® в Беларуси:

**СМАРТ
ПРОЕКТ**



Смартпроект ООО
ул. Гусовского, 6, оф. 2.6
г. Минск 220073, Беларусь
+375 17 290-84-48, +375 17 290-84-00
info@smartproekt.by, www.smartproekt.by



Новатех Системы Безопасности ЗАО
ул. Городецкая, 38А, 3й этаж
г. Минск 220125, Беларусь
+375 17 286-39-51, +375 17 286-39-52
sales@novatekh.by, www.novatekh.by

НОВЫЕ IP-РЕГИСТРАТОРЫ Full HD Real Time



8/3* и 16/6**
тревожных
входов/выходов

Двухнаправленное
аудио



HDMI
VGA



RVi-IPN16/2-PRO*



RVi-IPN16/8-PRO**



www.rvi-cctv.by

НАДЕЖНОСТЬ И
ФУНКЦИОНАЛЬНОСТЬ



- Запись потоков с 16 сетевых камер, при разрешении Full HD (1920x1080), в режиме реального времени
- Суммарный входящий битрейт 160 Мбит/с
- Максимальный объем памяти 8 ТБ* и 32 ТБ**
- Поддержка сетевых камер до 5 MPix

ЭРВИ групп

+7 (495) 735 3847, 735 3857

ONVIF

дения совершения основной оплаты в течение одного часа. Если сумма микроплатежа совпадет с введенной держателем карты суммой, валидация карты считается успешной и платежный сервер осуществляет online авторизацию на основную сумму оплаты и формирует операцию отмены по микроплатежу. В случае, если держатель карты неправильно ввел сумму микроплатежа три раза или не ввел ее в течение часа, платежный сервер формирует операцию отмены по микроплатежу и не осуществляет online авторизацию на основную сумму оплаты.

Также банки используют технологии Verified by VISA и MasterCard SecureCode, используют трехфакторную аутентификацию платежей интернет-банкинга 3D Secure, совершенствуются методы фрод-мониторинга, устанавливаются блокировки на суммы снятия денежных средств, дополнительные методы подтверждения платежей в географически опасных странах мира (Таиланд, США и другие). Иногда полностью запрещаются операции в некоторых странах, все больше карт выпускаются с микрочипами. ОАО «Банковский процессинговый центр» ежеквартально проверяет контент интернет-магазинов с эквайрингом белорусских банков согласно Своду рекомендаций. VISA и MasterCard предлагают все больше услуг по безопасному использованию банковских платежных карт – возможности геоблокировки, уведомления держателей карт об опасных транзакциях, когда параметры транзакции соответствуют определенным ограничениям по географии, сумме транзакции, по типу организаций торговли и сервиса, и наконец даже скоринговые интеллектуальные системы фрод-мониторинга.

В рамках деятельности рабочей группы был создан закрытый информационный ресурс, на котором специалисты по карточной безопасности банков и специалисты органов внутренних дел обмениваются контактной информацией и оперативно оповещают других участников о точках подтвержденной компрометации карт. Так, например, участники оперативно могут узнать в каких устройствах и в какой промежуток времени производилось считывание карт скиммерами.

Национальным банком Республики Беларусь разработаны типовые памятки держателям карт. Указанные памятки имеются во всех отделениях банков, а также на официальных

сайтах банков. С целью реализации государственной программы по повышению финансовой грамотности населения реализуется целый комплекс мероприятий с привлечением банков и средств массовой информации. Все больше банков перед операциями с банкоматами выдают оповещение клиентам с тем, чтобы они убедились в отсутствии скиммеров в банкомате и так далее.

Каковы результаты принятых мер, можете привести статистику?

Так, по сведениям Министерства внутренних дел Республики Беларусь, анализ оперативной обстановки на территории республики в 2012 году отражает тот факт, что количество преступлений в сфере незаконного оборота платежных карт снижается. Так, если за 9 месяцев 2011 года зарегистрировано 1528 преступлений, то за аналогичный период 2012 года – 1271, снижение составляет 16,8 %.

Если рассматривать структуру зарегистрированных преступлений, то подавляющее большинство совершено с использованием подлинных банковских платежных карт, но наибольшую общественную опасность представляют хищения, совершаемые с использованием поддельных карт, либо их реквизитов, а также с использованием специальных средств, предназначенных для несанкционированного копирования информации с магнитных полос банковских платежных карт.

Для объективной оценки состояния преступности следует иметь в виду, что в этой части официальная статистика не отражает реальное количество хищений, совершенных с использованием поддельных карт. Как правило, такие преступления совершаются в составе организованных групп, которые к моменту выявления и принятия решения о возбуждении уголовного дела уже совершили десятки и сотни эпизодов хищений, осуществили приготовление к совершению новых преступлений. При возбуждении уголовного дела в таких случаях, принимая во внимание наличие единого умысла на совершение ряда преступлений, следователь возбуждает одно уголовное дело. То есть на практике зачастую в одном уголовном деле расследуются сотни эпизодов хищений, объединенных единым умыслом, совершенных одними и теми же лицами из банкоматов, принадлежащих различным банкам, с использованием сотен банковских платежных карт, эмитированных раз-

личными банками.

Всего в 2012 году обезврежено 5 преступных групп (общей численностью 12 человек, в том числе 2 международных), специализировавшихся на совершении преступлений в сфере незаконного оборота платежных карт на территории страны.

Среди особенностей оперативной обстановки за истекший период можно считать уменьшение числа выявленных преступлений, совершаемых с использованием поддельных банковских платежных карт («белого пластика»).

Из работы в данном сегменте хочу выделить проведенный вашей компанией ООО «АэркомБел» 27 марта 2013 года семинар «Расследование инцидентов информационной безопасности в системах электронных платежей», ставший знаковым в данном направлении для Республики Беларусь, так как на этом мероприятии эксперты из Российской Федерации и Республики Беларусь впервые подняли пласт такой проблематики для белорусских банков и иных организаций.

Каковы дальнейшие планы по работе в развитии сегмента безналичных платежей и обеспечения безопасности платежей?

01.04.2013 г. Постановлением Совета Министров Республики Беларусь и Национального банка Республики Беларусь от №246/4 утвержден План совместных действий государственных органов и участников финансового рынка по развитию в Республике Беларусь системы безналичных расчетов по розничным платежам с использованием современных электронных платежных инструментов и средств платежа на 2013–2015 годы. План предполагает увеличение показателей доли безналичного денежного оборота в розничном товарообороте организаций розничной торговли и доли безналичного денежного оборота в объеме платных услуг населению к 1 января 2016 года до 50%.

11.04.2013 г. по предложению Национального банка Республики Беларусь в Ассоциации белорусских банков состоялось совместное заседание членов Комитета платежной системы и Комитета по информационным технологиям при Ассоциации. В заседании принял участие заместитель Председателя Правления Национального банка Республики Беларусь С.В.Дубков. По итогам заседания принято решение об объединении указанных комитетов путем создания

единого Комитета по безналичным расчетам, в рамках деятельности которого будут рассматриваться как ранее закрепленные вопросы, так и вопросы развития системы безналичных расчетов. Работа данного Комитета разделена на три подкомитета:

- Платежные карты, электронные деньги и иные инструментари.
- Безналичные расчеты юридических лиц.
- Информационные технологии.

15.04.2013 г. Распоряжением Председателя Правления Национального банка №140 деятельность рабочей группы по противодействию мошенничеству в области электронных платежей была завершена и передана в Подкомитет «Платежные карты, электронные деньги и иные инструментари» Комитета по безналичным расчетам, тем самым повысив значимость данного направления.

Весной 2013 года отмечался всплеск инцидентов мошенничества в системе электронных платежей. Большой общественный резонанс произвели случаи мошенничества с использованием скимминга.

25.04.2013 г. проведено межведомственное совещание при заместителе Генерального прокурора с участием представителей Верховного Суда, Следственного комитета, МВД, Департамента финансовых расследований КГК, Национального банка, Ассоциации белорусских банков, а также крупнейших банков страны. На совещании рассматривался вопрос принятия процессуальных решений о возбуждении уголовных дел по фактам хищения денежных средств банков с территории иностранного государства. Принято решение о том, что заявления будут концентрироваться в РУВД по месту регистрации центрального офиса банка, так как в Минске легче нарастить соответствующую компетенцию сотрудников МВД, сам факт заявления будет достаточным для возбуждения уголовного дела вне зависимости от того, где произошло мошенничество.

18 июня 2013 г. на заседании комитета по безналичным расчетам в Ассоциации белорусских банков было принято решение о создании документа, который введет в Республике Беларусь принцип «нулевой ответственности» для владельцев банковских карт. Принцип «нулевой ответственности» предполагает безусловный возврат банком клиенту украденных с карточки средств (по аналогии со статьей 9 Федерального закона Российской Федерации от 27.06.2011 №161-ФЗ «О национальной платежной системе»). С



инициативой создания этого документа выступил начальник Управления по расследованию преступлений против информационной безопасности Следственного комитета Республики Беларусь А.Е. Сушко.

Банки с введением такой ответственности будут нести прямые финансовые потери, в то время как на сегодняшний день несут потери держатели карт. Банки будут стимулированы проводить расследование таких инцидентов. В свою очередь, принятие такого рода нормативного акта создаст условия для фактов мошенничества со стороны держателей карт, что потребует разработки методик работы с такого рода правонарушителями.

На данный момент банки прорабатывают ряд вопросов, возникающих при реализации принципа нулевой ответственности. К примеру, по какой статье проводить возврат денежных средств. Решение о формате документа и сроках вступления его в силу пока не принято.

Так, в рамках работы над данным документом 10.10.2013 г. на очередном заседании комитета по безналичным расчетам в Ассоциации белорусских банков рассматривался вопрос об обращении в Совет Министров с предложением о внесении изменений и дополнений в Налоговый кодекс в части налогообложения клиентов банков при осуществлении банками возврата сумм физическим лицам, пострадавшим от мошенничества при проведении операций с использованием карточек на основе анализа действий банков при выявлении мошенничества и их решений о возмещении ущерба пострадавшим лицам.

Какие еще перспективные работы ведутся в данном направлении?

Необходимо продолжать работу над повышением компетенции служб

безопасности банков и отрабатывать принципы реагирования на случаи мошенничества. Особенно актуально это станет с введением принципа нулевой ответственности. В Российской Федерации принят федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Согласно статье 9 этого закона, вступающего в силу с 2014 года, устанавливается порядок возможности отмены транзакций с признаками мошенничества. К слову, там держателю карты банк будет обязан вернуть денежные средства на карту в течение 24 часов в случае хищения, когда нет явной вины держателя. А уже затем сам банк собирает материалы и передает в правоохранительные органы для возмещения ущерба, нанесенного уже банку, а не держателю карты.

Анализируя инциденты можно констатировать, что в большинстве случаев банки создали необходимые организационные и технические условия обеспечения внутренней защиты банка и устройств, но процесс этот не статичен, и банкам необходимо на постоянной основе совершенствовать методы и технологии внутренней защиты банков.

Кроме регламентации внутренних процедур должны быть предусмотрены также технические средства информационной безопасности, которые могут предотвращать такие случаи с помощью разграничения доступа, мониторинга совершенных пользователем операций, расследования инцидентов и пр.

Также следует учитывать опыт Российской Федерации, где, к примеру, разработаны Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиентов.

Для стабильной работы банковской системы и доверия населения к ней необходимо обеспечивать защиту денежных средств и информации клиентов (держателей карт).

Прошедшая 1 Национальная выставка-форум «Центр безопасности: Информационная безопасность. Телекоммуникации» стала отличной площадкой для повышения компетенции всех участников, задействованных в обеспечении безопасности, противодействии мошенничеству, а также расследовании инцидентов в системах электронных платежей. В ходе нашей специализированной секции мы наладили контакты с коллегами, обменялись опытом, а также изучили рынок продуктов и услуг, способствующих повышению безопасности, снижению риска мошенничества, а также дающих инструментарий при расследовании инцидентов.

Бывают случаи, когда банки недостаточно эффективно взаимодействуют с правоохранительными органами, либо не используют Свод рекомендаций. Внутренние расследования банков иногда проводятся формально. Немаловажным фактором является принятие решений банками о неразглашении инцидентов, так как это может негативно сказаться на репутации банка. Такие эпизоды, когда злоумышленники остаются безнаказанными, подстегивает криминальные круги использовать свои схемы и в дальнейшем. Нам необходимо совместными усилиями добиваться искоренения преступности в нашем сегменте, для чего каждый представитель службы безопасности банков должен понимать, как в дальнейшем собранная информация об инциденте будет использована при расследовании государственными органами. Банк должен понимать, каковы успехи в расследовании преступлений государственными органами, эффективность взаимодействия банков, Министерства внутренних дел Республики Беларусь, как органа, собирающего материалы преступления, Следственного комитета Республики Беларусь, как органа уголовного преследования, и органов прокуратуры на финише при принятии судебных решений.

В свете увеличения показателей доли безналичного денежного оборота насколько актуально обеспечить соответствие национальных систем стандарту PCI DSS?

Банки заинтересованы обеспечить соответствие стандарту PCI DSS. Международные платежные системы

Справка ТБ:

Payment Card Industry Data Security Standard (PCI DSS) – стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платёжных карт (Payment Card Industry Security Standards Council, PCI SSC), учреждённым международными платёжными системами Visa, MasterCard, American Express, JCB и Discover. Стандарт представляет собой совокупность 12-ти детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платёжных карт.

со значительным ростом количества операций в стране могут более жестко отнестись к соответствию белорусских участников платёжных систем стандарту PCI DSS.

Основной акцент стандарт PCI DSS делает на обеспечении безопасности сетевой инфраструктуры и защите хранимых данных о держателях платёжных карт, как наиболее уязвимых, с точки зрения угроз конфиденциальности, местах. Также следует отметить, что стандарт регламентирует правила безопасной разработки, поддержки и эксплуатации платёжных систем, в том числе процедуры их мониторинга. Важную роль стандарт отводит разработке и поддержке базы нормативных документов системы менеджмента информационной безопасности.

Требования стандарта PCI DSS распространяются на банки, организации торговли и сервиса (ОТС), поставщиков технологических услуг и другие организации, деятельность которых связана с обработкой, передачей и хранением данных о держателях платёжных карт. Этим организациям следует озаботиться такими вопросами, как выделение платёжной инфраструктуры в отдельный сегмент, защита хранящихся и обрабатываемых карточных данных, создание эффективной системы менеджмента информационной безопасности и другими аспектами приведения в соответствие требованиям стандарта своей информационной инфраструктуры.

Как определяется соответствие банка требованиям PCI?

Международные платежные системы обязывают организации, на которые распространяются требования стандарта, проходить регулярную проверку соответствия этим требованиям. Правила проверки соответствия различаются в зависимости от вида организации и ежегодного количества обрабатываемых в ее инфраструктуре карточных транзакций. Внешний аудит на соответствие требованиям стандарта может выполнять компания, обладающая статусом Qualified Security Assessor (PCI

QSA), подготовленные такой компанией отчеты о соответствии принимаются международными платёжными системами.

Различают уровни сертификации для ОТС и других участников. Существуют следующие методы проверки соответствия требованиям стандарта PCI DSS:

- внешний QSA-аудит, выполняемой PCI QSA-компанией на объекте проверяемой организации;
- заполнение листа самооценки (SAQ);
- автоматизированное ASV-сканирование уязвимостей периметра сети.

Метод проверки соответствия, или комбинация методов, выбирается в зависимости от уровня сертификации объекта. Сертификация по высшим уровням должна проводиться аудиторской компанией, обладающей статусом QSA. Для остальных уровней привлечение QSA не является обязательным требованием. Однако QSA может оказать консалтинговые услуги для прохождения сертификации по любому уровню.

Сайт www.pcisecuritystandards.org является официальным сайтом Совета по стандартам безопасности индустрии платёжных карт. Совет формирует редакцию стандарта PCI DSS, проводит ежегодную сертификацию работников организаций и самих организаций на соответствие требованиям статуса организации PCI QSA. Сертифицированные Советом организации имеют право проводить работы по аудиту на соответствие PCI DSS с выдачей соответствующих сертификатов на соответствие PCI DSS.

В Республике Беларусь нет ни одной организации, имеющей статус PCI QSA, однако в регионе СЕМЕА имеют право оказывать услуги иностранные организации (61 организация). Из организаций на рынке СЕМЕА есть 23 организации, имеющие в штате русскоязычных экспертов (из них 12 организаций PCI QSA находятся на территории России или Украины).

Беседовал Драгун Сергей



Индикаторы несанкционированного доступа

Компания ООО «Смарт Бизнес Технолджи» предлагает индикаторы несанкционированного доступа, применяемые банковскими кредитными организациями.

Пломбу можно охарактеризовать как устройство, которое объективно (механически, без участия человека) способно надежно удостоверить свою собственную целостность или ее отсутствие.

Что такое «хорошая» пломба и что такое «плохая»? Лучше спрашивать – надежна она или нет в качестве сигнального устройства, и в какой степени данная модель подходит для целей пользователя?

Перечислим принципиальные критерии оценки надежности пломбировочного устройства (ПУ):

- обладает ли данное ПУ комплексом признаков, придающих каждому экземпляру свойство уникальности?
- эффективно ли ПУ в качестве индикатора – конструкция и применяемые материалы должны исключать возможность вскрытия с применением механических, температурных, химических и иных методов без оставления характерных следов (криминалистическая стойкость/ценность)?
- насколько вероятна возможность репликации (заводской подделки)?
- есть ли в широком доступе технические средства (материалы и технологии) для эффективной маскировки следов атаки?
- Прочие критерии оценки изделия:
 - достаточно ли конструкция ПУ соответствует объекту пломбирования и требованиям системы безопасности?
 - отсутствует ли производственный брак?
 - приемлема ли для потребителя цена?

Бизнес организации, в том числе бизнес банков, практически невозможно реализовать эффективно и с минимальными рисками без решения задач безопасности. Важнейшая составляющая банковского надзора и аудита – оценка деятельности бан-

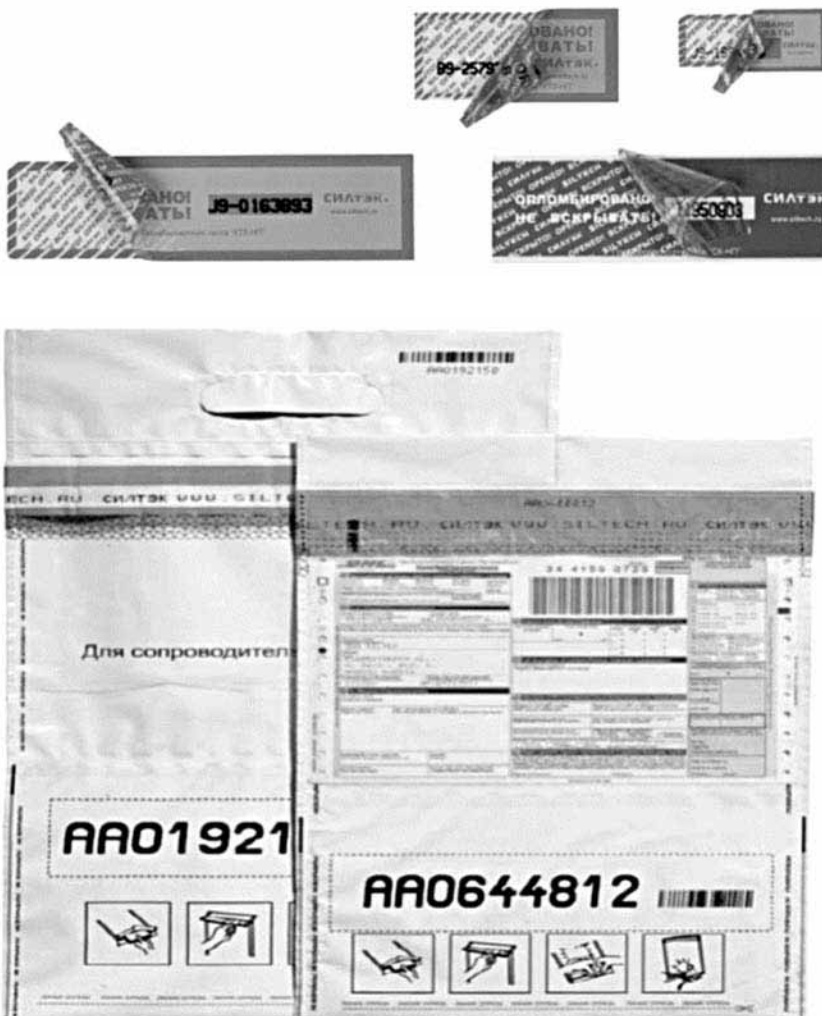
ка. Эта оценка во многом зависит от эффективности его систем безопасности.

Если укрепить пломбу на опечатываемом объекте таким образом, что вскрытие объекта пломбирования неизбежно повлечет нарушение целостности пломбы, пломба начинает выполнять функцию сигнального устройства: индикатора неприкосновенности или несанкционированного доступа

Сегодня белорусские банковские и иные кредитные организации всё более интенсивно применяют индикато-

ры несанкционированного доступа, разнообразные пломбировочные устройства. Целостность индикатора объективно свидетельствует о неприкосновенности объекта охраны, а нарушение целостности – о прорыве системы безопасности.

Банками индикаторы несанкционированного доступа применяются обычно для удостоверения сохранности денежных средств, иных ценностей, документов и прочих информационных носителей в процессе хранения и транспортировки, например, при инкассации денежных





средств и перевозке пластиковых карточек.

Индикаторы несанкционированного доступа применяются для удостоверения неприкосновенности офисной техники, содержимого АТМ-машин и их кассет, помещений и ключей к ним. На базе комплекса пломбируемых

сейф-контейнеров строится система безопасности внутреннего документооборота.

Применение индикаторов доступа наиболее эффективно в условиях, когда:

- неведение о состоявшемся прорыве системы безопасности связано с неприемлемыми рисками;
- действия персонала, обеспечивающего сохранность ценностей в процессе хранения и перемещения, нуждаются в объективном (независимом от человеческого фактора) контроле;
- процедура хранения и перемещения ценностей предусматривает их неоднократную передачу из рук в руки;
- решается задача по выстраиванию целостной системы безопасности, например, при организации внутреннего документооборота организации, сталкивающейся с рисками утечки информации или разукомплектования документов.

При этом ключевое условие эффективности индикаторов – продуманные процедуры их учёта, применения и мониторинга целостности. В любой системе безопасности очень важно осуществлять постоян-

ный контроль за тем, как система функционирует в целом, включая персонал.

Таким образом, современная пломба, как это называют юристы, представляет собой вещь, определенную индивидуальными признаками, или вещь, просто существующую в единственном экземпляре. Свинцовая же пломба – это вещь, определенная родовыми признаками. Закрытая свинцовая пломба может существовать во многих экземплярах, каждый из которых несет на себе один и тот же отпечаток. Ее можно сорвать и заменить такой же пломбой – факт замены, замечен не будет.

Высокая техническая и экономическая эффективность в этой задаче, принятых в наш ассортимент индикаторов несанкционированного доступа от ведущих мировых производителей, подтверждена не только отечественной, но и зарубежной многолетней практикой.

ООО «Смарт Бизнес Технолоджи»

+375(17) 510-94-09

+375(17) 510-96-59

+375(44) 777-97-01

УНП: 691581574

Семинары по вопросам банковской безопасности (на 2014 год*)

Организаторы:

- ООО «АэркомБел» (издатель журнала «Технологии безопасности»;
- Главное управление единого расчетного и информационного пространства Национального банка Республики Беларусь.

Март, 2014 г. Практический семинар:

«PCI DSS 2.0 – эффективные технические и экономические подходы к выполнению требований»

Апрель, 2014 г. Практический семинар:

«Расследование инцидентов информационной безопасности»

Приглашаем к участию: специалистов банковской и финансовой сферы, профильные компании и ведомства.

Предварительная регистрация на сайте aercom.by, по тел: 017-290-84-05

*Возможны изменения в графике проведения



Рынок СКУД в РБ – экспертные комментарии

В рамках разбора тематики развития СКУД в нашей стране мы провели опрос экспертов по основным вопросам развития систем и описанием текущей ситуации в сегменте.

1. Состояние рынка СКУД в РБ. Насколько белорусский рынок СКУД соответствует требованиям по эффективной защите всех потребительских сегментов?

2. Какова тенденция при установке СКУД на рынке:

- установка на этапе строительства?
- модернизация/наращивание существующих систем на функционирующем объекте?

3. Какие критерии преобладают у клиентов при запросах на оборудование:

- спрос на дешевое оборудование;
- запросы на надежность;
- предпочтение удобному и интуитивно понятному интерфейсу, возможности самостоятельной поддержки функционирования системы.

4. Какие основные требования к СКУД предъявляются сейчас, будут предъявляться в перспективе:

- гибкость СКУД;
- масштабируемость СКУД;

- интеграция СКУД с другими системами (охранными и управления предприятием).

5. Технологии идентификации на рынке РБ:

- Smart карты. Востребованность и переход на данную технологию в РБ;

- RFID, состояние и развитие на рынке РБ. Востребованность дальнобойных RFID считывателей, перспективы на рынке РБ;

- Биометрические системы. Востребованность. Какие технологии биометрии используются на рынке РБ. Прогноз развития на рынке РБ. Нишевой продукт и перспективы занятия доли рынка;

- Идентификация по нескольким параметрам, востребованность (чем обусловлена).

6. Каналы связи:

- IP-решения, востребованность, перспективы использования (PoE, Web интерфейс);

- RS – 485, востребованность, перспективы.

7. Прогноз на перспективу развития рынка:

- динамика развития;
- предпочтения заказчиков.



Григорьев Илья
Викторович,
учредитель Частного
предприятия «Фабрика
турникетов и систем»
г. Минск

Состояние рынка СКУД в РБ

Предложение вполне удовлетворяет спрос. Как тенденция – установка СКУД «для галочки», особенно на государственных объектах. С частным сектором проще, там больше ответственных, заинтересованных специалистов, которые разбираются в IT (в основном это системные администраторы предприятия), пытаются понять возможности и характеристики систем. Из моего опыта, только небольшое количество компаний полноценно используют все программные возможности СКУД, востребованность в ПО появляется только после происшествий.

Государственные программы по СКУД

На сегодняшний день проводится ряд государственных программ по установке СКУД на объектах. В частности активно реализуется программа Министерства образования РБ, создана комиссия, которая занимается вопросом автоматизации школ (в т.ч. установкой СКУД и СВН в школах), подключением к системе электронных дневников Schools.by и пр. Выделился ряд белорусских компаний, которые проводят установку программ по автоматизации школ, причем некоторые из них установку СКУД проводят за свой счет, монетизация происходит за

счет пользователей (SMS-сервис для родителей и пр.). Из проблематики существующих программ – отсутствие координации и единой платформы по автоматизации, что делает невозможным объединение подсистем как СКУД, СВН, ПО автоматизации и пр. Нам, как производителям, немного легче в этом плане, мы пошли по пути объединения и интеграции систем различных заинтересованных организаций в нашу систему, разработав тем самым некий единый комплекс по автоматизации школ, однако постоянное лоббирование государственных и частных компаний серьезно тормозит данный процесс.

Требования к СКУД, предъявляемые потребителем

Актуальна интеграция. Сегодня многие заказчики предъявляют требования к объединению подсистем безопасности (СКУД, СВН и пр.) на единой платформе. Это тенденция, к которой стремятся производители, мы, как компания-производитель, тоже работаем в этом направлении.

Многие решения, которые существуют под целевые задачи, просто не знакомы потребителям и заказываются после получения информации, например, так мы реализовываем функции «Контроль обходов охраны». Или вот пример. Многие предприятия платят немаленькие деньги за систему контроля посетителей, не зная, что в нашей системе она реализована просто как отдельная функция и абсолютно бесплатная. То же касается и функции «Компьютерный класс» для школ и др. учебных заведений.

Технологии идентификации на рынке РБ

Самая популярная, ввиду дешевизны, – пластиковая карта с чипом EM-Marlin (несмотря на разговоры по клонированию), думаю, популярность её еще будет долгой, т.к. это целый бизнес, однако проявляется тенденция к гибридным системам, вроде банковских пластиковых карт с чипом Mifire Plus с третьим уровнем доступа. Это достаточно защищенный продукт, однако в данный мо-

мент очень мало кто производит считывающие устройства для таких карт. В частности, наша компания такой считыватель уже разработала.

Биометрические системы востребованы, спрос на них с каждым годом активно растет, хотя существует предвзятое отношение потребителей о высокой степени ошибок и малой скорости идентификации при работе биометрических систем, сохранившееся с прошлых лет. Это не так, современные системы биометрии достаточно надежны. Если говорить, например, о сканерах отпечатков пальцев на основе не самого отпечатка, а рисунка вены, то такие сканеры в Японии уже давно используются в обычных банкоматах. Думаю, что в ближайшее время они получат большее распространение, в т.ч. с нашей помощью, т.к. сейчас мы их внедряем в собственные продукты.

Каналы связи

При установке СКУД все больше востребованы IP-решения. RS-485, 422 больше промышленный протокол и используется в основном там, где локальные сети не проложены, либо где нужно тянуть сеть на большие

расстояния. Но Ethernet его постепенно выдавливает, например мы пару лет назад добавили в наш контроллер поддержку Ethernet, сегодня по анализу продаж 90% поставленного оборудования реализуется с функцией работы по Ethernet. Есть востребованность и примеры использования 3G. Это предприятия, с распределенной структурой, которые осуществляют мониторинг систем на удаленных объектах, в т.ч. и СКУД по 3G каналу.

Прогноз на перспективу развития рынка

Бурной динамики развития СКУД в Беларуси, на мой взгляд, не планируется. Количество предприятий ограничено, большинство из них уже оборудованы теми или иными СКУД. Замена оборудования в ближайшие годы особо не актуальна. Скорее более актуально наращивание функционала существующих систем. Возможен рост в сегменте объектов по государственным программам. Это те же школы, транспорт и т.п. Монтажным организациям-интеграторам, я считаю, работа всегда найдется, однако мы же, как производитель, больше ориентируемся на российский и европейский рынки.



Царев Андрей
Владимирович,
директор Просвет ИВ
ООО

Состояние рынка СКУД в РБ

Существующие на сегодняшний день предложения удовлетворяют спрос в технической части. Основной силой в РБ, формирующей спрос в сегменте СКУД, является МВД. Именно по инициативе данной структуры появились постановления обязывающие организовывать СКУД в общественных учреждениях, в т.ч. в школах. МВД сейчас занимает самую активную позицию на рынке, т.к. все самые значимые проекты в стране реализуются за счет бюджетных средств, а это значит, что и влияние на проекты могут оказывать в первую очередь государственные структуры. Влияние коммерческих организаций в части формирования спроса на рынке СКУД – информационное, например, предоставление информации о новых продуктах и возможностях систем.

Какова тенденция при установке СКУД на рынке?

80% проектов – это модернизация существующих объектов. Из них 60% – это новая установка на старых предприятиях, где не существовало практически ничего, 40% – замена старого оборудования.

Какие критерии преобладают у клиентов при запросах на оборудование?

Цена-качество. Сегмент рынка, касающийся СКУД, более грамотный. На этот рынок пока не пришли китайские системы в массовом количестве. В Беларуси работает не так много торговых марок, которые могут предложить комплексный проект со всеми возможностями интеграции (Болид, Ровалэнт, Акова, PERCo). Если еще 10 лет назад на рынке преобладали импортные системы, то сейчас основная масса – это российские системы, вытеснившие

импортные по критерию цена-качество. Российские СКУД достигли достаточно высокого уровня надежности, предлагая более конкурентоспособные цены, по сравнению с европейскими и американскими производителями. Что касается белорусских производителей, то нельзя не отметить, что за последнее время ими сделан огромный шаг вперед, хотя остаются вопросы в технической части и полноте интеграции со вспомогательными системами.

Принятие решения на предприятии об установке СКУД

Поскольку основные потребители интегрированных (масштабных) систем – это холдинги и государственные структуры, то там, как правило, есть отделы, которые принимают решения о необходимости внедрения СКУД и анализируют дальнейшую эффективность этого решения. Затем наступает этап принятия решения на уровне руководства.

Выбор систем, при прочих равных условиях, чаще всего осуществляется по субъективным критериям (с какой-то системой уже ранее работали, о какой-то системе больше слышали).

Требования к СКУД со стороны заказчика сейчас/в перспективе

Гибкость, масштабируемость, возможность интеграции. В настоящее время конечный потребитель достаточно продвинут, он четко знает, какой результат хочет получить. Даже на самом маленьком предприятии руководство понимает, что повышение эффективности труда может быть достигнуто путем повышения трудовой дисциплины. Это общая тенденция, которая будет влиять на рынок и дальше. Со временем это все перерастет в системные интеграции.

Что касается системных интеграций, то на сегодняшний день их существует очень много, но данные реализации это, как правило, частная инициатива какого-либо разработчика и приводят они к частному результату. Универсальной интеграции различных систем СКУД и вспомогательных систем пока не существует, т.к. нет универсальных протоколов обмена. Каждый производитель предлагает свой способ интеграции. Инициатором, как правило, выступает продвинутый потребитель. Почти все ведущие разработчики СКУД имеют оборудование, которое инте-

грировано в той или иной степени с различными вспомогательными системами.

Кроме системных интеграций существуют еще и пространственные интеграции. Многие поставщики позволяют производить пространственную интеграцию в пределах сети Интернет всех собственных систем контроля доступа. У нас в стране данный вид интеграций пока развит очень слабо.

Технологии идентификации на рынке РФ

Следует разделять идентификацию массовую и персональную на специализированных узлах доступа. Заводская проходная и хранилище Национального Банка РФ требуют разных уровней идентификации. Соответственно, востребованность имеют все системы. Но я думаю, что сложные многофакторные и, как следствие, дорогие и относительно «медленные» системы идентификации, напр. – идентификация по сетчатке глаза, никогда не получат такого массового распространения, как более дешевые, а главное «быстрые» системы, напр. – бесконтактные карты.

Биометрические системы в стране развиты очень слабо. Востребованность есть, но только в определенных сегментах. Компании, работающие со СКУД, не являются производителями самих биометрических идентификаторов, они их покупают и интегрируют со своими системами. Сама система идентификации очень сложная и часто занимает немало времени. Спрос есть, но очень незначительный.

Проекты идентификации по нескольким параметрам востребованы на специальных объектах, КВО, банках и пр.

Каналы связи

IP-решения в СКУД реализованы у всех производителей в силу того, что есть спрос на российском и мировом рынках. На белорусском рынке он также есть, но есть трудности с каналами передачи данных, сдерживает их высокая

стоимость создания и аренды. Техническая возможность развития IP-каналов есть. Почти все производители систем безопасности готовы реализовывать любую распределенную систему. Сложность заключается в том, что для установки СКУД с интегрированной системой СВН требуется широкий канал передачи данных, а наш монополист «Белтелеком» не готов предоставить канал необходимой ширины. Оптики много, но она организована так, что даже с одной улицы на другую зачастую передавать данные с большой скоростью невозможно. Если говорить о финансовой составляющей, то даже такие заведения как, например, игорные дома, не готовы платить такие деньги за аренду, либо создание каналов передачи данных с высокой пропускной способностью.

Основные протоколы передачи данных в системах СКУД RS-485 и TCP/IP прекрасно сосуществуют, дополняя друг друга.

Прогноз на перспективу развития рынка

Мы отстаем от мировых тенденций СКУД в части реализации возможностей систем. Мир более продвинут в части использования IP-систем. Например, немецкие производители уже не первый год нам предлагают свои решения СКУД, такие как облачные хранилища данных, когда вся информация хранится на сервере производителя. Клиенту предоставляется ключ шифрования, он заходит в свою клиентскую часть, откуда управляет своим веб-офисом. Это пример полноценной распределенной системы. Национальный рынок пока не готов к таким решениям в силу высокой стоимости реализации.

СКУД как полноценный элемент «умного дома»

Востребованность на рынке есть, готовности потенциальных потребителей нет. Заказчики не готовы платить за системы такого уровня. Строительство офисов на сегодняшний день чаще всего заканчивается установкой простейшей СКУД «свой-чужой».



Петлицкий Александр,
заместитель
директора по технике
ООО «РОВАЛЭНТ-
КОМПЛЕКС»

Состояние рынка СКУД в РФ

Существует устойчивый спрос на рынке, есть выбор систем.

Какова тенденция при установке СКУД на рынке

Большая часть реализуемых нами проектов СКУД – модернизация.

Какие критерии преобладают у клиентов при запросах на оборудование?

Если это бюджетная организация или проект СКУД на этапе строительства, то запрос идет на дешевое оборудование. Если коммерческий сектор, то делают «для себя», соответственно закладывают оборудование иного (более высокого) уровня. В последнее время наблюдается тенденция в запросах на надежность и дизайн СКУД.

Основные требования, предъявляемые к СКУД сейчас со стороны заказчиков?

С каждым годом более востребованной становится интеграция СКУД с другими системами (напр. охранными, СВН, управления предприятием). Есть растущая тенденция к спросу на биометрические системы идентификации, в т.ч. сложные – идентификация по сетчатке, лицу.

Технологии идентификации на рынке РФ

В основном используются магнитные карты. Наблюдается востребованность биометрических решений, в основном со стороны коммерческого сектора, предприятий с иностранным капиталом, где биометрия заложена во внутренние стандарты. Поэтому мы интегрировали их в свои решения. Но если брать по реализации, то биометрические системы внедряются примерно в 5% от всех реализованных СКД.

Актуальность идентификации по нескольким параметрам

Достаточно редкие запросы. В моей практике максимальной была двойная идентификация, по сетчатке глаза и лицу.

Каналы связи

Основная масса заказчиков приходят к Ethernet и IP-решениям. Уже недорого и удобно.

Прогноз на перспективу развития рынка

Есть ряд критически важных объектов, где СКУД всегда будет высокого уровня. На объектах массового сегмента все будет зависеть от экономики и ситуаций. Зачастую понимание по необходимости установки СКУД приходит после происшествий на объекте.

ПРОИЗВОДСТВО ТУРНИКЕТОВ, СИСТЕМ КОНТРОЛЯ ДОСТУПА И УЧЕТА РАБОЧЕГО ВРЕМЕНИ

Частное предприятие "Фабрика турникетов и систем"

Производим:

- турникеты электромеханические
- турникеты роторные
- модульные ограждения
- калитки автоматические
- контроллеры системы доступа
- считыватели бесконтактные
- терминалы учета рабочего времени
- системы контроля обходов охраны
- биометрические системы
- автономные системы

Бесплатное программное обеспечение для предприятий и школ

Высокое качество. Наличие на складе.
Скидки монтажным организациям!



Турникет-трипод



Турникет-трипод тумбовый

Новинка! Кованые турникеты ручной работы с патиной под золото!

тел. в Минске (017) 508-77-88, 508-77-55

WWW.FABRIKA-TURNIKETOV.BY

УНН: 191600318



НОВЫЕ ВОЗМОЖНОСТИ ПО "ЭПИКУР V3"

Вот уже 9 лет наша компания занимается разработкой программного обеспечения системы контроля доступа и учета рабочего времени "Эпикур V3". За это время программа стала самой совершенной системой учета рабочего времени из существующих на рынке, оставаясь при этом по-прежнему бесплатной. Несмотря на это, наши разработчики постоянно дорабатывают систему, наращивая ее функционал. Предлагаем ознакомиться с нашими последними доработками.

Новый модуль для учебных заведений "Школа"

Предназначен для упрощенного использования системы в учебных заведениях, в частности в школах, где есть определенная специфика и не всегда есть в штате достаточно квалифицированные специалисты для настройки системы и ее использования. Поддержка SMS оповещений родителей о приходе/уходе учащегося, настраиваемые расписания, дисциплинарные отчеты и мн. др.

Новый модуль "Компьютерный класс"

Входит в состав модуля "Школа". Позволяет преподавателю информатики вести мониторинг в компьютерном классе, видеть на своем экране все что происходит на удаленных компьютерах, удаленно блокировать/разблокировать их, посылать сообщения. Система позволяет вести расписание занятий, а также имеет возможность авторизации пользователя по карте учащегося и в дальнейшем получение отчетности.

Новый модуль контроля обходов персоналом

Основная задача системы - контроль прохождения маршрутов персоналом (например, сторожами). В настройках модуля создаются маршруты движения (регистрируются RFID метки) и производятся настройки маршрута (время начала, конца обхода, последовательность прохождения, допустимое время прохождения и т. д.) После передачи данных с автономного коммуникатора сторожа в компьютер данные анализируются, составляется необходимая отчетность по сотруднику.

И многое другое

АВТОМАТИЧЕСКИЕ ШЛАГБАУМЫ для управления контролем доступа ТС-101Х



При помощи механической муфты и ключа можно поднять стрелу шлагбаума даже если напряжение питания отключено.

- Шлагбаумы поставляются в исполнениях для лево- и правосторонней установки;
- Стрела автоматически вернется в исходное положение в случае, если при поднятии или опускании стрелы возникнут какие-либо препятствия. Инфракрасные фотоэлементы устанавливаются по желанию заказчика;
- Процесс работы шлагбаума бесшумен;
- Применение петлевого детектора, монтируемого под дорожным покрытием в зоне работы шлагбаума, и дополнительной системы управления расширяют функциональные возможности шлагбаума (поставляются отдельно);
- Зеленый и красный светофоры могут применяться для обозначения положения.

Технические характеристики:

Модель: ТС101Х

Предлагаем 3 типа шлагбаумов:

- Скоростной, ТС-101L, время подъема/опускания стрелы 1 сек., применяется стрела 3 м;
- Среднескоростной, ТС-101М, время подъема/опускания стрелы 3 сек., применяется стрела 4,5 м;
- Медленный, ТС-101Н, время подъема/опускания стрелы 6 сек., применяется стрела 6 м;
- Температура эксплуатации: -40 °C +75 °C;
- Рабочая температура: -20 °C +75 °C;
- Питание: 220 V±10%, 50 Hz/60 Hz / 110 V±10%, 50 Hz/60 Hz;
- Потребляемая мощность: 80 W;
- Относительная влажность: 90%;
- Максимальная дистанция уверенного радиоуправления - не более 30 м.

Комплект поставки, габаритные размеры:

- | | |
|---|--------|
| - Длина основания стойки: | 329 мм |
| - Ширина стойки: | 301 мм |
| - Высота стойки: | 954 мм |
| - Кнопочный стационарный пульт управления по радиоканалу (ипит.=220 в). 12*8*4 см | 1 ед. |
| - Приемник радиосигнала | 1 ед. |
| - Ключ для соединения/рассоединения механической муфты привода стрелы | 1 ед. |
| - Миниатюрный пульт управления (радиобрелок) | 2 ед. |
| - Опора для стрелы | 1 ед. |
| - Инфракрасные фотоэлементы (поставляются по желанию клиента) | |

ПРИВОДЫ

Привод для РАСПАШНЫХ ворот WJKMB101



Параметры

Питание: 220В(120W)
Вес ворот: 300кг (макс)
Ширина ворот: 2,5м (макс)

Функция открытия/закрытия с помощью пульта дистанционного управления.

Определение препятствий при движении створок и автоматическое отключение.

Монтаж и настройка не занимают много времени.

Подключение предупреждающей лампы и подсветки проезда с подстраиваемым временем включения.

Автоматическое закрытие с расширенным временным диапазоном.

Большие возможности по настройке и регулировке.

Привод для РАЗДВИЖНЫХ ворот WJKMP102



Параметры

Питание: 220В(120W)
Вес ворот: 300кг (макс)
Ширина ворот: 2,5м (макс)

УНП: 101295470

ЗАО «Техноцентр»,
Минск. Ул. Короля, д. 9 к 4
(2-ой этаж)

ТЕХНО-ЦЕНТР

собственное производство,
Республика Беларусь

Тел./факс: (017) 299-55-55,
(017) 245-47-28, 245-44-98,
(017) 245-49-80, 245-39-47

office@techno-centre.com

www.techno-centre.com



Волнистый Сергей
Викторович, директор
ООО «Импросигнал»

Состояние рынка СКУД в РБ

Считаю, что уровень технических предложений рынка СКУД в стране достаточно широк и в состоянии удовлетворить практически любые запросы Заказчиков.

Каковы тенденции при установке СКУД на рынке?

Сложно ответить однозначно, мы сталкиваемся с запросами по подготовке предложений по выработке проектного решения для СКУД как на этапе самого проектирования, так и на этапе уже функционирующего объекта. Из практики, наверное, чаще реализовываются проекты на этапе функционирования объекта. Возможно, это связано со сроком жизни процесса проектирования и наши предложения, подготовленные на этапе строительства, еще не дошли до окончательной реализации. Правда прослеживается еще и проблема, состоящая в том, что на этапе проектирования объекта мало кто из Заказчиков может достаточно точно спланировать ТЗ на СКУД.

Какие критерии преобладают у клиентов при запросах на оборудование?

Запросы идут очень широкие: кто-то ищет простейшие системы, кому-то нужны системы достаточно высокого уровня. Мы стараемся закладывать в свои предложения только проверенное оборудование, так как только в этом случае можем

гарантировать устойчивую работу, как запорных устройств, так и контролеров и ПО.

Есть потребность в СКУД для небольших объектов, где кол-во пользователей малая и выделять или нанимать для обслуживания и конфигурирования системы (добавление/удаление пользователей, получение отчетов, задание прав пользователей) отдельно инженера нецелесообразно. В связи с чем ряд производителей, понимая указанные запросы, реагирует, предлагая ПО с максимально удобным и понятным интерфейсом для неквалифицированного пользователя.

Какие основные требования к СКУД предъявляются сейчас, будут предъявляться в перспективе?

Столкнулись с тем, что сами вынуждены в ряде случаев предлагать масштабируемые системы СКУД, поскольку Заказчик на этапе ТЗ бывает достаточно близорук и не всегда может объективно оценить свои потребности. Что касается интеграции, есть потребность увязки как с охранными системами, так и с системами видеонаблюдения, также ряд Заказчиков готов на предприятиях внедрять СКУД на глубоком системном уровне.

Технологии идентификации на рынке РБ

В настоящий момент у нас в работе находится проект СКУД большого производственного предприятия, где для управления несколькими транспортными воротами применяется RFID считыватели с дальностью считывания больше 5 м, при этом карты доступа клеятся на лобовое стекло автомобилей.

Случаи применения нашей компанией оборудования с биометрией пока больше исключение, чем практика.

Каналы связи

Для больших систем стараемся применять IP-решения.

Прогноз на перспективу развития рынка

Рынок готов потреблять и использовать оборудование СКУД, объемы будут значительно расти как минимум за счет использования в секторе малых, небольших и средних по численности сотрудников предприятий.



Марковник Денис
Викторович, инженер
технического отдела,
компания «Унибелус»

Состояние рынка СКУД в РБ

Рынок насыщен, присутствуют системы от производителей из дальнего и ближнего зарубежья, которые позволяют обеспечить эффективную защиту всех потребительских сегментов.

Тенденции при установке СКУД на рынке

На сегодняшний день большинство проектов это модернизация/наращивание существующих систем на функционирующем объекте.

Критерии клиентов при запросах на оборудование

На сегодняшний день основными критериями являются надежность и многофункциональность системы.

Требования, предъявляемые к СКУД сейчас/в перспективе

Масштабируемость и возможность интеграции с другими системами.

Технологии идентификации на рынке РБ

Smart-карты – востребованность таких карт в системах СКУД на сегодняшний день минимальна, и поступательный процесс

перехода на smart-карты в Беларуси может затянуться.

RFID – примеров успешных инсталляций и последующего эффективного использования RFID достаточно, и перспективы увеличения таких систем на рынке есть.

Биометрические системы – на сегодняшний день являются востребованными, максимально распространены устройства считывания отпечатка пальца, геометрии руки, рисунка радужной оболочки глаза. В ближайшей перспективе как минимум 30% рынка будет принадлежать именно таким системам.

Идентификация по нескольким параметрам – используется редко, хотя большинство интеллектуальных считывателей позволяют применять такой способ без дополнительных капиталовложений. Критически важные точки на КВО – места, где многоуровневая идентификация применяется сейчас в РБ.

Каналы связи

IP-решения – уже на сегодняшний день IP-решения в разы чаще используются, их доля будет постоянно увеличиваться. Увеличение кол-во устройств (контроллеров, интеллектуальных считывателей), поддерживающих POE, наряду со снижением стоимости инжекторов питания и сетевых коммутаторов POE, будет способствовать увеличению доли IP на рынке СКУД. RS – 485 – нет перспектив.

Прогноз на перспективу развития рынка

Ничего революционного на рынке СКУД в ближайшее время не произойдет. Востребованными будут комбинированные системы (биометрия + бесконтактные карты Mifare, iClass SE), программное и аппаратное обеспечение которых обладает максимальной надежностью и обновляется не реже одного-двух раз в год.



Парсиев Дмитрий,
директор компании
«ВидеоСкуд»

Состояние рынка СКУД в РБ

На рынке безопасности Беларуси присутствуют различные технические решения СКУД, в т.ч. разработанные передовыми иностранными компаниями и отвечающие самым требовательным запросам. Встречаются идентификация по отпечаткам пальцев, сетчатке глаза, по сканированию овала лица. Но, к сожалению, наш опыт использования данных технологий говорит о «сырости», либо очень завышенной цене.

Какова тенденция при установке СКУД на рынке?

Последние годы все чаще СКУД проектируется на этапе строительства, в частности для большинства объектов с массовым пребыванием людей. Такой подход позволяет учесть основные функциональные задачи, перспективы развития и модернизации системы. При модернизации существующих систем Заказчики, как правило, вынуждены наращивать систему элементами именно установленной системы (из-за отсутствия единых протоколов обмена информацией) или полностью заменять систему на иную.

Критерии клиентов при запросах на оборудование

Спрос на дешевое оборудование в секторе СКУД, как правило, присущ малым автономным системам. Многофункциональные сетевые системы в основном имеют одинаковый уровень цен. Наша практика показывает, что Заказчики предпочитают СКУД с ПО на русском языке, с интуитивно понятным интерфейсом, общепринятыми терминами и определениями, что упрощает эксплуатацию и обслуживание.

Требования к СКУД сейчас/в перспективе

Гибкость СКУД в рамках единой системы одного производителя легко обеспечивается. К сожалению, отсутствие единых протоколов обмена информацией (за исключением считывателей) не позволяет использовать компоненты разных производителей.

Интеграция СКУД с элементами охранных и пожарных систем осуществляется, как правило, на релейном уровне. Давно используется разблокировка дверей и иных элементов ограничения доступа при эвакуации людей. В этом случае иногда возникают «противоречия» в одновременном взаимодействии СКУД, ОС и АПС.

В части интеграции – наша компания неоднократно интегрировала СКУД в системы управления предприятием: взаимодействие с бухгалтерией (начисление ЗРП), столовой (расчет за обед по карточке доступа), библиотекой (получение книг), гостиницы (получение платных услуг) и т.д., спрос на такие системы растет.

Технологии идентификации на рынке РБ

Smart-карты – будут востребованы при развитии интеграции СКУД с другими системами (управления предприятием).

Технология RFID – к сожалению, еще достаточно дорога и не развита в Беларуси. Тем не менее, мы уже выполнили несколько подобных объектов.

Биометрические системы – на рынке в основном пред-

ставлены оптическими сканерами отпечатков пальцев, в меньшей степени емкостными (более надежными). Биометрия сканирования сетчатки глаза и овала лица еще достаточно дорогая. При установке биометрических систем разных производителей мы неоднократно встречали людей, отпечатки пальцев которых не сканируются современными системами – это биологическая особенность.

Каналы связи

IP-решения в СКУД давно стали нормой и как следствие, все технологии присущие IP-системам в целом, переключались и в принципы построения СКУД. RS-485, на мой взгляд, будет пользоваться спросом, т.к. обеспечивает дешевый помехоустойчивый, относительно «длинный» канал связи. Конечно скорость обмена информацией в этом канале связи незначительная, но вполне достаточная для организации некоторых сегментов СКУД.

Прогноз на перспективу развития рынка

Динамика развития СКУД в Беларуси полностью повторяет общепринятые мировые тенденции, т.е. никаких революций в этой области не предвидится. Наши клиенты, как правило, заказывают системы с учетом времени работы персонала с использованием RFID карт EM Marine (редко HID ProxCard II для повышения имитостойкости). Для построения интегрированных систем используем карты MIFARE с собственной памятью, позволяющей хранить и изменять информацию о пользователе. Думаю, что тенденции сохранятся. ■

Промышленные биометрические системы собственного производства:

Система учета рабочего времени
Bioscan ACS TT;



Система контроля доступа
Bioscan ACS;

Сканер отпечатков пальцев
Bioscan 21;

Биометрический турникет
Bioscan Wicket;



Биометрический WEB-сервис;
RFID считыватели
и электронные карты;

Системы удаленного мониторинга
и архивирования параметров;



Автоматизация производства.

BioSoftTrade

ООО «БиоСофтТрейд»

Тел.: (017) 260-96-67; Тел./факс: (017) 260-94-43

Velcom: (029) 326-38-30; MTC: (029) 750-66-20.

www.biosofttrade.by

www.biosofttrade.com

УНП 190739708

Вниманию руководителей предприятий и служб безопасности!

Изменения в лицензионных правах на использование авторского программного продукта «ВОРОН-НЕЙРО» или «ЗУБР-НЕЙРО» на территории Республики Беларусь



Компания «Прикладная радиофизика», являясь разработчиком и производителем волоконно-оптических средств охраны периметров, выпускаемых по технологии «ВОРОН™», доводит до сведения всех участников рынка технических средств охраны Республики Беларусь следующее:

- с 01.06.2013 г. ООО "Прикладная радиофизика" полностью прекратила поставки для ООО "Гамбитфорт" всех комплектующих изделий и программных продуктов, на основе которых (за исключением шкафа и монитора) выпускалось волоконно-оптическое средство охраны периметров «Зубр» под эгидой ООО «Гамбитфорт» в Республике Беларусь;

- ООО «Гамбитфорт» не является представителем компании «Прикладная радиофизика» в Республике Беларусь;

- ООО «Гамбитфорт» не имеет законных прав для производства периметровых средств охраны на основе технологии «ВОРОН™»;

- ООО «Гамбитфорт» не имеет достаточной квалификации для самостоятельного производства, монтажа и обслуживания волоконно-оптических средств охраны периметров на основе технологии «ВОРОН™»;

- ООО «Гамбитфорт» не имеет лицензионных прав на использование

авторского программного продукта «ВОРОН-НЕЙРО» или «ЗУБР-НЕЙРО».

Просим проявлять осторожность при получении предложений о поставке волоконно-оптических средств периметровой охраны с любым названием, если оно исходит не от компании «Прикладная радиофизика».

По всем возникающим вопросам, связанным с применением волоконно-оптических средств для охраны периметров, просим обращаться в компанию «Прикладная радиофизика».

ООО «Прикладная радиофизика»
142432 Московская обл.,
г. Черноголовка,
Северный проезд, д.1
Тел.: +7 496 524 26 33;
+7 926 248 73 62
www.neurophotonica.ru
info@neurophotonica.ru

БЕЗОПАСНЫЙ ДОМ

ПРОЕКТИРОВАНИЕ : МОНТАЖ : ОБСЛУЖИВАНИЕ

Проектирование, монтаж, наладка и техническое обслуживание:

- систем пожарной сигнализации;
- систем оповещения о пожаре;
- систем охранной сигнализации;
- систем телевизионного видеонаблюдения и контроля управления доступом;
- локальных вычислительных сетей (ЛВС) и структурированных кабельных сетей (СКС);
- компьютерных сетей с использованием витой пары и волоконно-оптического кабеля;
- учреждений автоматических телефонных станций (мини-АТС);
- систем и сетей громкоговорящей, диспетчерской связи.

ОДО «БЕЗОПАСНЫЙ ДОМ»
 220094, г. Минск, 2-й Велосипедный пер., д. 30, комн. 402
 Тел./Факс: (017) 298-38-05(15); (029) 150-95-97
www.odobd.by, odobd@mail.ru

Лицензии:

№02010/6670 выдана МВД РБ от 03.03.2006 г. №8км,
действительна до 02.03.2021 г.;

№ 02300/1268 выдана МЧС РБ от 15.03.2006 г. №4км,
действительна до 14.03.2016 г.

Шлюзовая кабина рентгеновского досмотра – инновационная технология контроля доступа посетителей

АДАНИ предлагает оригинальные технологии и комплексные технические решения в области рентгеновских систем обеспечения безопасности, на базе которых создано семейство специализированных рентгенографических сканеров для досмотра человека, багажа, грузов и транспортных средств. Рентгеновские инспекционные системы персонального досмотра КОНПАСС, основанные на использовании проникающего рентгеновского излучения малой интенсивности, отлично зарекомендовали себя более чем в 25 странах мира, как наиболее эффективное средство обеспечения безопасности. На этих же принципах разработана и система контроля доступа с возможностью персонального рентгеновского досмотра КОНПАСС-ДОСТУП (К-ДОСТУП).

Шлюзовые кабины (тамбур-шлюзы) давно существуют на рынке и являются одним из важнейших звеньев в цепи обеспечения комплексной безопасности крупнейших объектов: правительственных и государственных учреждений, аэропортов, железнодорожных вокзалов, банков, тюрем и т.п.

Основная функция шлюзовой кабины – защита от нежелательного входа на объект, проноса оружия, выноса оборудования, разделение людских потоков, противодействие терроризму, информирование о захвате заложников и т.д.

В стандартные шлюзовые кабины могут дополнительно интегрироваться специальные датчики для обнаружения металлических предметов, радиоактивных и отравляющих веществ. Посредством встроенной камеры может передаваться видеоизображение людей. С помощью биометрических считывателей может осуществляться идентификация личности.

В то же время, при наличии большого количества специальных встроенных датчиков часто происходит их ложное срабатывание, шлюзовая камера бло-

кируется, и частью процедуры контроля становится обязательный досмотр посетителя. В результате существенно сокращается пропускная способность, и практически сводятся к минимуму все удобства и преимущества шлюзовых кабин.

Система К-ДОСТУП является новинкой в продуктовой линейке АДАНИ. Данный продукт представляет собой шлюзовую кабину стандартной конфигурации, составной частью которой является сканирующая система персонального досмотра КОНПАСС. Уникальной особенностью конструкции является скрытое сканирование посетителя (он не подозревает о процедуре досмотра), что исключительно важно для принятия оперативных решений при выявлении лиц с преступными намерениями или террористов.

Дополнительно кабина может быть оснащена автоматической системой сканирования посетителей по сигналу одного из специальных датчиков, а также автоматической системой детектирования (распознавания) опасных предметов. Оператор-контролер осуществляет контроль доступа дистанционно с помощью системы видеонаблюдения в отдельном помещении и, в случае необходимости, подает сигнал тревоги.

В условиях возросших террористических угроз кабина К-ДОСТУП позволяет поставить надежный барьер террористам-смертникам с пластиковой взрывчаткой или нетрадиционным оружием, спрятанными под одеждой или в естественных полостях тела.

Система К-ДОСТУП – идеальное решение для обеспечения безопасности инфраструктуры, VIP-зданий, железнодорожных и авиационных вокзалов, а также военных объектов.



«АДАНИ» УП,
Республика Беларусь, 220075,
г. Минск, ул. Селицкого, 7
Тел./факс: (017) 346-29-03, 346-29-02
E-mail: info@adani.by
Сайт: www.adanisystems.com

УНП: 100054851



СКУД на базе оборудования «Болид»: сегодня и завтра

Можно смело утверждать, что системы контроля и управления доступом (СКУД) на базе ИСО «Орион» являются сегодня наиболее применимыми и конкурентоспособными на рынках стран СНГ. Это объясняется, прежде всего, оптимальным соотношением функционала, качества и цены этих систем.

ИСО «Орион» – это не только СКУД. Система представляет собой наиболее универсальный аппаратно-программный комплекс среди представленных на рынке. Комплекс позволяет в рамках единого информационного пространства строить взаимодействующие системы охранной и пожарной сигнализации (ОПС), пожарной автоматики, СКУД, видеонаблюдения и диспетчеризации. В основе архитектуры ИСО «Орион» заложен модульный принцип: она состоит из множества распределяемых по защищаемому объекту взаимозаменяемых приборов, которые, в зависимости от настроек, решают одну или несколько из указанных выше задач. В качестве транспортного уровня используются RS-485 интерфейс и, как правило, сети Ethernet. Кроме того, существуют решения по организации беспроводных линий связи.

Внедрение СКУД на базе ИСО «Орион» позволяет решить три основные задачи:

- Организация охраны предприятия.

Интеграция СКУД с системой ОПС для комплексного решения задач безопасности. Обеспечение реакции охранной составляющей системы на попытки несанкционированного доступа, взлома дверей и т.д. Возможность автоматической постановки/снятия с охраны помещений по факту прохода в зону доступа сотрудника. Предоставление свободного доступа в случае возникновения пожара.

- Контроль перемещения персонала.

Каждому пользователю достаточно выдать один ключ ("Touch Memory" или карту «Proximity») для

его идентификации системой охраны объекта, что позволит исключить возможность «праздного шатания» сотрудников и обеспечит правильную организацию труда.

- Организация учета.

Создание системы учета рабочего времени (на основе анализа времени прихода/ухода сотрудников с предприятия или своего рабочего места). Контроль места нахождения сотрудника на объекте с точностью до зоны доступа.

Контроллеры

Базовым элементом построения СКУД являются контроллеры доступа «С2000-2». В отличие от приборов иных производителей, «С2000-2» – универсальный прибор, для которого алгоритм работы определяет сам пользователь. Каждый контроллер может обслуживать в зависимости от настроек: две двери с одним считывателем или одну дверь с контролем направления прохода, или турникет, или шлагбаум, или шлюз.



Контроллеры «С2000-2» на аппаратном уровне поддерживают сетевой и зональный режимы запрета повторного прохода (antipassback). При работе в системе под управлением пульта «С2000М» или ПО АРМ «Орион Про» сообщения о проходах ретранслируются всем контроллерам системы, и правило antipassback срабатывает для всех точек доступа на входе в одно помещение. Функция "Зональный antipassback" ("Контроль маршрута") позволяет сделать этот режим более строгим: в этом случае учитываются проходы в различные зоны

доступа, и если предпринимается попытка прохода через один из считывателей контроллера, то для выполнения правила antipassback требуется, чтобы последний зарегистрированный проход был в зону, доступ в которую контролируется другим считывателем данного контроллера.

«С2000-2» также позволяют задавать специальные режимы доступа для отдельных групп пользователей: доступ с дополнительным кодом (поддержка многофакторной аутентификации), а также доступ по правилу двух/трех лиц или доступ с подтверждением (доступ по предъявлению двух/трех идентификаторов различных пользователей с согласованными уровнями доступа).

Для различных групп пользователей существует функционал ограничения доступа по времени для каждой точки/зоны доступа (окна времени). Система дает возможность определять временные интервалы отдельно для рабочих и праздничных дней, осуществлять перенос рабочих дней, создавать скользящие графики работы и даже сложные графики, не имеющие явно выраженного периода повторения.

Для предоставления доступа широкому кругу лиц, идентификаторы которых затруднительно или невозможно занести в память контроллера (например, их слишком много) и при условии, что код всех этих идентификаторов удовлетворяет некоторому правилу (например, начинается с определенной последовательности цифр), предназначен механизм так называемых «шаблонов доступа». Этот функционал поможет решить задачу организации доступа в зону банкоматов при отделениях банков.

Контроллеры доступа передают тревожные извещения в случаях несанкционированного открытия дверей или заградительных устройств (без разрешения на доступ) и их блокировки (открытие на время, превышающее настроенный таймаут).



Управление

Для управления ИСО «Орион» на верхнем уровне разработано ПО АРМ «Орион Про». Основные задачи ПО СКУД – хранение и обработка журнала событий системы (создание отчетов по передвижениям и учету рабочего времени сотрудников), ведение базы данных сотрудников, работа со списками их полномочий, обеспечение оператору возможности блокировать/разблокировать считыватели системы и предоставлять доступ (в том числе и от имени других сотрудников).

На сегодняшний день АРМ «Орион Про» позволяет строить глобальные распределенные комплексы СКУД. В одном комплексе может быть задействовано до 63 ПК, каждый из которых контролирует до 1024 приборов и отображает текущее состояние системы; до 15 ПК, занимающихся конфигурированием СКУД; до 63 ПК с различными модулями для создания отчетов (для контроля трудовой дис-

СКУД ИСО «Орион» – непрерывно развивающаяся система. В начале 2013 года завершилась работа по интеграции биометрических контроллеров «C2000-BIOAccess-F4» и «C2000-BIOAccess-F8» в АРМ «Орион Про». В ноябре началось серийное производство нового поколения контроллеров «C2000-2». На конец года запланировано очередное обновление АРМ «Орион Про» с поддержкой подсистемы распознавания автомобильных номеров «Орион Авто».



Биометрия

Биометрические контроллеры «С2000-BIOAccess-F4» и «С2000-BIOAccess-F8» представляют собой законченные решения для управления однонаправленной точкой доступа без контроля направления прохода. Доступ на вход предоставляется по факту идентификации отпечатка пальца, на выход – по кнопке. Приборы обеспечивают локальное хранение 2200 шаблонов для идентификации отпечатков. Коэффициенты эффективности распознавания FAR и FRR составляют около 1% и 0,001% соответственно. Контроллеры могут подключаться к АРМ «Орион Про» по локальной сети. Наличие в контроллерах клавиатуры и встроенного считывателя proximity карт позволяет обеспечить работу СКУД в режимах верификации по различным комбинациям параметров доступа (например, «карта+палец» или «код+палец»). АРМ «Орион Про» конфигурирует приборы, прописывая в их память новые отпечат-

ки пальцев; получает от приборов события для отчетов, в том числе по учету рабочего времени и запуска сценариев управления; предоставляет оператору возможность управлять приборами в реальном времени.

Новое оборудование, разработки

В 2014 году на смену контроллерам «С2000-BIOAccess-F4» и «С2000-BIOAccess-F8» придет новый прибор «С2000-BIOAccess-F18». Он сможет хранить в своей памяти 2500 шаблонов отпечатков пальцев, будет иметь меньшие размеры, современный дизайн и цветной ЖКИ-дисплей.

Новое поколение контроллеров доступа «С2000-2» 2.00 оснащено значительно большим объемом энергонезависимой памяти: 32768 кодов ключей и 32768 событий; 100 окон времени и 100 уровней доступа. Прибору добавлен новый вход/выход «Busy» для синхронизации работы нескольких контроллеров (для организации сложных точек доступа, например, парковочных пандусов для въезда/выезда) и подключения датчика присутствия человека в шлюзе. Добавлен режим работы «с подтверждением кнопкой». Контроллер может быть переведен в режим «открытого доступа» не только открывающим ключом или командой по информационному интерфейсу, но и по внешнему релейному сигналу. Реализован принципиально новый режим «открытого доступа» для электромеханических защелок.

Кроме того, сегодня мы занимаемся разработкой принципиально нового контроллера доступа «С2000-КД», который будет подключаться к АРМ «Орион Про» по локальной сети и иметь память на 50000 ключей и событий.

В состав очередного обновления АРМ «Орион Про» 1.12 войдет подсистема «Орион Авто», обеспечивающая автоматическое распознавание номеров и автоматическую верификацию въезжающих на территорию предприятия автомобилей. Номера автомобилей могут также быть идентификаторами для СКУД (шлагбаум будет открываться по факту распознавания известного номера). Кроме того, система сможет накапливать номера всех автомобилей, проезжающих через определенные контрольные точки, а также время и направление их проезда, формируя на основе этих

данных специальные отчеты. Этот функционал будет полезен для контроля бесплатных открытых паркингов торговых центров.

Перспективы

В заключение хотелось бы отметить, что наше предприятие уже более 20 лет занимается разработкой, производством и поставкой технических и программных средств для систем ОПС, СКУД, видеонаблюдения, управления противодымной защитой, оповещения, автоматического управления пожаротушением и управления инженерным оборудованием зданий. В составе ИСО «Орион» выпускается более 200 различных изделий, применение которых позволяет решить практически любую, стоящую перед проектным предприятием задачу по оснащению объектов системами безопасности и не только. Изделия системы «Орион» выпускаются на той же элементной базе, что и изделия зарубежных производителей. На нашем предприятии применяется самое современное технологическое оборудование, выпущенное ведущими мировыми компаниями в 2008-2013 годах. Процессы проверки изделий при их производстве полностью автоматизированы. На предприятии внедрена система менеджмента качества в соответствии с ГОСТ Р 9001-2008, подтвержденная независимыми аудиторами Госстандарта России и экспертами международной организации TUV, Германия.

Имеется большой опыт внедрения ИСО «Орион» на различных объектах России и стран СНГ в различных отраслях хозяйства: более 100 000 крупных промышленных комплексов и жилых зданий, в том числе высотных, а также 750 000 больших, средних и малых объектов оборудованы системами СКУД, ОПС, автоматики пожаротушения, дымоудаления и оповещения.



ОрионПроект, ЧСУП
 Авторизованный представитель
 компании ЗАО НВП «Болид»
 на территории Республики Беларусь
 220131, г. Минск,
 1-й Измайловский пер., д. 51, оф. 4
 Тел.: (017) 290-04-58, 290-04-59
 Сайт: www.orionproject.by
 E-mail: info@orionproject.by

РУНП: 191107028

Построение распределенной СКУД для офисов крупной компании



Парсиев Дмитрий, директор
«Видео-СКУД» ООО

В рекламных материалах часто можно встретить рекомендации по применению одного и того же оборудования и ПО СКУД для самого широкого перечня объектов: промышленных предприятий, банков и финансовых учреждений, учебных заведений, офисов крупных и средних компаний. Варьируются только количественные характеристики: количество точек доступа, количество сотрудников на объекте, количество рабочих мест управления СКУД. Основывается такой подход, очевидно, на кажущемся однообразии стандартных функций СКУД на объекте, среди которых базовые:

- контролируемый доступ сотрудников;
- контролируемый доступ посетителей;
- контролируемый доступ автотранспорта (служебного и сотрудников), с регистрацией и хранением времени и места всех событий в системе с целью создания различных отчетов.

Такой обобщенный подход не только не учитывает специфические задачи, стоящие при создании системы безопасности, но, в первую очередь, порочен тем, что не анализирует существующие угрозы для конкретного класса объектов, методику противодействия им, взаимодействие персонала службы безопасности и сотрудников компании.

Особенности построения распределенной СКУД

Часто крупные компании территориально представляют собой крупный центральный офис и сеть филиалов различной величины, расположенные в одном городе, в разных городах или

за рубежом. Особенностью взаимодействия центрального офиса и филиалов является наличие высокоскоростной компьютерной сети. Поэтому вопрос выбора среды передачи информации между отдельными сегментами и частями СКУД решается в пользу уже установленной на объекте компьютерной сети Ethernet. Соответственно, и оборудование, устанавливаемое в офисе СКУД, должно обеспечивать возможность работы в таких сетях, не являясь источником помех и дополнительной нагрузки. Важное значение имеет и наличие криптозащищенного протокола обмена между подключенными в сеть контроллерами и программным обеспечением.

Особое внимание следует уделить сохранности системной базы данных СКУД и защите хранящейся в ней информации. Для этого необходимо, чтобы в программное обеспечение СКУД были встроены специализированные сервисы обслуживания и резервирования. Программное обеспечение автоматизированных рабочих мест СКУД обычно не требовательно к ресурсам компьютерной техники.

Характерным требованием к СКУД, устанавливаемой в офисе крупной компании, является одновременное решение задач безопасности объекта и задач взаимодействия с системами управления персоналом компании.

С точки зрения обеспечения безопасности объекта основными задачами СКУД является защита служебной информации, защита материальных ценностей и личного имущества сотрудников в дневное время. Решается данная задача путем обеспечения контролируемого доступа в офис:

- выдача сотрудникам идентификационных (наиболее распространены бесконтактные карты доступа);
- разделение территории офиса по зонам с правом доступа в каждую из них только определенных групп сотрудников;
- установка временных ограничений на вход в те или иные зоны офиса различных групп сотрудников.

Но при реализации этих базовых функций накладываются особые условия, характерные для СКУД офисов крупных компаний. Наибольшие сложности могут здесь вызвать наличие большого потока посетителей. Некоторые пути решения:

- Для оперативного занесения данных о посетителе в СКУД должны быть предусмотрены функции автоматического распознавания информации с предъявляемых посетителями документов;

- В СКУД должны поддерживаться алгоритмы работы с устройствами автоматического изъятия выданных посетителю карт при выходе из офиса;

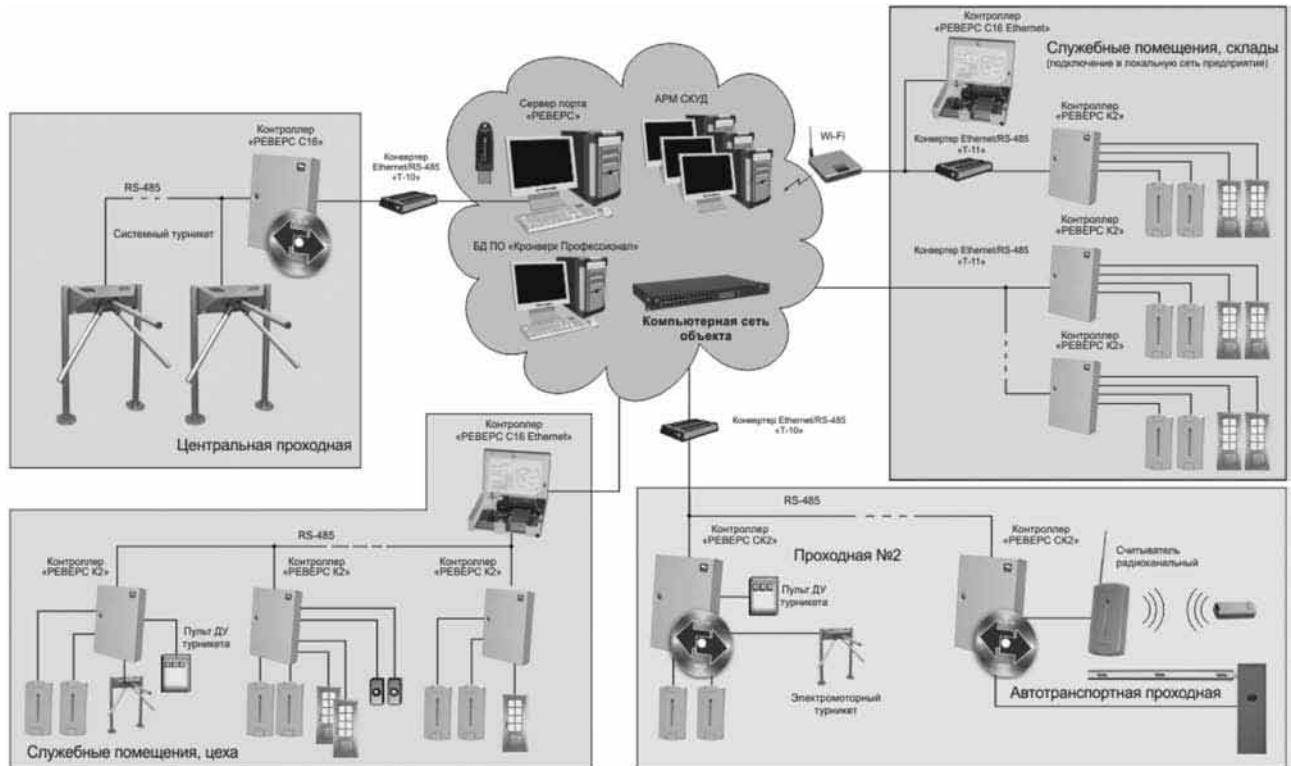
- Наличие в СКУД возможности автоматического изменения режима выбранных точек доступа по времени. Например, с наступлением времени, разрешенного для свободного доступа посетителей в офис, двери, ведущие в холл или в выбранные внутренние помещения офиса, автоматически переходят из режима «пропуска по картам» в открытый режим для доступа всех желающих. Переход обратно в системный режим производится так же автоматически, по заранее утвержденному расписанию.

Желательно, чтобы хозяин кабинета, оборудованного офисной СКУД, выходя из него и оставляя его пустым на время своего отсутствия, мог поменять режим прохода в кабинет таким образом, чтобы другие сотрудники (в обычное время проходящие в этот кабинет по картам) не могли бы пройти в данное помещение до его появления.

Для некоторых зон офиса крупной компании (серверная, помещения финансовых подразделений) могут потребоваться меры по дополнительному подтверждению прав доступа владельца пропуска. Оптимально в этом случае использовать сканеры биометрических признаков, например отпечатков пальцев. В этом случае необходимо, чтобы установленная в офисе СКУД имела возможность поддержки таких сканеров, а отпечатки пальцев сотрудников рассматривались СКУД так же, как и бесконтактные карты доступа.

Особенности выбора исполнительных устройств в составе распределенной СКУД

Для уличных входов наиболее часто применяются автоматические вращающиеся (карусельные, револьверные) двери, позволяющие обеспечить проход с улицы с минимальными потерями теплого или охлажденного воздуха в



холле (дверной проем у них всегда замкнут). Внутри здания применяются автоматические раздвижные двери (прямые и полукруглые), на их базе возможно построение шлюза. Автоматические двери должны иметь датчик безопасности в створе дверей и возможность ручной разблокировки.

В отличие от проходных промышленных предприятий и учебных заведений, где подавляющее большинство исполнительных устройств – турникеты-триподы, на проходных в офисах достаточно часто устанавливаются трехлопастные «роторные» турникеты со стеклянными створками и распашные калитки для экстренных выходов или прохода делегаций, так же оборудованные стеклянными створками или створками со стеклянным заполнением. В качестве замков для обычных дверей наиболее часто применяются врезные электромеханические замки или защелки (ЭМЗ) ведущих зарубежных производителей. Для каждой из конструкций дверей (специальных огнезащитных, стеклянных, раздвижных, маятниковых и др.) разработаны различные модели ЭМЗ.

В отличие от промышленных предприятий, где часто требуется специализированная система учета автотранспортного грузопотока предприятия, для крупных офисов система пропуска автотранспорта часто является вспомогательной и служит только для парковки легкового служебного и личного автотранспорта. Оптимальными идентификаторами в данном случае являются радиоканальные брелоки, позволяющие разблокировать исполнительные

устройства (шлагбаумы, ворота, парковочные столбики) не выходя из машины с расстояния 7-10 м. Некоторые производители выпускают двухканальные брелоки, которыми можно дистанционно открыть шлагбаум, а внутри офиса использовать как обычные карты доступа. Сверхвысокая скорость работы исполнительных устройств обычно не требуется, более серьезное внимание следует уделять установке дополнительных элементов обеспечения безопасности проезда.

Интеграция дополнительных функций, приложений

Часто необходимо взаимодействие между ПО СКУД и кадровыми программами – желательно иметь возможность получить список сотрудников из этих программ в СКУД. Важно и обратное взаимодействие, когда информация о проходах сотрудника передается в программы начисления и расчета заработной платы, например «1С:Предприятие. Зарплата и управление персоналом».

Полноценная реализация взаимодействия между СКУД и широким спектром программных бизнес-приложений оптимально при использовании ТСР-серверов с открытым протоколом. Применяя эти инструменты, разработчики внешних бизнес-приложений получают возможность использовать в своих целях любые компоненты СКУД, не нарушая целостности решения, и не будучи связанными особенностями оборудования конкретной СКУД.

Многие функции СКУД можно с успехом применить для организации

внутриофисной деятельности. Имеющееся зональное разбиение возможно использовать для поиска конкретного человека на объекте. О появлении в офисе определенных сотрудников можно информировать путем передачи SMS сообщения на нужные телефоны, а используя механизм реакции СКУД на системное событие, можно включать то или иное оборудование, например, кофеварку или кондиционер в конкретном помещении. Имеющиеся на руках сотрудников бесконтактные карты можно использовать как инструмент учета в столовых, зонах релаксации и торговых автоматах.

Систему безопасности для офисов крупных компаний невозможно рассматривать без учета взаимодействия всех ее подсистем: охранного телевидения, охранной и пожарной сигнализации, СКУД и других. Различные компоненты дополняют друг друга, повышая общую надежность за счет частичного дублирования функций, защищают саму систему от постороннего вмешательства. Это может выглядеть так: появление тревожного события (например, сообщение о пожаре) фиксируется внутри-объектовой радиосистемой пожарной сигнализации, взаимодействуя с которой СКУД открывает исполнительные механизмы (двери, калитки) на путях эвакуации, обеспечивая беспрепятственный выход людей из конкретной зоны, а система охранного телевидения передаст команду на переключение камер видеонаблюдения на зону эвакуации, с целью обеспечения реакции оператора на возможные изменения ситуации.

«WEB-офис» – новое поколение IP-СКУД

Производитель ООО «СКД-С» (РФ)

«WEB-офис» – это полнофункциональное решение СКУД для средних и малых объектов, позволяющее организовать:

- проход и проезд на территорию и в помещения по предъявлению идентификаторов;
- учет рабочего времени сотрудников;
- удаленный контроль за нахождением сотрудников на объекте;
- проход посетителей (с ограничением времени действия пропуска – с точностью до 1 часа, с автоматическим запретом пропуска при выходе);
- работу с различными идентификаторами (бесконтактные карты, PIN-код, штрих-код) в одной системе.

Простота установки и использования

Подключается в компьютерную сеть или в сеть INTERNET. Программное обеспечение СКУД «WEB-офис» встроено в контроллер «РЕВЕРС С16 WEB». Имеет простой, интуитивно понятный web-интерфейс для занесения пользователей в систему, дистанционного получения отчетов и управления оборудованием.

Масштабируемость

СКУД «WEB-офис» поддерживает управление доступом через 16 турникетов или дверей, оборудованных электромеханическими или электромагнитными замками (вход/выход по идентификатору). Опыт показывает, что этого количества

вполне достаточно для средних предприятий и различных офисов. Подключение исполнительных устройств и считывателей идентификаторов осуществляется через дополнительные контроллеры «РЕВЕРС М1» и «РЕВЕРС К2».

Хранение списка пользователей в контроллерах «РЕВЕРС М1» и «РЕВЕРС К2» (до 8000 идентификаторов в каждом контроллере) позволяет обеспечить полную работоспособность точки доступа в случае обрыва линии связи с контроллером «РЕВЕРС С16 WEB».

Возможности ПО «WEB-офис»:

- создание необходимого количества АРМ мониторинга и управления СКУД по сетям INTERNET;
- дистанционное управление исполнительными устройствами СКУД по сетям INTERNET;
- удаленное составление и просмотр оперативных отчетов по текущему местоположению сотрудников внутри офиса;
- ведение учета рабочего времени и нарушений трудовой дисциплины (опоздания, ранний уход) персоналом;
- подключение камеры D-LINK и кнопки вызова для входных дверей (пропуск посетителей).

Эффективное применение

Гибкость настроек контроллера «РЕВЕРС С16 WEB» и простота модификации его программного обеспечения WEB-офис обуславливает

широкое прикладное использование на объектах различного назначения:

ПАРКИНГ

Программное управление проездом автотранспорта через INTERNET. Оптимально для парковок крупных жилых комплексов. Для идентификации автомобилей могут использоваться:

- Радиоканальные считыватели (дальность 10-15 м);
- Считыватели бесконтактных карт доступа (дальность 0,1-0,5 м);
- Оптические (лазерные) сканеры штрих кода (оптимально для разовых посетителей, формирование и печать штрих-кода возможно осуществлять с помощью ПО «WEB-паркинг»).

СЕТЬ БЮДЖЕТНЫХ МИНИ-ОТЕЛЕЙ

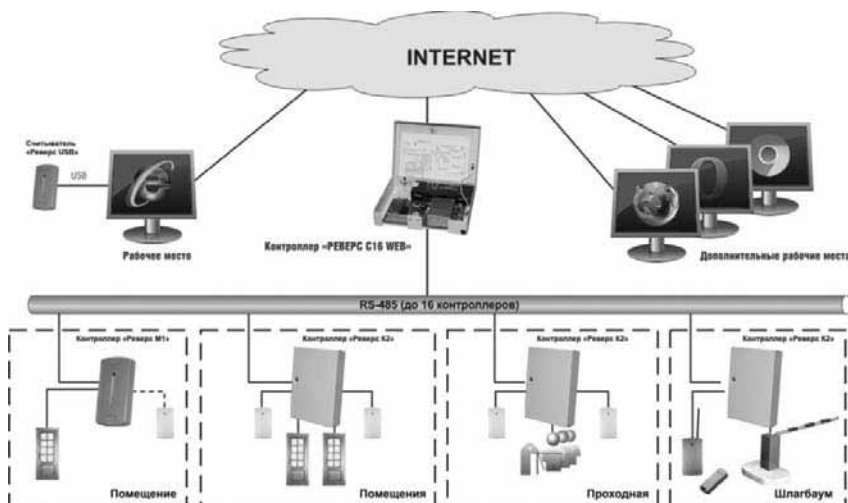
Самостоятельное заселение и выезд гостей минимизирует затраты на обслуживающий персонал. Проход по PIN-коду, высланному на указанный при бронировании e-mail или SMS. Можно задать срок действия PIN-кода (с 14.00 указанной даты начала бронирования до 12.00 даты окончания бронирования).

ЦЕНТР МЕДИЦИНСКИХ УСЛУГ

Разрешение доступа посетителям и клиентам только после оформления в регистратуре. Однократный проход клиентов и посетителей по штрих-коду, напечатанному на бланке талона-направления к специалисту. Автоматическое удаление разовых посетителей из списка при выходе их с территории центра. Проход на территорию и во внутренние помещения центра медперсоналом осуществляется по бесконтактным картам.

WEB-ШКОЛА

Контроль посещаемости учащихся родителями и надзорными органами через INTERNET. Возможность интеграции данных в электронные дневники.



«Видео-СКУД», ООО

Республика Беларусь, 220125,
г. Минск, ул. Уручская, дом 23А, офис 1
Тел./факс: +375 (17) 265-67-63;
+375 (29) 686-87-63.
www.videoskud.by
info@videoskud.by

УНП: 191216787



Развитие САП 777 «КомплексПаркинг»



Петлицкий Александр,
заместитель
директора по технике
ООО «РОВАЛЭНТКОМПЛЕКС».

В стране происходит дальнейшая модернизация городской инфраструктуры. Продолжается организация автоматизированных парковок, которая является актуальной задачей, как для городских служб, так и для владельцев корпоративной недвижимости при возведении паркингов.

Из государственных программ следует отметить утвержденную Мингорисполкомом программу «400 тысяч» по организации мест для парковок ма-

шин со сроком реализации до 2020 г. Программа проходит по двум направлениям. Первое направление – создание парковочных мест при проездах, дорогах, улицах и на дворовых территориях. Второе направление – поиск территорий, которые не будут востребованы, и размещение там недорогих временных парковок. К примеру, это территории будущих магистралей. Ставится задача ежегодно строить по 20 таких охраняемых площадок.

Соответственно сегмент рынка систем автоматизированных парковок (САП) продолжает рост. САП 777 «КомплексПаркинг» – первая, известная нам отечественная разработка, выполненная компанией «РОВАЛЭНТКОМПЛЕКС».

Одна из первых значимых инсталляций САП 777 «КомплексПаркинг» – проект по созданию автоматизированной парковки для национального аэропорта «Минск-2», реализация проекта началась в 2011 году. О развитии проекта, результатах внедрения системы, расширении её функционала и новых возможностях мы говорили с заместителем директора по технике компании «РОВАЛЭНТ-

КОМПЛЕКС» – Петлицким Александром.

Каковы результаты Вашей работы над САП 777 «КомплексПаркинг» за период первых инсталляций (с 2012 года) до сегодняшних дней?

На сегодняшний день мы видим, что по функционалу аналогичных систем нет не только в Беларуси, но и в России. Есть отдельные решения, но объединенных в одном комплексе мы не видим. Уникальность нашей разработки – на одной платформе максимально реализован и расширен функционал парковки.

Наша платформа состоит из четырех основных подсистем:

- паркинг (платежная система);
- платежная система (платежные терминалы с выдачей сдачи, без выдачи, с безналичными платежами) (Рис.1);
- светодиодные табло любых конфигураций с полноцветным разрешением (Рис. 2);
- навигация по парковке (объединение светодиодных табло с ультразвуковыми датчиками, определяющими наличие авто в зоне парковки).



Рис.1. Платежный терминал



Рис. 2. Светодиодное табло

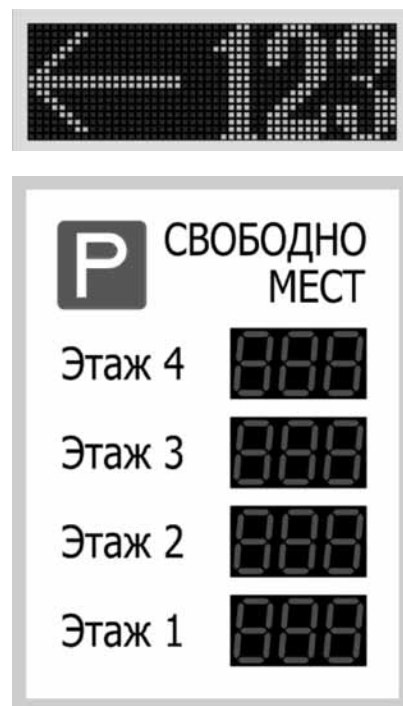


Рис.3. Навигация по парковке

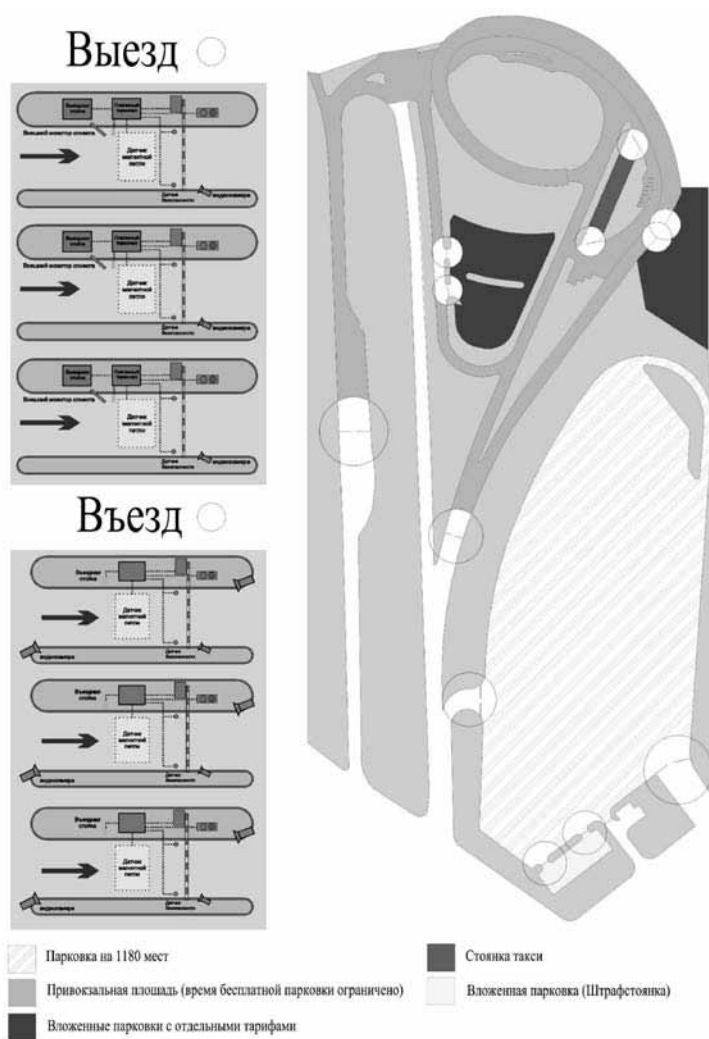


Рис. 4. Схема САП 777 «КомплексПаркинг», аэропорт «Минск – 2»

Здесь главную роль играет разработанное программное обеспечение, которое позволяет осуществлять полноценную навигацию: показывает наличие мест, определяет направления движения посетителей, исключает заторы и пробки и пр.). Данное оборудование мы планируем применить при запуске 2-й очереди САП аэропорта (Рис.4).

Какие актуальные доработки в САП 777 «КомплексПаркинг» можете отметить?

1. Работы по навигации. Тема актуальная. Спрос на данное оборудование оказался очень высоким. Системы навигации позволяют улучшить пропускную способность внутри паркинга, увеличить оборачиваемость машиномест, уменьшить время поиска свободного места, уменьшить загрязнение воздуха внутри паркинга, улучшить безопасность внутри паркинга, сократить время поиска автомобиля. Мы начали собственное производство ультразвуковых датчиков (Рис. 5),

определяющих наличие автомобиля в зоне парковки. К ним «привязывается» табло, где указано количество свободных мест на парковке. Наши датчики имеют возможность интеграции, могут внедряться в другие системы.

Компанией «РОВАЛЭНТКОМПЛЕКС» разработаны различные методы нави-

гации, которые позволяют найти свободное место при въезде на парковку и быстро найти автомобиль владельцу. Поиск можно осуществить различными путями: в первую очередь, помогает элемент (идентификатор), с помощью которого человек въехал на парковку. Это может быть талон со штрих-кодом, магнитная карточка или можно воспользоваться терминалом с сенсорным дисплеем. Приложив идентификатор к терминалу, на дисплее отразится кратчайший путь до места парковки. Возможность навигации заложена в платежные терминалы. Кроме того, по паркингу могут быть расставлены отдельные навигационные терминалы.

При потере талона со штрих-кодом (идентификатора), предусмотрена возможность найти свой авто по другим признакам. Вводится приблизительное время въезда, система анализирует занятые места в период времени, время подъезда и выдаёт возможные места парковки. Все это делает ПО на основании информации с устройств (ультразвуковых датчиков, магнитных петель, камер и т.д.) и введенных данных (время въезда, номер машины и т.д.). Навигация и поиск упрощаются, если парковка оборудована системой распознавания номеров.

2. Разработана возможность автономной работы САП 777 «КомплексПаркинг». В случае отключения от сервера, въезд и выезд между собой не синхронизированы, они работают автономно. В штрих-коде хранится вся информация о въезде: номер машины, время и дата въезда и др. И с выезда нам не нужно делать запрос на сервер, вся информация о въезде закодирована в штрих-коде билета.

3. Работы по исключению злоупотребления персоналом парковок. Совместно с сотрудниками аэропорта



Рис. 5. Ультразвуковые датчики

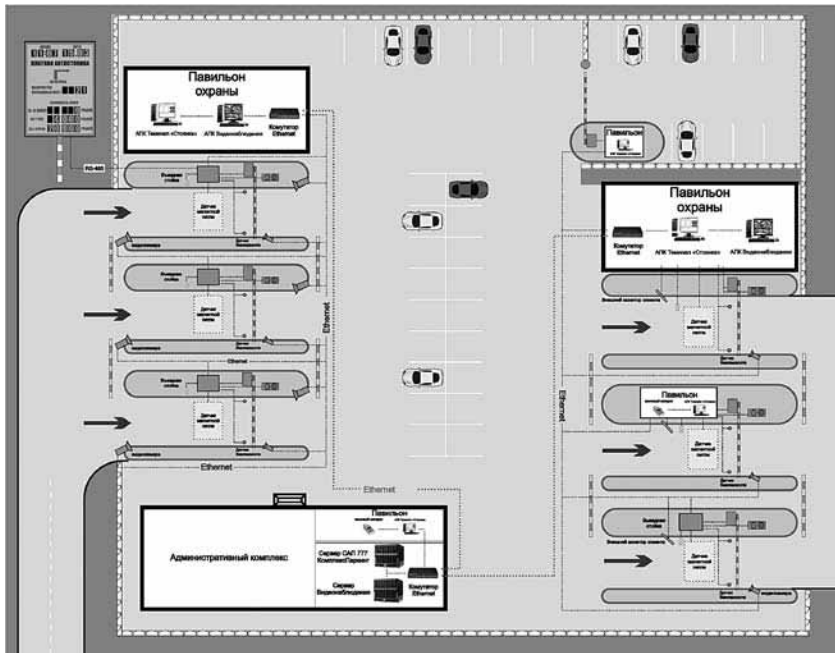


Рис. 6. Принципиальная схема САП 777 «Комплекс Паркинг»

была проведена большая работа в этом сегменте. Добавлено около сотни мелких контролирующих функций и изменений в ПО САП 777 «КомплексПаркинг». Результат этой работы – теперь персонал, ни в каком случае не сможет вмешаться в работу системы. Например, были исключены возможности: т.н. «паровоза» из авто при въезде, неправомерного пропуска персоналом авто (исключено участие персонала в подъеме шлагбаума ручным способом), исключена регулировка времени и пр.

Насколько сокращается обслуживающий персонал при использовании Ваших решений?

При максимальном использовании системы необходим только обслуживающий персонал, в среднем, двух человек достаточно.

Существуют ли нюансы технического обслуживания системы?

Если рассмотреть на примере аэропорта «Минск-2», нюансов по техническому обслуживанию никаких не было. Гарантийных и негарантийных замен не было. На практике, все зависит от загрузки паркинга конечно, но в целом, обслуживания почти никакого не требуется, тем более специального. Например, кассовая лента при огромном потоке на объекте парковки в аэропорту «Минск-2» меняется примерно раз в месяц, т.к. предусмотрена её увеличенная зарядка.

Какие системы распознавания номеров используются?

САП 777 «КомплексПаркинг» сделана на платформе «Интеллект», в которую внедрен модуль распознавания номеров «Ураган».

Какие нестандартные решения используете в САП 777 «КомплексПаркинг»?

К нестандартным решениям можно отнести использование платежных терминалов без выдачи сдачи, сдача с суммы положенной на терминал зачисляется на телефон. Это удешевляет стоимость платежных терминалов. Мы наладили производство платежных терминалов с функцией осуществления платежей с использованием банковской карты.

Также в терминалах будет заложена функция вызова такси. Это отдельная работа, будет создана база данных такси, предусмотрена отдельная стоянка, разработана отдельная технология по работе с такси. На платежном терминале будет изображена карта Беларуси, где клиент может выбрать нужный регион и произвести оплату банковской картой с платежного терминала.

Какие виды идентификаторов могут использоваться в САП 777 «КомплексПаркинг»?

Для посетителей могут использоваться билеты со штрих-кодом, proximity-карты, билеты с магнитной полосой, номера автомобилей, распознанные системой Ураган, Smart карты (используются в основном для России). Для служебного персонала используются proximity-карты. Мы

можем интегрировать любую систему и вид идентификации.

В системе используются возможности интеграции с ИСО «777»?

Ядро системы, функционал – это и есть сервер ИСО «777». Все исполнительное оборудование САП 777 «КомплексПаркинг» работает через сервер ИСО «777» по протоколу Ethernet.

Как используются системы видеонаблюдения в САП 777 «КомплексПаркинг»?

Камеры используются на въезде/выезде (для фиксации состояния авто), для фиксации лица водителя и государственных номеров (с последующей работой с б/д номеров).

Вами получен большой опыт при построении системы автоматизированной парковки. Какие рекомендации можете дать? Какие нюансы и вопросы следует учитывать при построении и организации автоматизированных парковок?

Максимально автоматизировать паркинг во избежание «человеческого фактора».

Не следует экономить на количестве датчиков въезда (оптические, магнитная петля). Посредством их осуществляется въезд/выезд, именно они помогают избежать очередей, т.н. паровозов и пр.

Внимательно подбирать и не экономить на покрытии. Что существенно упростит эксплуатацию паркинга в зимний период.

Использовать платежные терминалы. Например, в России практически не осталось ручного обслуживания. Это существенно упрощает и эксплуатацию и администрирование, а также минимизирует злоупотребление со стороны персонала.

На каком объеме паркинга/автостоянки целесообразно устанавливать САП 777 «КомплексПаркинг»?

На паркингах с объемом от 50 мест она будет выгодна. Под этот проект мы сделали сайт <http://autoparking.by>, где можно подобрать весь функционал.

РОВАЛЭНТКОМПЛЕКС, ООО
223056, Минский район,
пос. Юбилейный, ул. Луговая, 11
Тел./факс: (017) 510-23-26, 510-23-27
(сбыт), 506-21-52, (029) 777-75-90,
350-1-777
E-mail: support@rovalant.by, support@rovalantcomplex.com
Сайт: www.rovalantcomplex.com,
www.rovalant.by,
www.autoparking.by

РУНП: 190832170

СКУД без проводов: идеи, реализации, перспективы

Задачей данного обзора является знакомство специалистов с новой, перспективной топологией организации полноценных беспроводных СКУД, базирующихся на протоколе беспроводной передачи данных IEEE 802.15.4, более известной как «технология ZigBee». Конечно, правильнее было бы назвать эту статью «введением», а не обзором, как из-за новизны предлагаемой концепции построения беспроводных СКУД, так и из-за ограниченности реального предложения рассматриваемых систем на рынке.

В последние несколько лет беспроводные технологии активно внедряются во многих системах безопасности. В частности, они весьма успешно используются в системах охранной и пожарной сигнализации. Беспроводные (зачастую – даже с питанием от обычных батарей) датчики, извещатели, сирены и другое оборудование, работающее по радиоканалу, предлагает большое число производителей, в том числе и российских. Причины такого успеха лежат на поверхности. Вместе с отказом от проводов эти системы приобретают ощутимые преимущества, как для конечных пользователей (повышается безопасность и надежность систем, не зависящих от перебитых или перегоревших проводов), так и для инсталляторов (так как установка систем не только значительно упрощается, но и увеличиваются возможности по расширению и наращиванию систем на функционирующих объектах).

Однако в такой сфере обеспечения безопасности, как СКУД, ситуация на данный момент совсем другая. О беспроводных СКУД много говорят как в среде инсталляторов, так и разработчиков – но реально предлагает такие системы считанное число западных производителей. Да и внедрять такие системы у нас пока готовы далеко не все – на данный момент в Беларуси установлено буквально несколько систем.

Попробуем разобраться в ситуации, а также убедить специалистов, что беспроводные СКУД – не миф и теоретические изыскания «на тему», а реальная альтернатива «классическим» проводным системам.

Для начала разберемся с самой идеей «беспроводности», т.е. определим:

- а) о каких системах мы говорим;
- б) от каких именно проводов необходимо избавиться.

Итак:

а) Мы рассматриваем не автономные СКУД на 1-2 двери и сотню другую пользователей, а универсальные системы на большое количество пользователей и точек доступа (как минимум – несколько тысяч), с управлением и контролем в реальном времени, с достаточным числом уровней и временных расписаний доступа (256 и более) и т.д.

б) В идеале «беспроводная СКУД» должна быть таковой в абсолютном выражении – т.е. без проводов вообще.

Существующие сегодня (и предлагаемые на нашем рынке) классические СКУД используют провода весьма широко, причем с абсолютно разными целями. Разделим все эти провода на три категории. Во-первых, магистральные каналы связи (чаще всего используются стандарты передачи данных по протоколам RS485 или IP). В эту же категорию «оптом» запишем еще и всевозможные конвертеры и преобразователи интерфейсов (это хоть и не провода в чистом виде, но «довесок», от которого тоже не лишним будет избавиться). Во-вторых, провода для «обвязки» двери, т.е. шлейфы, соединяющие контроллер доступа со считывателями, исполнительными механизмами, датчиками, кнопками выхода и т.д. В-третьих, питающие линии как для контроллеров, так и периферии – считывателей, исполнительных устройств.

Такое «классификационное» деление проводов сделано намеренно – поскольку перевод каждого из трех типов в беспроводное состояние решается по-разному.

Магистраль. По этим каналам осуществляется связь контроллеров доступа с базой данных СКУД (центральным сервером БД). Как правило, эти каналы передачи данных занимают львиную долю общего километража кабелей, и перевести их в беспроводной радиоканал проще всего (теоретически). Технологий для этого уже сейчас существует достаточно много: Wi-Fi, WiMAX, GSM, Bluetooth, ZigBee и др. Если в системе используются IP-контроллеры, то и выдумывать-то ничего не надо – достаточно просто поставить 2 точки доступа Wi-Fi «на концах провода». На самом деле, здесь не все так просто, но сначала рассмотрим следующие пункты.

«Обвязка» точки доступа. Термин достаточно условный, но все специалисты его прекрасно понимают. Несмотря на небольшой метраж таких кабелей в расчете на систему, именно возможность (точнее – невозможность) их прокладки на конкретном объекте в большинстве случаев ограничивает количество помещений, оборудуемых СКУД. А при развертывании СКУД на уже функционирующем объекте, именно прокладка этого «последнего метра кабеля» становится основной головной болью инсталляторов. Еще одна проблема – разнообразие типов протоколов, которые используются в «обвязке». В отличие от магистралей, где таких протоколов не наберется и пяти штук, здесь мы имеем полное разнообразие. Теоретически, все они также могут быть переведены на беспроводной радиоканал. Стоимость всевозможных конвертеров абсолютно точно уничтожит весь смысл перевода системы в «беспроводное» состояние.

Питающие линии. Здесь также одна сплошная проблема... Технологий передачи питающего напряжения достаточной мощности без проводов практически нет (как минимум, нет промышленных образцов, пока только прототипы). Единственная альтернатива – использование батарей или аккумуляторов. Однако можно предста-

вить размер (и стоимость) комплекта батарей, достаточного для работы, так любимого нашими installторами, магнитного замка сроком хотя бы на год-два без перезарядки или замены (более частая смена батарей уничтожит перспективу применения такой системы для большинства пользователей из-за эксплуатационных расходов).

На первый взгляд – полный тупик... Да, у нас все еще остается реальная альтернатива переводу магистралей в беспроводное состояние, а кабели по 2-му и 3-му пунктам можно оставить как есть. Многие наши разработчики других вариантов даже и не рассматривали. Но это будет уж никак не «беспроводная СКУД».

Тем не менее, все перечисленные проблемы имеют решение, причем известно оно достаточно давно. Чтобы избавиться от проводов нужно или применять сразу несколько беспроводных конвертеров (что, как было указано выше, сводит к нулю саму идею), или ... обнулить их длину. Т.е. комплект оборудования, куда входит контроллер, считыватель, датчик положения (если нужен), исполнительное устройство (замок) и т.д. должен превратиться в единое устройство – электронный замок. Провода «извне» к нему не подводятся, несколько сантиметров провода внутри самой конструкции замка мы учитывать не будем. Даже источником питания электронных замков служит не блок питания от сети 220 В, а обычные батарейки: от одного комплекта (как правило, от 1 до 6 стандартных батареек, которые всегда можно купить в любом магазине) электронные замки работают 2-4 года.

Такие характеристики достигаются благодаря «хитрому» исполнительному механизму электронного замка: двигатель (иногда – соленоид) в таких замках осуществляет только блокировку/разблокировку запирающего механизма, а дверь открывает сам пользователь, нажимая на ручку замка. Благодаря такой схеме в электронных замках применяются микродвигатели с экстремально низким потреблением энергии.

Подобные системы (системы электронных замков) изобретены более 20 лет назад, но они обладали рядом особенностей, достаточно серьезно ограничивающих область их применения:

1. До последнего времени, в таких системах магистральные каналы связи не использовались вообще. Электронные замки не имели связи с сервером системы в режиме реального времени. Время от времени оператор си-

стемы мог обеспечить связь замков с сервером благодаря переносу (в буквальном смысле) информации от БД к замку и обратно через специальный прибор – портативный программатор. То есть, для сбора протокола проходов через точку доступа или, наоборот, для внесения изменений в параметры точки доступа, он должен был подойти к замку с программатором, подключить его к замку для загрузки данных, и затем вернуться к компьютеру. Управление же точкой доступа (электронным замком) в режиме реального времени (открытие или блокировка двери с рабочего места оператора системы) вообще не предусматривалась.

2. Для удобства управления правами доступа пользователей при отсутствии магистрали (точнее, для возможности назначения прав новым пользователям после того, как замки были запрограммированы), эти права в системах электронных замков записываются непосредственно на карту пользователя. Т.е. карта ВСЕГДА выступает не в роли *идентификатора* доступа, а в роли носителя прав доступа. Отсюда – следующая особенность.

3. Для управления пользователями, т.е. для изменения или отмены прав доступа, оператор должен получить физический доступ к карте (напомним, именно она является носителем информации о доступе) или к замку (чтобы внести в его память черный список с перечнем утерянных карт). Чтобы изменить права доступа карту надо переписать. Чтобы отменить утерянный ключ надо обойти все замки, где эта карта была действительна.

Назвать такую систему полноценной СКУД нельзя. До последнего времени они применялись в основном в отелях, где при большом количестве точек доступа (электронных замков) отсутствие необходимости в прокладке проводов с лихвой окупает все описанные недостатки. Однако – времена меняются...

Идея создания беспроводной универсальной СКУД

Для эволюционного перехода от электронного замка к универсальной СКУД необходимо обеспечить связь между замками и сервером СКУД в режиме реального времени. Конечно, организовать такую связь можно и классическим методом, т.е. проложить кабели. Однако, в таком случае мы теряем главное преимущество – простоту монтажа и возможность развертывания системы «на живую», в уже функционирующем офисе, например. Да и цена такой систе-

мы будет достаточно высока. В классических СКУД можно (и нужно) использовать один контроллер на несколько дверей (4, 8, 16...), а поскольку контроллер является наиболее дорогостоящим элементом системы, цена «в расчете на одну дверь» будет не столь высока. С электронным замком, у которого контроллер «вживлен» внутрь, всегда выполняется равенство «один контроллер = одна дверь».

Однако если к возможностям электронных замков добавить беспроводной радиомодуль, расклад сил может кардинальным образом измениться. Ведь в этом случае, в дополнение ко всем имеющимся преимуществам, мы получаем действительно беспроводную, но отвечающую всем требованиям, универсальную СКУД.

Выбор технологии

Выбор технологии для организации беспроводного магистрального канала между электронными замками и сервером СКУД – весьма принципиальная задача. Упомянутые ранее технологии Wi-Fi или Bluetooth, равно как и GSM-сети, для этих целей на самом деле не годятся. Как по причине высокого энергопотребления, так и из-за особенностей организации топологии сети. Любая из указанных технологий съедала бы весь заряд комплекта батарей автономного замка за несколько дней (в лучшем случае), а необходимость подвода внешнего питания (установка блоков питания и прокладка кабеля к замку) уничтожает сам смысл термина «беспроводная СКУД».

Поэтому в качестве транспорта был выбран протокол IEEE 802.15.4. – он представляет прекрасные возможности как по организации достаточно разветвленных многоуровневых сетей (со смешанной топологией «точка-точка», «звезда»), так и по параметрам энергопотребления передающих устройств.

Исходя из краткого описания истории возникновения и технических характеристик этого протокола, останемся на нескольких нюансах, имеющих непосредственное отношение к тематике СКУД. Основным преимуществом этого стандарта как магистрального транспорта для беспроводных СКУД, основанных на применении электронных замков, является экстремально низкое потребление энергии самим радиомодулем.

На заявленную же скорость передачи до 250 кбит/с и расстояния уверенного приема сигнала до 100 м при этом рассчитывать не стоит. Во-

Справочно:

Разработчиком стандарта IEEE 802.15.4 выступил альянс компаний: *Invensys, Honeywell, Mitsubishi Electric, Motorola, Philips* и др. Этот стандарт описывает беспроводные персональные вычислительные сети (WPAN – Wireless Personal Area Network). Стандарт IEEE 802.15.4 был принят достаточно давно (формирование спецификации IEEE 802.15.4 началось в конце 90-х гг. прошлого века, действующая сейчас спецификация протокола датирована 2006-м годом). ZigBee – название набора протоколов высокого сетевого уровня, использующих радиопередатчики, основанные на стандарте IEEE 802.15.4. Название ZigBee появилось как комбинация от "Zig-zag" – зиг-заг и "Bee" – пчела, поскольку топология сети предполагает возможность передачи информации по траектории, подобной зигзагообразному полету пчелы от цветка к цветку. ZigBee нацелена на приложения, которым требуется большее время автономной работы от батарей и большая безопасность при меньших скоростях передачи данных. Основная особенность технологии ZigBee заключается в том, что она при относительно невысоком энергопотреблении поддерживает не только простые топологии беспроводной связи («точка-точка» и «звезда»), но и сложные беспроводные сети с ячеистой топологией с ретрансляцией и маршрутизацией сообщений.

Стандарт IEEE 802.15.4 предусматривает работу в трех диапазонах, наиболее быстрый и емкий из которых – 16 каналов в диапазоне 2450 МГц (шаг центральных частот – 5 МГц, самая нижняя из них – 2405 МГц) – как раз попадает в спектр нелегализуемых частот. Скорость в этом канале – 250 кбит/с. Дальность передачи – от 10 до 100 м, в зависимости от отдаваемой мощности и окружающей среды.

первых, эти параметры сильно зависят от конкретной реализации модуля и от состояния окружающей среды (толщина и тип стен, перекрытий и т.п.). Во-вторых, в заявленных 250 кбит/с достаточно хорошую часть «съедает» служебная информация самого протокола, обеспечивающая работоспособность устройств при достаточно больших допустимых потерях пакетов.



Еще один нюанс – «плата за использование» частотного диапазона 2,4 ГГц, в котором уже живут несколько других технологий (тот же Wi-Fi и Bluetooth). Из-за такого «соседства» в реальности вряд ли удастся беспрепятственно использовать все 16 представленных протоколом каналов.

Возможно, именно эти проблемы пока мешают использованию протокола IEEE 802.15.4 в «классических» СКУД, т.к. зависимость их работоспособности от качества магистральной достаточно высока.

Однако с системами, построенными на электронных замках, ситуация принципиально другая. Во-первых, эти системы изначально создавались

для использования в условиях, когда никакой магистрали нет вовсе, поэтому и в беспроводном варианте они отлично выполняют весь базовый набор функций, даже при полностью «упавшей» сети. Во-вторых, сам принцип системы доступа здесь отличается от «классики» кардинально. Главное отличие – использование электронных «носителей информации о доступе» вместо «идентификаторов доступа». Права доступа **записываются** на саму карту в момент выдачи ключа пользователю, а не сохраняются «в недрах» БД СКУД и/или памяти контроллера, ассоциированные с неким «идентификатором», выданным на руки пользователю. То есть, контроллеры электронных замков не должны хранить в своей памяти таблицу доступа со списком всех карт, которые надо «пускать», а только собственные параметры плюс реальное время-дату. При предъявлении ключа происходит сравнение информации, считанной из памяти карты, с информацией из памяти контроллера (попадает ли данный контроллер в список зон, разрешенных на карте, с учетом реального времени-даты, текущего режима работы контроллера и т.п.). И решение «открывать/не открывать» контроллер принимает самостоятельно, без участия сервера системы.

Наличие беспроводной связи электронного замка с сервером не является обязательным условием функционирования системы, оно лишь снимает те ограничения, которые не позволяли ранее называть такие системы полноценной СКУД. Вместе с тем, все эти «дополнительные» функции не столь чувствительны ни к скорости прохождения сигнала от сервера к замку и обратно (конечно, речь не идет о минутах или даже о десятках секунд, но задержка в 1-2 секунды вполне возможна), ни к возможным

пропаданиям связи и их длительности.

К этим возможностям относятся:

1. Мониторинг состояния системы и управление точками доступа в реальном времени;

2. Сбор аудита системы (кстати, электронные замки имеют свою собственную энергонезависимую память, куда все события обязательно записываются, даже если беспроводная связь работает без сбоев);

3. Управление пользователями, т.е. возможность отмены, изменения прав доступа и отслеживания пользователя в реальном времени;

4. Некоторые другие возможности, характерные для особых условий применения. Например, в гостиничных системах стало возможным удаленное продление срока проживания или переселение из одного номера в другой без посещения гостем стойки размещения.

Несколько слов скажем о топологии беспроводной сети, построенной на основе протокола IEEE 802.15.4. Выше упоминалось, что радиомодули, работающие по этому стандарту, имеют ограничения по дальности «видимости». В реальных условиях это расстояние не более 20-40 м (мы, конечно, подразумеваем развертывание системы в помещении). Для организации нормальной СКУД в большинстве случаев этих расстояний недостаточно. Поэтому сетевая инфраструктура состоит не только из приемника и передатчика, но и промежуточных повторителей-ретрансляторов сигнала, а также шлюзов, соединяющих беспроводные сети с сегментом локальной сети. Например, путь прохождения сигнала может выглядеть как «точка доступа – повторитель – повторитель – ... – шлюз – локальная сеть – сервер». Количество повторителей между точкой доступа и шлюзом (это обязательные элементы инфраструктуры) зависит как от «географии» объекта, так и от конкретной реализации системы. Например, в системах SALTO Wireless, которые мы будем рассматривать далее, максимальное количество повторителей между замком и шлюзом – 4. Но при этом инфраструктура сети не обязательно должна быть линейной. Каждый шлюз (он, кстати, тоже совсем не обязательно должен быть только один на всю систему) может одновременно работать с 4-мя повторителями и 16-ю замками, каждый повторитель – еще с 4-мя другими повторителями и так же 16-ю замками. В итоге мы получаем «древовидную» топологию сети со множеством ответвлений.

Эффективная информационная площадка для профессионалов индустрии безопасности

выставка-форум
**Инженерно-техническая
безопасность**
4-5 июня, 2014

Центр
безопасности



**Профессиональная аудитория
Новейшие технологии
Проблемно-ориентированные доклады**

Тематические разделы:

- технические средства и системы охраны;
- пожарная сигнализация и автоматика;
- системы оповещения и связи;
- системы охранного телевидения и наблюдения;
- системы контроля и управления доступом;
- антитеррористическое и досмотровое оборудование;
- комплексные системы безопасности;
- инженерно-технические средства защиты;
- банковское оборудование.

cb.aercom.by

Организатор:

Программная поддержка:

Технический партнер



ТЕХНОЛОГИИ БЕЗОПАСНОСТИ Журнал
для руководителей предприятий и специалистов отрасли безопасности



www.axiom.by



Не требует доказательств



ПРОФЕССИОНАЛЬНЫЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

ОДО «Сфератрэйд»
ул. Машиностроителей 29-117,
Минск 220118 Беларусь

УНН100972915

Velcom: +375 29 641 50 50
МТС: +375 29 541 50 50
Тел/факс: +375 17 341 50 50



И последнее. Вернемся еще раз к теме проводов... Шлюзы и повторители, которые создают сетевую инфраструктуру, на современном этапе нуждаются в проводах. Во-первых, им требуется внешнее питание. Их перевод на питание от батарей теоретически возможен, но все-таки производители предпочитают пока использовать внешние источники питания. Во-вторых, основная задача шлюза, как видно из вышесказанного, – производить стыковку беспроводной сети с обычной локальной сетью объекта. Т.е., шлюзы также используют провод, чтобы донести информацию до сервера. Конечно и здесь можно обойтись Wi-Fi точкой доступа или же встроить шлюз прямо в компьютер, но удобнее разместить его в той точке пространства, где он оптимально будет выполнять свои обязанности.

Кстати, благодаря технологии PoE (т.е. передаче питания прямо по витой паре) провода по обоим пунктам можно «уместить» в один кабель.

Однако, как нам кажется, наличие в системе нескольких метров проводов для подключения и питания шлюзов и повторителей точно не может лишить системы, построенные на этой технологии, честно заработанного звания «Беспроводная СКУД».

Реализация и примеры инсталляций

На сегодняшний день существует всего несколько подобных беспроводных СКУД, что объясняется, прежде всего, новизной технологии. Промышленные (неэкспериментальные) образцы оборудования появились в большинстве своем совсем недавно, когда сразу несколько производителей представили свои беспроводные решения с интервалом в 2-3 месяца.

Одну из этих систем приведем в качестве примера реализации описанной идеи беспроводной СКУД, не останавливаясь на подробных ТТХ (все эти цифры есть в отдельной врезке). Речь пойдет о системе SALTO RFID Wireless (Испания).

Как видно из названия, это система основана на бесконтактных (но обязательно – перезаписываемых) электронных ключах и электронных замках, использующих беспроводной протокол IEEE 802.15.4. Главной её особенностью является возможность комбинации (в любой пропорции) беспроводных онлайн-замков как с «классическими» проводными IP-контроллерами и считывателями, так и полностью автономными электронными замками, не имеющими связи с сервером в реальном времени. Это позволяет, в зависимости от конкретного объекта, создавать любые системы, с любым набором функционала и адекватной данному функционалу ценой. Например, часть точек доступа, наиболее важных с точки зрения надежности управления и контроля в реальном времени, можно оборудовать проводными IP-контроллерами. Другая часть помещений, где управление в реальном времени просто не нужно (часть кабинетов, переговорные и т.д.) оборудуются обычными электронными замками. А основная часть точек доступа – беспроводными онлайн-замками. Т.е., заказчику системы или инсталлятору совсем не обязательно выбирать между полностью проводной, автономной или беспроводной системой, по каждой конкретной точке доступа можно спокойно решать, какой из типов оборудования наиболее приемлем как по возможностям, так и по стоимости. Более того, автономные замки могут быть легко обновлены до

версии «беспроводной онлайн» спустя какое-то время после развертывания системы, для этого достаточно просто вставить в замок радиомодуль, приобретенный отдельно.

Такой подход к построению СКУД выгодно отличает системы SALTO от классических проводных систем, прежде всего по возможностям развертывания и расширения систем. И если для «классических» СКУД среднее количество точек доступа на объект зачастую колеблется около десяти, а еще чаще вовсе ограничивается несколькими «турникетами на входе в здание», то для систем SALTO среднее количество точек доступа на объекте приближается к пятидесяти. Клиент может установить такую систему как на турникет, так и на основную массу всех дверей в офисе, в банке или в университете – это не потребует дополнительных расходов на прокладку проводов до определенного помещения или двери.

Несколько слов о примерах инсталляций таких систем у нас и в мире. Поскольку на данный момент локомотивом описанной беспроводной технологии являются исключительно производители электронных замков, а их вотчиной до последнего времени были исключительно отели, то и первые установки таких систем также были осуществлены именно в отельном бизнесе. Например, LeMeridien Moscow Country Club, пятизвездочный отель, спорт-клуб, гольф-клуб и комплекс загородных резиденций в Красномгорском районе Московской области. Это достаточно показательный пример возможностей системы, не привязанной к прокладке проводов. Оборудование этого объекта комплексной СКУД SALTO Hotel RFID началось более 3-х лет назад и продолжается до сих пор, поскольку все это время комплекс продолжал функционировать, а бюджет на переоснащение объекта комплексной СКУД подразумевал поэтапное внедрение, в зависимости от выделяемых средств и сезонной загрузки. И хотя в отеле насчитывается всего около 130 номеров, общее количество точек доступа уже превысило 600. Изначально это были только 2 типа устройств доступа – «классические» проводные IP-контроллеры доступа (таких на весь объект не наберется и десятка) и автономные электронные замки на основной массе дверей. Когда компания SALTO Systems представила свою беспроводную систему, было решено произвести установку такого оборудования на части номеров, чтобы определить, насколько удобна и полезна новая технология. Естествен-

но, основное условие заказчика при этом – дооснащение ранее оборудованных номеров таким образом, чтобы отель не понес никаких дополнительных затрат, связанных с простоем номеров или необходимостью проведения специальных ремонтных работ. Установка заняла несколько рабочих дней. Большинство сотрудников, не говоря уже о гостях, даже не заметили, что в отеле шла настройка нового оборудования. Через несколько месяцев заказчик планирует подвести итоги тестовой эксплуатации и определить, в каких масштабах и на каких участках будет оправдано применять беспроводные электронные замки, а где ограничиться «обычными», без радиомодуля. Если же говорить о внедрении подобных систем на Западе, то там ситуация несколько иная. Прежде всего, это связано с тем, что там нет такого доминирования исключительно проводных систем, СКУД на основе автономных замков используются достаточно широко, отнюдь не ограничиваясь отельным сектором. Так SALTO Systems (Испания) установил в данном регионе уже несколько тысяч беспроводных СКУД.

процесса по глобальному и стремительному внедрению беспроводных технологий во все социальные сферы. Возможно, через какое-то время от беспроводных СКУД откажутся вовсе, но на наш взгляд такое вряд ли случится. Также не произойдет и полное погружение в беспроводность. СКУД, работающие «по воздуху» найдут свою нишу, где с ними не смогут конкурировать другие технологии. И как только это случится, появится достаточно большое предложение и на этом рынке. Еще один, более чем реальный сценарий, – появление беспроводных интегрированных систем безопасности. Конечно, видео по технологии ZigBee не будет передаваться никогда, зато беспроводная магистраль, развернутая для СКУД, перспективна для систем охранно-пожарной сигнализации, учета рабочего времени и некоторых других.

Скачок вперед через инновации

Именно перспективность данного направления доказывает успешный опыт SALTO Systems (Испания). Так, в опубликованном в 2013 г. Исследовании

Взяв за основу своей работы внедрение инноваций, SALTO Systems пересмотрела в корне область систем контроля доступа в том виде, в котором она была сформирована ещё в 2001 г. Миссия компании была ясна с самого начала: прийти на рынок и установить эталоны, на которые будут ориентироваться другие. Именно последнее ранжирование показывает, что SALTO Systems движется в правильном направлении и возглавляет его.

Реконструируя системы безопасности во всем мире, особенно в тех секторах, где безопасность наиболее важна (аэропорты, медицинские, образовательные, правительственные учреждения и отели), SALTO Systems полна решимости сделать управление доступом мирового класса доступным для каждой организации. Гарантируя это, SALTO Systems предлагает простые в использовании, чрезвычайно эффективные и полностью масштабируемые технологические решения. SALTO Systems объединяет в своих системах инновации и доступность.

На данный момент компания создала системы фактически для каждого типа двери: они применимы к любому их количеству – от 1 до 64 000 – и расположению в различных местах. К тому же, открытость структур SALTO Systems значит, что они совместимы с существующими системами, таким образом, пользователи могут объединить управление доступом с другими ресурсами самообслуживания и бесконтактными сервисами.

Касательно будущего: учитывая, что инновации – главная жизненная основа SALTO Systems, рынок ожидает еще много новых решений, которые станут определяющими направлениями, и именно от них будут отталкиваться остальные. Это миссия компании, и её SALTO Systems постоянно придерживается.

Таким образом, можно уверенно сегодня заявлять о том, что SALTO Systems – одна из самых стремительно развивающихся компаний в мире по производству беспроводных систем контроля доступа.



Перспективы

На данный момент никто не рискнет гарантировать технологии, которую мы описали, светлое будущее, хотя все предпосылки для этого есть. Достаточно, например, посмотреть на более чем солидный список имен компаний-основателей альянса ZigBee. Применение этой технологии на узком участке фронта – СКУД – лишь малая часть

IMS «Мировой рынок оборудования контроля доступа» говорится о том, что SALTO Systems поднялась сразу на несколько позиций и стала 8-м крупнейшим производителем в мире. Для бизнеса, начало которому было положено всего 12 лет назад, этот головокружительный успех означает, что Salto Systems – наиболее быстро растущая компания в своем секторе.

СЕРТИФИКАЦИЯ

Легион безопасности, ООО
Дистрибьютор компании SALTO
(Испания) в Республике Беларусь
220118, г. Минск, ул. Машиностроителей,
29-117, к. 7
Тел: (017) 340-42-17,
E-mail: info@mobotix.by

УНП: 100972915

Система контроля и управления доступом в зданиях Банка

Компания «Совершенные системы» представляет свой опыт в построении СКУД на банковских объектах. Для организации СКУД в зданиях банка, служебных и иных контролируемых помещениях нами используется сетевая электронная пропускная система под ТМ «СФИНКС». Сетевая СКУД состоит из сети контроллеров, управляющих считывателями и исполнительными устройствами, подключенной к серверу СКУД. Функционально такая СКУД должна обладать следующими возможностями:

Разграничение прав доступа

Позволяет разделить персонал на иерархические группы в зависимости от уровня доступа на объекты. Также можно ввести запрет доступа на предприятие в нерабочее время, не в свою смену, в выходные и праздничные дни. Для посетителей возможна выдача разовых ключей доступа, срок действия которых будет ограничен по времени. Информация обо всех проходах персонала сохраняется и используется в дальнейшем для учёта, а в случае необходимости – при проведении служебных расследований. Всегда можно установить, кто первым входил и последним выходил из помещения.

Функция защиты от передачи ключей доступа

СКУД не позволит войти на объект два раза по одному и тому же ключу доступа. Ни через одну дверь (турникет), ни через разные. В сочетании с функцией видеоидентификации позволяет определить правомерность использования ключа доступа сотрудником и предотвратить передачу ключей доступа посторонним.

Функция охраны

Позволяет переводить систему управления доступом в режим, при котором открыть дверь и попасть в помещение смогут только строго определённые сотрудники.

Эффективное управление персоналом

Программное обеспечение системы позволяет получать отчёты об опоздавших, не вышедших на работу или ушедших с работы преждевременно за любой необходимый отрезок времени. Таким образом, контроль за дисциплиной сотрудников банка осуществляет система, освобождая администрацию от данных функций. Программный модуль "Учёт рабочего времени" автоматически формирует таблицы учёта рабочего времени стандартной формы и передает информацию в программу 1С:Бухгалтерия.

Ограничение доступа к информации

Так же, как система управления доступом ограничивает доступ в отдельные помещения предприятия, она должна ограничивать доступ к информации системы для различных категорий пользователей.

Централизованное управление всем зданием

Так, в случае срабатывания пожарной сигнализации, сотрудник охраны может моментально, не вставая с рабочего места разблокировать все двери в здании для беспрепятственной эвакуации работников и посетителей.

Также при получении информации о краже сотрудник охраны может моментально, не вставая с рабочего места,

заблокировать все выходы из здания и задержать злоумышленника.

Для каждого здания Банка можно создать в системе контроля доступа графические планы помещений с размещением информации о камерах, точках доступа и датчиках, доступных в системе.

Каждое событие в системе контроля доступа Банка протоколируется, архивируется и сопровождается соответствующим видеороликом, снятым одной или несколькими камерами видеонаблюдения.

СКУД парковки

Система контроля и управления доступом позволяет разграничить доступ на парковку Банка для сотрудников и посетителей. В качестве преграждающих элементов применяются автоматические шлагбаумы (ворота с электроприводом). Для считывания индивидуальных карточек (брелоков) используются всепогодные считыватели бесконтактных карточек. Для возможности доступа на парковку автомобилей, не имеющих карточки (автомобили такси, специальных служб и т.п.), дополнительно устанавливаются аудио/видеодомофон, который позволяет связаться с охраной и получить доступ на парковку. Выезд осуществляется аналогичным способом. За парковкой ведется видеонаблюдение.

Каждое событие в системе контроля доступа парковки протоколируется, архивируется и сопровождается соответствующим видеороликом, снятым одной или несколькими камерами видеонаблюдения.

В дополнение к вышеуказанным требованиям система безопасности банка может быть расширена следующими функциями:

- Интеграция с системой пожарной сигнализации и пожаротушения;
- Распознавание номеров автотранспорта с возможностью автоматического открытия шлагбаума (ворот);
- Поиск в архиве по области изображения и параметрам объектов;
- Детектирование наличия лиц в поле зрения камер;
- Автоматическое сопровождение объектов поворотными камерами без участия оператора;
- 2-х сторонняя диспетчерская аудиосвязь в местах установок видеокамер;
- Быстрое сканирование паспортов посетителей и печать пропусков;
- Автоматическая реакция на события, поступающие от системы видеоаналитики, охранной и пожарной сигнализации и пр., системы контроля доступа (например, блокировку/открытие дверей в случае появления/пропажи/длительного нахождения предмета в зоне обзора видеокамеры, автоматическая разблокировка запасных выходов в случае пожара);
- Функционирование системы безопасности при отключении централизованного электроснабжения не менее 4 часов;

- Интеграция подсистем безопасности банками, управление ими из единого места оператора.

Стоимость внедрения и эксплуатации СКУД «СФИНКС» значительно ниже, чем у сопоставимых по техническим возможностям систем контроля доступа, используемых в Республике Беларусь. Кроме технических и ценовых преимуществ СКУД «СФИНКС» предоставляет уникальное сервисное предложение:

Все корпоративные пользователи СКУД «СФИНКС» автоматически становятся участниками **бесплатной** программы сервиса, в которую входят:

- 5 лет гарантии производителя на все компоненты системы
- Безлимитная техническая поддержка
- Независимость условий сервиса для заказчика от места покупки оборудования
- Бесплатные обновления купленных ранее версий
- Полная совместимость версий
- Поддержка интеграции с информационными системами клиентов
- Адаптация продукта и поддержка специальных функций

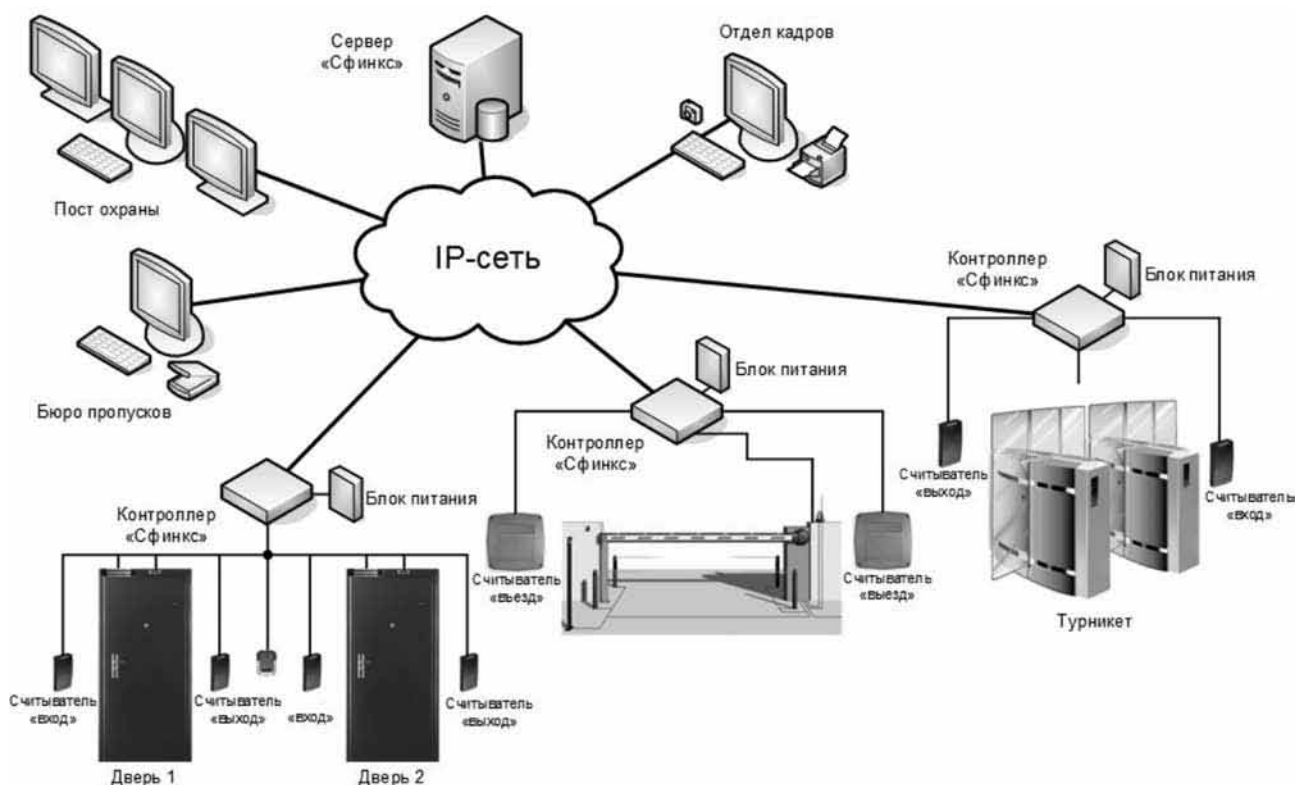
Возможности СКУД «СФИНКС»

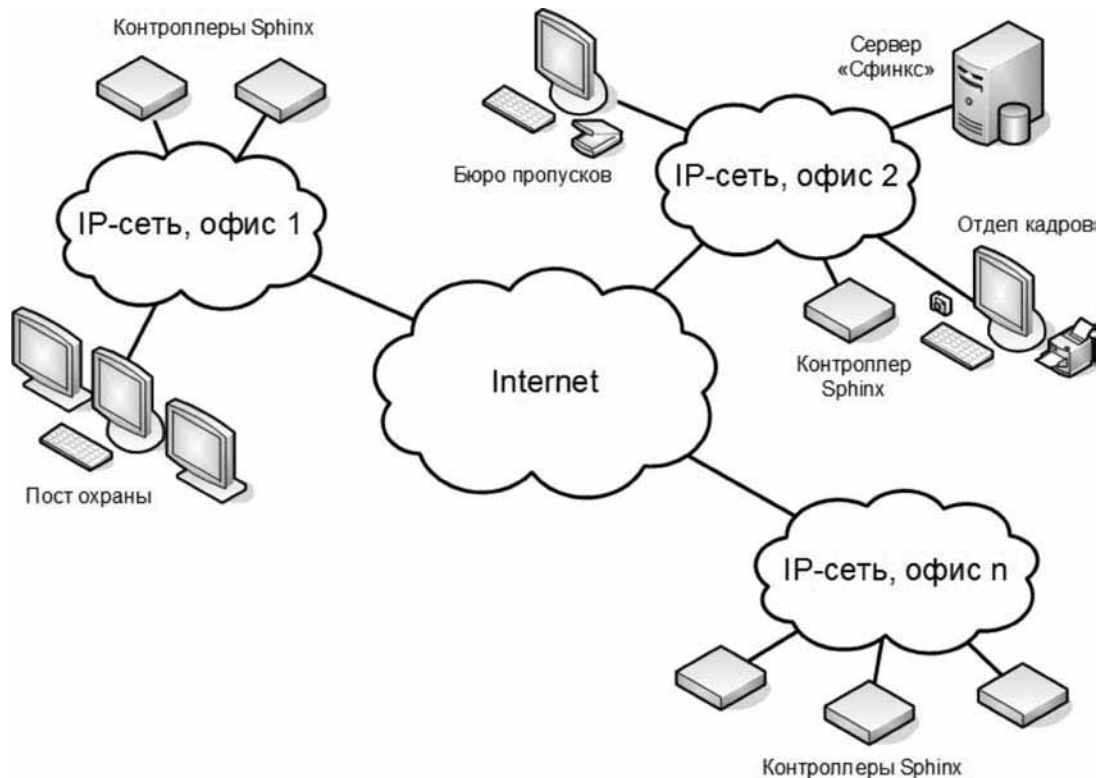
Контроллер «Сфинкс» всегда принимает решение о санкционировании доступа автономно, на основании информации об идентификаторах и режимах доступа, постоянно имеющейся «на борту» контроллера. При этом он не ожидает реакции сервера или какого-либо другого компонента системы. Время принятия решения пренебрежимо мало (порядок времени – десятки миллисекунд) и не зависит от количества объектов доступа, режимов, интенсивности проходов, количества контроллеров, качества связи с сервером и любых иных внешних факторов. Для обмена информацией между контроллерами и сервером «Сфинкс» используются стандартные Ethernet-интерфейс и IP-протокол. Каждый контроллер после первоначальной настройки представляет узел компьютерной сети, имеющий



Инсталляции СКУД «СФИНКС» в Республике Беларусь

ОАО «БНБ-Банк» первым из белорусских банков перешел на использование СКУД «СФИНКС». Совместными усилиями специалистов ООО «Совершенные системы» и сотрудников службы безопасности банка была налажена эффективная система централизованного управления контролем доступа головного офиса и подразделений с использованием расширенных модулей СКУД «СФИНКС». Это позволило сократить трудозатраты персонала службы безопасности, увеличить информативность отчетности СКУД, повысить безопасность охраняемых помещений, улучшить управляемость СКУД в целом. Использование СКУД «Сфинкс» помогло решить все стоящие перед службой безопасности банка задачи, связанные с организацией контроля доступа в помещения банка.





собственный IP-адрес. Возможна работа через сеть любой сложности и любой протяжённости. Создаваемый при работе IP трафик минимален. Например, в режиме ожидания контроллером события он равен нулю.

Архитектура СКУД «Сфинкс» – одноранговая, что обеспечивает максимальную устойчивость, стабильность работы и живучесть системы. Для увеличения количества точек доступа достаточно смонтировать необходимое количество стандартных контроллеров «Сфинкс». Не требуется приобретение каких-либо дополнительных устройств, типа управляющих контроллеров или концентраторов.

Возможности интеграции

В настоящее время доступна интеграция с системами видеонаблюдения Trassir, Ewclid, Intellect, Domination и Domination АВТО. Все функции интеграции со стороны «Сфинкса» – бесплатны. Интеграция СКУД «Сфинкс» и си-

стем видеонаблюдения обеспечивает следующие функции:

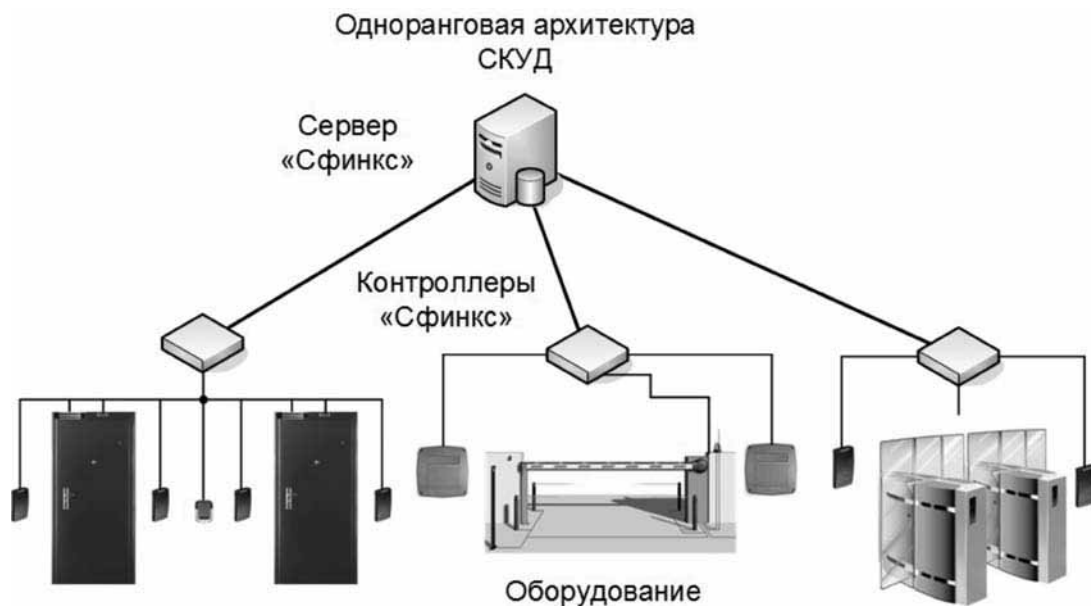
- Синхронизация архивов;
- Живое видео;
- Передача событий в систему видеонаблюдения;
- Распознавание автомобильных номеров.

Режимы доступа

СКУД «Сфинкс» позволяет создавать режимы доступа практически любой сложности, включая многосменные графики, праздничные дни, исключения из правил и т.д.

Возможно включение специальных правил доступа, как то доступ с дополнительным вводом PIN-кода, проход только вдвоём, проход только с дополнительной санкцией охранника, проход только через сборник пропусков. Количество режимов в общем случае неограниченно.

Картоприёмники (КП) предназначены для сбора карт посетителей при выходе или выезде их с территории пред-



приятия. К контроллеру «Сфинкс» может быть подключено до 2-х картоприёмников (на вход и на выход). Поддерживаются любые модели КП, предусматривающие управление от СКУД. Возможна также бюджетная реализация функции: использование вместо картоприёмников простых дополнительных считывателей, установленных на посту охраны. Для картоприёмников, имеющих вход управления «вернуть карту», возможен проход как разовых (с изъятием), так и постоянных (с возвратом) пропусков.

СКУД «Сфинкс» при необходимости позволяет реализовывать сложные схемы доступа персонала. Возможны:

- Карта/отпечаток пальца + PIN-код;
- Проход только вдвоём;
- Проход только с дополнительной санкцией охранника;
- Проход только через сборник пропусков;
- Проход через шлюз.

При переходе с уже имеющейся системы на СКУД «Сфинкс», стандартной функцией импорта можно получить из таблицы MS Excel в БД «Сфинкс» следующие данные:

- ФИО;
- Табельный номер;
- Должность;
- Отдел;
- Код пропуска;
- Примечание.

Основные функции СКУД «Сфинкс»:

- Модульная структура ПО, позволяющая сделать оптимальный выбор для конкретного объекта;

- Удалённая активация дополнительных модулей ПО;
- Автоматическая диагностика и резервирование базы данных;
- Клиент-серверная архитектура ПО. Взаимодействие сервера с клиентскими местами через IP-сеть. Функционирование любого числа удалённых клиентских мест с потенциальным доступом ко всем функциям системы;
- Взаимодействие сервера с контроллерами системы через IP или RS485 сеть;
- Удалённое управление точками доступа (блокирование, разблокирование, управление автономной памятью);
- Управление разнообразными преграждающими устройствами: турникетами, дверьми, воротами, шлагбаумами, шлюзами;
- Принятие решения контроллером – всегда автономное, даже в случае использования сложных схем доступа;
- Зональный контроль и пресечение повторных проходов (Antipassback);
- Сложные схемы доступа (карта + PIN-код, проход только вдвоём, проход только с дополнительной санкцией охранника, проход через шлюз);
- Создание списка персонала предприятия и ограниченный допуск персонала по точкам доступа, по направлению и по времени;
- Импорт персонала из таблицы MS Excel;
- Идентификация объектов доступа по их электронным или биометрическим идентификаторам;
- Регистрация всех происходящих в системе событий: проходы, запреты доступа, потеря и восстановление связи с контроллерами, взломы, удерживания дверей, пожары;
- Оперативное нахождение сотрудников на территории;
- Настройка прав доступа операторов к функциям системы;
- Интеграция с ActiveDirectory, после чего сотрудник может входить в свою учётную запись только находясь в одной из разрешённых зон доступа;
- Протоколирование действий операторов системы;
- Гибкая настройка прав операторов системы на доступ к различным функциям и вкладкам программы;
- Создание графических планов объекта и размещение на них точек доступа с возможностью управления и видеонаблюдения, с возможностью просмотра живого видео;
- Контрольный считыватель с множеством функций: мгновенный ввод кодов пропусков в систему, дальнейший быстрый поиск их в базе данных, оперативная выдача пропусков посетителям и вход операторов в систему.

Базовые отчёты:

- Быстрый доступ к произвольной выборке событий системы (функция «Архив»);
- По событиям системы (проходам, запретам доступа, проходам с пульта, взломам, изменениям статуса связи контроллеров);
- Список персонала;
- Список режимов;
- Журнал действий операторов;
- Кто где находился в заданный момент времени.

Учёт рабочего времени:

- Создание рабочих графиков персонала. Допускаются периодические графики с периодом от 1 до 31 дня. На каждый день может быть задан интервал рабочего времени и обеденного перерыва;
- Назначение рабочих графиков персоналу. Допускается назначение графиков сразу любой группе персонала (индивидуально, отделу, группе отделов и т.п.). Предусмотрен ввод «исключений из правил» – праздников, выходных

Февраль, 2014

Практический семинар

Актуальные подходы к построению СКУД

Вопросы внедрения, практика построения, интеграция (СВН, 1С, ОПС).

На основе ТМ «Сфинкс»/«Trassir»

Современные подходы
Лучшие практики
Задачи и решения

Отдельная секция:
Построение СКУД на банковских объектах

Предварительная регистрация
на сайте: aercom.by



на работу в неурочное время и т. п.;

- Получение отчётов за любой исторический период;
- Нарботка персонала (табель). Стандартная форма Т-13. Учёт по заданному графику или по фактическому присутствию;
- Автоматическая выгрузка таблицы Т-13, заполненной данными на основании информации о проходах, накопленной в СКУД, в программу «1С:Предприятие»;
- Отчёт о нарушениях графика. Содержит информацию об опозданиях на работу, поздних приходах с обеда и ранних уходах с работы;
- Отчёт – список отсутствий в течение рабочего дня.

Наблюдение:

- Наблюдение в режиме реального времени за происходящими в системе событиями;
- Поиск событий на поэтажных графических планах объекта;
- Поддержка многомониторных конфигураций;
- Конструктор видов экрана для поста наблюдения, позволяющий как угодно располагать и настраивать компоненты пользовательского интерфейса;
- Возможность интегрировать живое видео в вид наблюдения, в том числе для реализации функции видеопознания;
- Функция автоскрытия с экрана персональных данных прошедших людей по прошествии установленного времени;
- Звуковое оповещение оператора об ожидании санкции на доступ сотрудника;
- Возможность для оператора давать санкцию на доступ сотрудникам, предъявляя свой идентификатор.

Оформление пропусков:

- Создание и редактирование произвольного количества шаблонов пропусков;
- Назначение разных шаблонов пропусков произвольным группам сотрудников;
- Печать пропусков на основании шаблонов и персональных данных сотрудников;
- Печать непосредственно на принтер или в файл;
- Распечатка как одной карточки, так и нескольких наклеек, оптимально размещённых на листе произвольного формата.

Обслуживание посетителей:

- Создание списка пропусков посетителей;
- Интерфейс для выдачи/сбора пропусков (АРМ Бюро пропусков).

При выдаче происходит привязка к паспорту или другому документу посетителя;

- Ограничение срока действия пропуска;
- Хранение истории выдачи пропусков;
- Распознавание документов посетителей. Фотографии, полученные из предъявленных документов, могут отображаться на посту наблюдения.

Реакция на события:

- Создание списка действий, которые будут выполняться системой автоматически при наступлении определённых событий (фактов и запретов доступа, взломов, изменений статуса связи с точками доступа);
- Позволяет выполнять события по расписанию и осуществлять управление точками доступа путём перевода их в заблокированный, разблокированный или нормальный режимы;

Автопарк:

- Задание списков личных автомобилей сотрудников и служебного автотранспорта предприятия, имеющих право на проезд на территорию предприятия;
- Интерфейс для установления соответствия между сотрудниками и их личными автомобилями, а также для выдачи путевых листов на служебный автотранспорт;
- Хранение истории создания путевых листов;
- Фиксация перемещения сотрудников, «привязанных» к автомобилю, вместе с автомобилем.

Платёжная система:

- Позволяет предоставлять сотрудникам платные услуги и производить их учёт при помощи личных идентификаторов;
- Создавать для сотрудников различные типы счетов, отличающихся единицами измерения, минимальным шагом их изменения и размером кредита;
- Создавать различные «меню», пунктами которых могут являться как товары, так и услуги;
- Выбирать позиции заказа с помощью сканера штрих-кода или ввода с клавиатуры;
- Получать отчёты о движениях по счетам.

Взаимодействие с другими системами:

- Системы видеонаблюдения Domination, Ewclid, Trassir, Интеллект.
- Произвольное программное обеспечение заказчика – прямое взаимодействие с базой данных СКУД, либо обмен данными через открытый интерфейс интеграции.

Отчёты «Сфинкс»

- Полный список событий системы: состоявшиеся проходы, запреты доступа, санкционированные с пульта управления проходы, взломы, изменения статуса связи с контроллерами, факты удержания дверей в открытом состоянии;
- Нарботка персонала (табель Т13). Возможны отчёты по фактической наработке или строго по графику, за вычетом обедов, от первого входа до последнего выхода;
- Нарушения графика: опоздания, ранние уходы, факты отсутствия в течение рабочего дня, возможно игнорирование нарушений меньше заданного интервала;
- Список персонала: ФИО, отдел, должность, табельный номер, режим, код пропуска, список разрешённых точек доступа, срок действия пропуска;
- Список режимов: название, тип, время действия, список дней с рабочим временем и интервалами доступа;
- Журнал действий операторов: время выполнения действия, имя оператора, IP-адрес клиентского места, номер и название точки доступа, табельный номер и ФИО объекта доступа, описание действия;
- Кто где находился в заданный момент времени. Возможно либо указание точной даты и времени, либо опция «текущий момент времени». Предусмотрен выбор объектов и зон доступа, итоговый список может быть отсортирован по объектам или по зонам доступа;
- Список въездов-выездов (автопарк). Данные, упорядоченные по датам: модель, гос. номер автомобиля, его режим и времена въездов и выездов;
- Журнал проходов посетителей. Дата, время, точка доступа, направление, данные посетителя (ФИО, дата рождения, документ, удостоверяющий личность, место жительства и примечание);
- Журнал движений по счетам (платёжная система). Время, оператор системы, владелец и тип его счёта, значения счёта до и после операции, детализация операции (позиция, стоимость, количество, итог).

Совершенные системы, ООО

223051, Минский р-н, а/г Колодищи, ул. Короткая, д. 8, комн. 31
Тел./факс: (017) 508-23-33, (029) 370-20-22
E-mail: info@soversys.by
Сайт: www.soversys.by

УНП: 191152890



Построение СКУД распределенных объектов на базе оборудования GeoVision

Компания «Спецэлектро ЛТД» является официальным дистрибьютором GeoVision в Республике Беларусь. Специалистами компании были проведены ряд инсталляций данной системы на объектах нашей страны. Об особенностях и преимуществах работы системы мы говорили с Алексеем Седнёвым, инженером-инсталлятором.

Сегмент применения СКУД GeoVision в Беларуси достаточно широк – офисы, банки, гипермаркеты, торговые центры. Установка системы сейчас проводится с перспективой и возможностью будущей интеграции между объектами (офисами) и задачами централизованного контроля, что является одним из достоинств системы. Также СКУД GeoVision позволяет осуществлять интеграцию существующего на объектах оборудования СКУД, СВН, ОС в единую систему.

Состав системы:

- Программная часть: GV-AS Manager, GV-AS Remote, GV-AS Web;



- Аппаратная часть, IP-коммутаторы от одной до 8 дверей;



Система имеет возможности:

- объединения подсистем;
- построения иерархической системы посредством глобальной сети;
- полная интеграция в единый ком-

плекс с возможностью масштабирования с системами видео-наблюдения GeoVision;

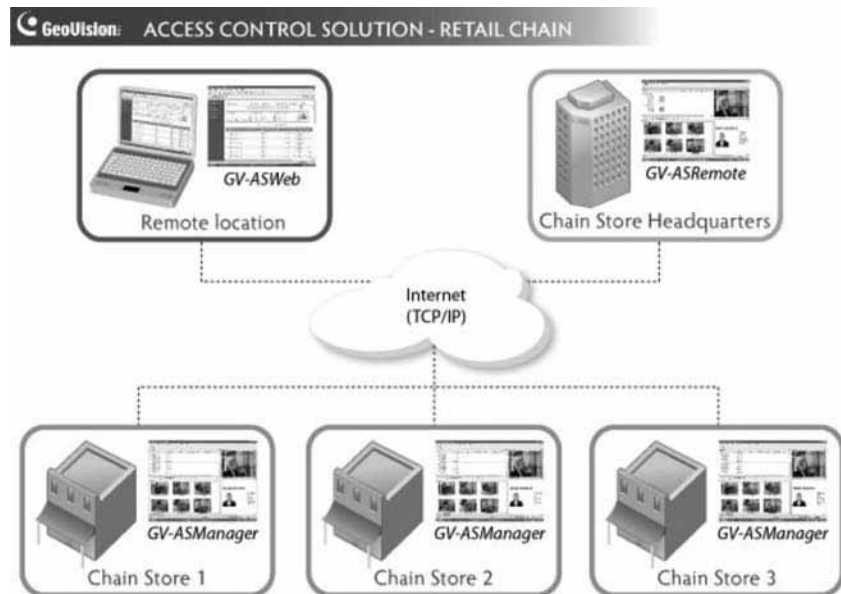
- организации мониторинга пожарных и охранных систем посредством цифровых входов IO.

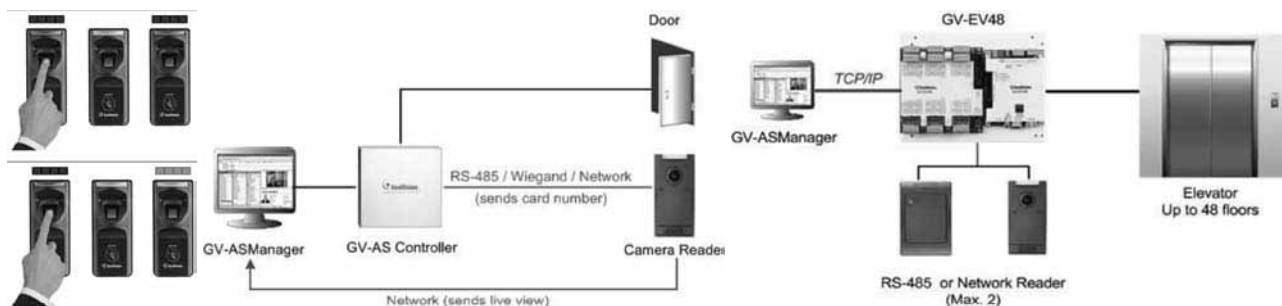
Организация СКУД для офиса на базе GeoVision

Как правило, основные требования для СКУД офиса: контроль прихода-ухода с работы, создание системы «Антипроходов», разграничение доступа по категориям сотрудников.

Для решения данных задач применя-

ются контроллеры GV-AS810 (позволяющие осуществлять контроль до восьми дверей с одно/двухсторонними проходами), GV-AS410 (до четырех дверей с одно/двухсторонними проходами), GV-AS210 (до четырех дверей с одно/двухсторонними проходами), GV-EV48 (контроллер, используемый в лифтах с управляемым поэтажным доступом: до 48 этажей). Специализированные точки доступа защищены биометрическими считывателями GV-GF Fingerprint Reader. При помощи комбинированного IP-ридера GV-CR420 со встроенной 4-х Мп широкоугольной камерой





можно организовать режим доступа карта+детекция лица. Ридер интегрируется как в систему доступа, так и в систему видеонаблюдения.

Из основных особенностей СКУД GeoVision можно отметить следующие:

- возможность подключения к одному контроллеру до восьми дверей и до шестнадцати бесконтактных считывателей;
- возможность контроля доступа на этаж посредством лифта;
- применение в качестве связи сервера с приборами IP-протокола;

Используемые идентификаторы: Em-Marlin и Mifare.

Системы видеонаблюдения, используемые в интеграции со СКУД GeoVision

В основном используются IP-камеры 1,3–2 Мп, как с ИК подсветкой, так и без, оснащенные вариофокальными объективами, режимы работы день/ночь, питание по PoE, с WEB интерфейсом. Используются поворотные камеры с 18-20-кратным оптическим зумом от 2 Мп.

Большинство объектов, на которых устанавливалась и проектируется система СКУД GeoVision в Беларуси, относятся к многофункциональным. После вступления в силу Постановления Совета Министров №1135, на всех вводимых в эксплуатацию объектах использовались увеличенные ёмкости хранения данных с расчётом времени хранения не менее 30 суток. По всем остальным параметрам система IP-видеонаблюдения GeoVision соответствует требованиям Постановления №1135. В качестве хранилищ данных на крупных объектах используются специализированные сервера бренда GeoVision с возможностью установки до 20 жёстких дисков (до 4 Тбх20) на каждый сервер.

Интеграция

СВН и СКУД. Уровень интеграции СВН и СКУД GeoVision очень глубокий, отличается качеством и надёжностью работы. СКУД GeoVision полностью интегрируется с оборудованием СВН на базе GeoVision (DVR, а также с IP-решениями). К каждой точке доступа можно «при-

вязать» до двух видеокамер. В момент авторизованного прохода через контролируемую точку доступа делается фотоснимок и привязка к видеоролику. Можно осуществлять мониторинг камер в режиме реального времени, а также управление поворотными PTZ камерами.

Пожарная сигнализация. Интеграция осуществляется на уровне тревожных входов IO. В случае возникновения чрезвычайной ситуации, пожарная сигнализация выдаёт сигналы на входы IO, система автоматически разблокирует все контролируемые точки доступа и оповестит оператора о событии. Если бы интеграция была на уровне интерфейса (в новой версии ПО появилась возможность сделать это на базе IO так, что общий интерфейс не обязателен), можно было бы осуществить автоматическое всплытие изображения с камер, установленных в точке возможного возгорания.

Охранная сигнализация. Преимущество в использовании СКУД GeoVision в том, что с одной программы и одного рабочего места мы видим несанкционированный доступ к защищаемым помещениям, осуществляем мониторинг и управление системой доступа. В перспективе было бы разумно полностью объединить систему контроля и управления доступом и автономную систему охранной сигнализации.

Организация интегрированной системы безопасности головного офиса.

Централизованный мониторинг и контроль осуществляется программным модулем центрального мониторинга GV-AS Remote. Программный модуль имеет возможности:

- контроля многочисленных удалённых GV-ASManagers, установленных на локальных серверах;
- удалённого многоканального мониторинга в режиме реального времени;
- удалённого воспроизведения ранее записанных событий;
- обеспечения базового контроля за срабатыванием дверей и сигнализаций.

Система под управлением AS Manager

работает автономно и самостоятельно в рамках выделенного объекта. Все настройки и конфигурирование системы на объекте выполняются непосредственно при помощи ПО AS Manager. AS Remote служит исключительно для удалённого мониторинга и контроля. Для более детального изучения журналов событий, синхронизированных с видео, используется модуль GV-AS Web, доступ к которому осуществляется посредством WEB-интерфейса. Для удалённого контроля объектов (в любое время суток) сервера с установленным ПО AS Manager должны быть включены.



В заключение можно констатировать, что построение СКУД на базе GeoVision имеет ряд весомых преимуществ. В частности, благодаря мощным сетевым возможностям, многофункциональному надёжному ПО, возможностям глубокой интеграции с подсистемами СКУД GeoVision получается надёжной, гибкой и имеет перспективы неограниченного масштабирования.

**Седнёв Алексей,
«Спецэлектро ЛТД»**



Спецэлектро Лтд, ООО
Республика Беларусь, 220026,
г. Минск, ул. Корицкого, 3
Тел./факс: (017)295-22-12, (017)295-43-34,
(017)295-77-92
E-mail: info@spetselectro.com
Сайт: www.spetselectro.com

УНП: 100080014

Интеллектуальные решения безопасности CEM Systems

СП «Унибелус» ООО, официальный представитель CEM Systems (Великобритания), предлагает интеллектуальные решения для управления безопасностью для объектов любого размера. Полнофункциональная, проверенная временем система AC2000 от CEM является основой надежных решений для управления безопасностью на объектах любого масштаба – от небольших до огромных, состоящих из нескольких зданий.

AC2000 – многофункциональная СКУД

Система AC2000, являющаяся основным предложением CEM, позволяет заказчикам получить надежную, инновационную и многофункциональную систему управления доступом. AC2000 представляет собой комплексную систему управления безопасностью с возможностью интеграции со средствами безопасности сторонних производителей, такими как системы видеонаблюдения, системы ОПС, домофонные системы, системы защиты периметра и т.д. AC2000 не только использует передовой ассортимент аппаратных средств CEM, включая интеллектуальные считыватели IP-карт, комплексные дактилоскопические считыватели и работающие по сети Ethernet контроллеры, но и обеспечивает полную совместимость с узлами считывания от сторонних производителей.

AC2000 SE (Standard Edition) –



мощная комплексная система управления средствами безопасности для средних и крупных объектов. Система AC2000 SE является многофункциональным, полностью интегрированным

решением, предназначенным для обеспечения контроля доступа, обработки тревожных сообщений и работы с карточками доступа и фотографиями. С учетом того, что CEM выпускает как аппаратные, так и программные средства, AC2000 SE может быть дополнительно адаптирована в

соответствии с конкретными требованиями, что делает ее одной из наиболее всеобъемлющих систем управления безопасностью, представленных на рынке.

Являясь идеальным решением для средних и крупных объектов, система AC2000 SE может выступать в качестве центральной системы управления средствами безопасности (SMS), обеспечивая полную интеграцию с охранными системами сторонних производителей. Признанная отраслевым эталоном надежности, отвечающая самым высоким требованиям безопасности наша система AC2000 SE успешно используется на многих крупнейших объектах по всему миру.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА:

- Высокая стабильность и устойчивость
- Полная системная интеграция
- Интеллект на уровне считывателя обеспечивает нулевое время простоя
- Практически неограниченное расширение
- Полностью настраиваемое решение
- Усовершенствованные средства протоколирования и анализа
- Полная интеграция с биометрическими системами
- Оптимизация операций на объекте
- Стандартная система передачи данных
- Локализованные версии

AC2000 Lite – интегрированная система безопасности



для малых и средних объектов. Предназначенная для небольших и средних зданий система AC2000 Lite является идеальным, экономически выгодным решением для

осуществления контроля доступа, обработки тревожных сигналов и работы с карточками доступа и фотографиями для объектов с количеством защищаемых дверей не более 128. Обеспечивающий основные функции системы AC2000 SE программный пакет AC2000 Lite является точкой отсчета в сфере СКУД, как одно из наиболее полных решений, доступных на современном

рынке по управлению средствами безопасности для небольших и средних объектов.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА:

- Экономичный вариант системы управления безопасностью
- Контроль до 128 дверей и до 10 000 пользователей
- Многофункциональный программный пакет, поставляемый на одном CD, включает в себя программные модули контроля доступа, графического интерфейса тревожных событий, средства подготовки идентификационных карт, модули учета рабочего времени и использования прав доступа, модули интеграции с системами видеонаблюдения и многое другое.

AC2000 AE (Airport Edition) – комплексная специализированная система управления безопасностью для аэропортов.



едиственная на рынке специализированная система управления средствами безопасности для аэропортов. AC2000 AE – это

мощное и полностью интегрированное решение управления средствами безопасности, ее функции выходят далеко за рамки обычной системы контроля доступа. Широкий спектр функций, специфичных для авиации, включая активацию стоек регистрации, разделение пассажиропотоков и мониторинг посадочных трапов делает AC2000 AE не просто системой контроля доступа, но и органичным элементом рабочей среды аэропорта. AC2000 AE является бизнес-решением, призванным помочь аэропортам получить дополнительный доход и работать более эффективно. Система AC2000 AE, созданная в результате тесного 25-летнего сотрудничества с аэропортами, стала ведущим выбором для систем безопасности аэропортов по всему миру.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА:

- Единственная в отрасли специализированная система контроля доступа для аэропортов
- Постоянно совершенствуется для

удовлетворения требований в сфере авиации

- Облегчает работу сотрудников аэропортов и повышает эффективность таких операций, как контроль посадки, активация стоек регистрации, связь с системой выписки накладных.

Аппаратные решения

СЕМ является неизменным лидером отрасли в разработке передовых аппаратных решений.

Сетевые IP-считыватели



Передовой ассортимент IP-считывателей производства СЕМ поддерживает внутреннюю базу данных, что обеспечивает возможность круглосуточной непрерывной проверки полномочий карт доступа, сводя к нулю время неработоспособности системы.

Считыватели СЕМ, являющиеся наиболее совершенными в отрасли, оснащены клавиатурой для ввода PIN-кода, ЖК-дисплеем для отображения сообщений и сохраняют внутреннюю базу данных для автономной работы на защищаемой двери.

Портативные считыватели



Портативные считыватели СЕМ обеспечивают гибкость и адаптивность для не-медленной организации

точек контроля доступа, не требующих физического оснащения стационарных защищенных проходов. Портативные считыватели СЕМ представляют собой легкие переносные карт-ридеры, являющиеся идеальным решением реализации мобильных мер безопасности. Оснащенный крупным сенсорным TFT-экраном с простой системой навигации портативный считыватель обеспечивает функции проверки идентификационных карточек на удаленных объектах или временных проходах, не имеющих сети электропитания, и может использовать-

ся в качестве мобильного устройства для выборочной проверки правомерности доступа внутри зон с ограниченным доступом.

Интегрированные решения с идентификацией по отпечаткам пальцев



СЕМ предлагает линейку считывателей карт с возможностью биометрической идентификации. Комплексный считыватель, осуществляющий функции СКУД и дактилоскопической идентификации, может использоваться для управления доступом на критические объекты инфраструктуры, требующие дополнительных прав доступа. Сочетание программного обеспечения AC2000 и поставляемого СЕМ считывателя отпечатков пальцев S610f позволяет клиенту создать комплексную биометрическую систему контроля доступа без необходимости покупки отдельной биометрической системы.

Интеллектуальный Терминал Доступа



На сегодняшний день emerald является наиболее многофункциональным терминалом доступа в отрасли. Устройство сочетает в себе контроллер точки доступа, считыватель карт и интегрированный интерком. Встроенная клавиатура с функцией скремблирования позволяет обеспечить дополнительный уровень безопасности в критических зонах.

Система питания средств контроля доступа по Ethernet сети (PoE+)

Технология PoE+ обеспечивает задачу по существующей локальной вычислительной сети не только данных, но и напряжения питания для IP-устройств контроля доступа, защищающих двери. Это сокращает стоимость проекта за



счет устранения необходимости подведения силовой сети к каждой двери, оснащенной устройством контроля доступа. Инновационная технология PoE+ от СЕМ позволяет подавать питание на устройства контроля доступа, установленные на дверях, с током до 2 А (в зависимости от длины пролета), что в сочетании с функцией "умного" резервного аккумулятора делает решение PoE+ по-настоящему уникальной и надежной концепцией.

Внедрения

В настоящее время системы СЕМ используются для защиты объектов более чем в 40 странах по всему миру. Решения СЕМ обеспечивают поддержку пользователей во многих сферах, в том числе в нефтехимической отрасли, авиации и здравоохранении, в общеобразовательных и финансовых учреждениях. На территории Республики Беларусь решения СЕМ установлены и успешно используются на следующих объектах:

1. РУП «Национальный аэропорт Минск»;
2. Офисное здание Белорусской калийной компании;
3. Логистический центр ООО «Двадцать четыре»;
4. Республиканское транспортно-экспедиционное унитарное предприятие «Белинтертранс – транспортно-логистический центр» Белорусской железной дороги;
5. ОАО «Полоцкий молочный комбинат»;
6. Автовокзал «Центральный» (г. Минск);
7. ГУ «Центральная поликлиника МВД РБ»;
8. РУП «Белоруснефть-Витебскоблнефтепродукт»;
9. Министерство экономики РБ;
10. ИООО «Газпромнефть-Белнефтепродукт»;
11. ГУ «Республиканский научно-практический центр эпидемиологии и микробиологии».

Унибелус, СП ООО
220033, г. Минск, ул. Нахимова, 10
Тел./факс: (017) 291-15-05, 230-72-40
E-mail: info@unibelus.com
Сайт: www.unibelus.by

РУНП: 100834637

Системы контроля и управления доступом, представленные на рынке Беларуси, 2013

Характеристики		
Общая информация		
Наименование СКУД	«BRAVO»	«GeoVision»
Представитель в РБ (компания)	ЧП «Фабрика турникетов и систем», производитель	ООО «Спецэлектро ЛТД»
Страна происхождения/год появления на рынке/ориентир. стоимость	Республика Беларусь/2005 г.	Тайвань/1998 г.
Срок гарантийных обязательств, мес.**	24	24 (60 при условии ТО)
Авторизованная (сервисная) поддержка в РБ	Да, ЧП «Фабрика турникетов и систем»	Да, ООО «Спецэлектро ЛТД»
Склад в РБ. ЗИП	Да, всегда в наличии	Да
Категория объектов	Предприятия, учебные заведения	Гипермаркеты, торговые центры, банки, многофункциональные объекты и пр.
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/Ч; ток нагрузки, А)**	Внешний 12 В АКБ 7 А/ч	ИБП есть. АКБ 2,2-40 А/ч
Наличие в СКУД беспроводных электронных устройств*	Устройства на базе WIFI, GPRS	- нет
Каналы передачи данных (считыватель-контроллер-сервер) *	выделенные линии связи; GPRS; RS485, RS422	выделенные линии связи
Канал передачи данных (электронное устройство-сервер)*	Ethernet; RS 422; RS 485; GPRS	перезаписываемая память идентификатора
Контроллеры		
Объем энергонезависимой памяти (кол-во событий), шт. **	300 000	1000000
Кол-во пользователей в системе (max), шт.**	50 000	40000
Вид*	автономные; сетевые	автономные; сетевые
Интерфейс подключения считывателей (протокол) *	Dallas Touch Memory; USB; RS 485	Wiegand 26-64 bit; RS 485
Кол-во исполнительных устройств, управляемых одним контроллером, шт.**	8	от 1 до 48
Интерфейс связи контроллера с сервером	Ethernet, RS 422, RS 485, GPRS	Ethernet, RS 485
Кол-во контроллеров в системе/доплата за доп. контроллер	Не ограничено	255 (до 4 бесплатно)
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – 1200 Контр-ра от устр./сервера хран. данных – 1200 (GPRS – не ограничено)	Исполнит-го устр-ва от контр-ра – 1200 Счит. устр-ва от контр-ра – 1200 Контр-ра от устр./сервера хран. данных – не ограничено
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	электромеханические замки, электромагнитные замки, турникеты, поясные / полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции, терминалы СКД по отпечаткам пальцев, терминалы СКД по геометрии лица, мн. другое	механические замки, электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции, другое
Предельные температурные условия эксплуатации (min/max), С**	от -30°C до +50°C (для различных устройств)	от 0°C до +65°C
Кол-во ИУ(max), шт. **	Не ограничено	48
Считыватели		
Поддерживаемые типы считывателей*	- контактные - бесконтактные - биометрические	- бесконтактные, с указанием дальности (60 мм) - биометрические
Класс климатического исполнения (IP)**	IP 40	До IP 66
Формат обмена с идентификатором *	Em Marine, Mifare, HID, Indala, ISO 15693, i-Code, Check Point, GSM	Em Marine, Mifare
Возможность реализации*	- 1-на факторная аутентификация; - 2-х факторная аутентификация; - 3-х факторная аутентификация	-1-факторная аутентификация; - 2-х факторная аутентификация;
Программное обеспечение (ПО)		
Требование к ОС	минимальные	Win XP/Vista/7/8/8.1x32/64
Кол-во клиентских мест в системе, шт./доплата за доп. место**	Не ограничено, все места бесплатные	-
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, возможность доработки SDK	Резервирование, архивирование, интеллектуальный поиск по архиву
Модули (функционал ПО)*	Контроль доступа и учет рабочего времени, биометрия, SMS оповещение, модуль школа + компьютерный класс и мн. др.	Интеграция с СВН: аналоговое/IP на базе Geovision, ACTi, AXIS, Arecont Vision, Bosch, Canon, CNB, Dlink, EtroVision, HUNT, Hikvision, IQinVision, JVC, LG, Mobotix, Panasonic, Pelco, Sony, Samsung, Sanyo, UDP, VERINT, VIVOTEC. ONVIF. Интеграция с ОС и ПС

Характеристики		
Общая информация		
Наименование СКУД	«Реверс» (модернизация СКУД «Кронверк»)	«Exsnet»
Представитель в РБ (компания)	ООО «Видео-СКУД»	ООО «Видео-СКУД»
Страна происхождения/год появления на рынке/ориентир. стоимость	Россия/2012 г. (СКУД «Кронверк» 2000 г.)/от 1 500 000 рублей	Россия/2009 г./от 400 000 руб.
Срок гарантийных обязательств, мес.**	24	24
Авторизованная (сервисная) поддержка в РБ	Да, ООО «Видео-СКУД» (Сертифицированный системный интегратор, Региональный сервисный центр, Дистрибьютор)	Да, ООО «Видео-СКУД» (Сертифицированный системный интегратор, Региональный сервисный центр, Дистрибьютор)
Склад в РБ. ЗИП	Да	Да
Категория объектов	Промышленность, адм. здания, офисы, школы и т.д.	Промышленность, адм. здания, офисы, школы и т.д.
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/Ч; ток нагрузки, А)**	Встроенный ИБП 12 В/1 А (АКБ 12 В 2,2 А/ч)	- нет
Наличие в СКУД беспроводных электронных устройств*	- нет	- нет
Каналы передачи данных (считыватель-контроллер-сервер)*	- выделенные линии связи и/или радиоканал	- выделенные линии связи
Канал передачи данных (электронное устройство-сервер)*	- перезаписываемая память идентификатора и/или радиоканал	- перезаписываемая память идентификатора
Контроллеры		
Объем энергонезависимой памяти (кол-во событий), шт. **	48 000	-
Кол-во пользователей в системе (max), шт.**	20 400 / не ограничено в режиме программного доступа	1020
Вид*	автономные; сетевые	автономные
Интерфейс подключения считывателей (протокол) *	Dallas Touch Memory; Wiegand 26, 33, 34, 40,42; USB; RS 485	Dallas Touch Memory, Wiegand 26`
Кол-во исполнительных устройств, управляемых одним контроллером, шт.**	от 1 до 16	1
Интерфейс связи контроллера с сервером	Ethernet, RS 232, RS 485	-
Кол-во контроллеров в системе/доплата за доп. контроллер	Не ограничено/от 1 500 000 рублей	-
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – 100 Счит. устр-ва от контр-ра – 25 Контр-ра от устр./сервера хран. данных – не ограничено	Исполнит-го устр-ва от контр-ра – 100 Счит. устр-ва от контр-ра – 25
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	механические замки, электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции, другое	механические замки, электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы
Предельные температурные условия эксплуатации (min/max), С**	Считыватели от -40°С до +50°С, контроллеры от +5°С до +40°С	от -30°С до +50°С
Кол-во ИУ(max), шт. **	Не ограничено	1
Считыватели		
Поддерживаемые типы считывателей*	- контактные - бесконтактные 0,1-1,5 м - биометрические - радиоканальные (1-15 м) - сканеры штрих кода Honeywell с интерфейсом RS-232 - сканеры биометрических признаков (отпечатков пальцев MA3000) и т.д.	- контактные - бесконтактные 0,1-1,5 м
Класс климатического исполнения (IP)**	IP 40	IP 54
Формат обмена с идентификатором *	Em Marine; Mifare; HID; Indala	Em Marine; HID
Возможность реализации*		- 1-факторная аутентификация
Программное обеспечение (ПО)		
Требование к ОС	ОС WINDOWS от версий 2000, и выше.	ОС WINDOWS от версий 2000, и выше
Кол-во клиентских мест в системе, шт./доплата за доп. место**	Не ограничено/бесплатно	-
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, возможность доработки SDK	Резервирование
Модули (функционал ПО)*	Интеграция: 1:С, с СВН/СОТ (CCTV ИНТЕЛЛЕКТ, ONVIF), с ОС и ПС, периметральной ОС	-

Системы контроля и управления доступом, представленные на рынке Беларуси, 2013

Характеристики		
Общая информация		
Наименование СКУД	PERCo, СКУД S-20, www.perco.ru	«Сфинкс»
Представитель в РБ (компания)	ИВОО «Просвет»	ООО «Совершенные системы»
Страна происхождения/год появления на рынке/ориентир. стоимость	Россия/1988 г.	Россия/2006 г./от 890 000 бел. руб. за точку доступа
Срок гарантийных обязательств, мес.**	до 24	60
Авторизованная (сервисная) поддержка в РБ	ИВОО «Просвет»	ООО «Совершенные системы»
Склад в РБ. ЗИП	Да	Да
Категория объектов	Офис, пром. предприятие, распределенные объекты	Возможность адаптации под любой объект
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/Ч; ток нагрузки, А)**	нет	Предоставляем выбор
Наличие в СКУД беспроводных электронных устройств*	нет	нет
Каналы передачи данных (считыватель-контроллер-сервер) *	- выделенные линии связи, локальная сеть предприятия	- выделенные линии связи
Канал передачи данных (электронное устройство-сервер)*	- радиоканал	нет
Контроллеры		
Объем энергонезависимой памяти (кол-во событий), шт. **	150000	до 400 000
Кол-во пользователей в системе (max), шт.**	50000	до 96 000
Вид*	сетевые	сетевые
Интерфейс подключения считывателей (протокол) *	RS 485	Dallas Touch Memory; Wiegand 26, 33, 34,40,42
Кол-во исполнительных устройств управляемых одним контроллером, шт.**	1	до 4
Интерфейс связи контроллера с сервером	Ethernet	Ethernet; RS 485
Кол-во контроллеров в системе/доплата за доп. контроллер	до 1000	Не ограничено/Бесплатно
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – до 100. Счит. устр-ва от контр-ра – до 1200. Контр-ра от устр./сервера хран. данных – не ограничено	Исполнит-го устр-ва от контр-ра – до 100. Счит. устр-ва от контр-ра – 100. Контр-ра от устр./сервера хран. данных – не ограничено
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	механические замки, электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат/полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции, другое	механические замки, электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат/полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции, другое
Предельные температурные условия эксплуатации (min/max), С**	от -40°C до +40°C	от -35°C до +45°C
Кол-во ИУ(max), шт. **	256	Неограниченно
Считыватели		
Поддерживаемые типы считывателей*	- бесконтактные, до 90 см - биометрические	- контактные - бесконтактные, с указанием дальности - биометрические
Класс климатического исполнения (IP)**	до IP 67	предоставляем выбор
Формат обмена с идентификатором *	Em Marine; Mifare; HID	Em Marine; Mifare; HID; Indala; ISO 15693; i-Code; Check Point; GSM
Возможность реализации*	- 1-факторная аутентификация; - 2-х факторная аутентификация; - 3-х факторная аутентификация	- 1-факторная аутентификация; - 2-х факторная аутентификация; - 3-х факторная аутентификация
Программное обеспечение (ПО)		
Требование к ОС	Win XP SP3 и выше	Linux, Windows
Кол-во клиентских мест в системе, шт./доплата за доп. место**	3/доплата за доп. клиентские места в зависимости от выбранной конфигурации ПО	Не ограничено/Бесплатно
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK
Модули (функционал ПО)*	Интеграция: 1:С, с СВН/СОТ (ONVIF), с ОС и ПС	Интеграция: 1С, СВН/СОТ (Trassir, Domination, Ewclid, Macroscop, Линия, VideoNet, Intellect), любые IP-камеры (ONVIF), с ОС и ПС, с периметральной ОС

Характеристики		
Общая информация		
Наименование СКУД	ИСО «Орион»	Интегрированная система безопасности ИСБ «777» Комплекс
Представитель в РБ (компания)	ЧСУП "ОрионПроект"	ООО «РОВАЛЭНТКОМПЛЕКС»
Страна происхождения/год появления на рынке/ориентир. стоимость	Россия/1998 г./ около 80 у.е. за контроллер	Республика Беларусь/1997 г., постоянная модернизация. Стоимость зависит от масштаба проекта. От 3.5 млн. руб.
Срок гарантийных обязательств, мес.**	18	24 месяца с даты ввода в эксплуатацию
Авторизированная (сервисная) поддержка в РБ	ЧСУП "ОрионПроект"	Да
Склад в РБ. ЗИП	Да	Да
Категория объектов	Может применяться на объектах всех категорий	Возможность адаптации на объекты всех категорий
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/ч; ток нагрузки, А)**	Собственная линейка резервированных ИП с выходным током от 1 до 8 А и возможностью подключения АКБ от 4 до 80 А/ч.	Встроенный ИБП (7 А/ч; 3 А), а также внешние ББП (собственная линейка), в зависимости от подключаемой нагрузки
Наличие в СКУД беспроводных электронных устройств*	нет	Электронные: замки, накладки на механический замок, цилиндры
Каналы передачи данных (считыватель-контроллер-сервер)*	- выделенные линии связи и/или радиоканал	выделенные линии связи и/или радиоканал
Канал передачи данных (электронное устройство-сервер)*	-	Перезаписываемая память идентификатора, и/или радиоканал
Контроллеры		
Объем энергонезависимой памяти (кол-во собитий), шт. **	32768	10000
Кол-во пользователей в системе (max), шт.**	32768 на один контроллер. В системе не ограничено.	100000
Вид*	сетевые	автономные, сетевые
Интерфейс подключения считывателей (протокол)*	Dallas Touch Memory; Wiegand 26, 33, 34,40,42; USB	Dallas Touch Memor; Wiegand 26, 33, 34,40,42; US; RS 232; RS 485
Кол-во исполнительных устройств управляемых одним контроллером, шт.**	2	128
Интерфейс связи контроллера с сервером	RS 485	Ethernet; RS 485
Кол-во контроллеров в системе/доплата за доп. контроллер	64512 контроллеров (63 ПК по 1024 контроллера). Количество контроллеров, управляемых системой лицензируется.	8000 контроллеров/3000 000 бел. руб. за КСО; 1440 000 за расширение ключа на 1 устройство
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – определяется падением напряжения (характер-ми кабеля). Счит. устр-ва от контр-ра – 100 (протокол Wiegand). Контр-ра от устр./сервера хран. данных – 3000 (RS-485, без доп. повторителей)	Исполнит-го устр-ва от контр-ра – 1200, без репитера, (каждый репитер + 1200) Счит. устр-ва от контр-ра – 50 Контр-ра от устр./сервера хран. данных – 1200, без репитера, (каждый репитер +1200)
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	Эл.мех. замки, эл.маг. замки, турникеты, калитки (поясные/полнорост., для аварийных выходов), ворота (распашные/подъемно-секцион./откатн.), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции	Замки (мех., эл.мех., эл.магн.), турникеты, калитки (поясн./полнорост., для аварийных выходов), ворота (распашные/подъемно-секцион./откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции. Любое эл. мех. или эл.магн. устройство. Логика работы системы гибко программируется
Предельные температурные условия эксплуатации (min/max), С**	от -30 °С до +50 °С	от -50 °С до +65 °С
Кол-во ИУ(max), шт. **	до 129 024	1 000 000
Считыватели		
Поддерживаемые типы считывателей*	контактные, бесконтактные (дальность определяется характеристиками считывателей), биометрические	контактные, бесконтактные, 15 см, биометрические
Класс климатического исполнения (IP)**	IP 20	IP 54 – IP 65 (различного)
Формат обмена с идентификатором *	Em Marine, Mifare, HID, Indala, ISO 15693	Em Marine, Mifare, HID, Indala, ISO 15693, i-Code, Check Point, GSM
Возможность реализации*	- 1-факторная аутентификация; - 2-х факторная аутентификация.	- 3-х факторная аутентификация
Программное обеспечение (ПО)		
Требование к ОС	Microsoft Windows XP, 2003 Server, Vista, 7	Windows XP sp3, Vista, 7, 8.1, Windows server 2003r2, 2008r2, 2012, 2012r2
Кол-во клиентских мест в системе, шт./доплата за доп. место**	200/количество сетевых рабочих мест лицензируется.	255/1.7 млн. бел. руб.
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK
Модули (функционал ПО)*	Интеграция: 1:С, с СВН/СОТ (Интеллект, SecurOS, Видеоинспектор, VideoNet, TRASSIR, PHOBOS, GOALcity, CVS, MACROSCOP, EWCLID. Прямая работа с IP поддерживающими технологию RASPLUS, с ОС и ПС, с периметральной ОС	Интеграция: Intellect, GEUTEBRUCK, Samsung. Полная интеграция: ОС ИСБ777, ПС (Бирюза), периметральной ОС (Рубикон, Раскат) СО (Гонг), СМ Неман (Ровалэнт)

Системы контроля и управления доступом, представленные на рынке Беларуси, 2013

Характеристики	SALTO inspired access	roger ®
Общая информация		
Наименование СКУД	SALTO	Roger
Представитель в РБ (компания)	ОДО «Сфератрэйд»	ОДО «Сфератрэйд»
Страна происхождения/год появления на рынке/ориентир. стоимость	Испания/2001 г.	Польша/1991 г.
Срок гарантийных обязательств, мес.**	36	36
Авторизованная (сервисная) поддержка в РБ	ОДО «Сфератрэйд»	ОДО «Сфератрэйд»
Склад в РБ. ЗИП	Да	Да
Категория объектов	Гостиницы, учреждения образования, административные учреждения, бизнес-центры, аэропорты, объекты спортивного назначения, производственные предприятия, банки, объекты военного назначения	Административные учреждения, бизнес-центры, объекты спортивного назначения, производственные предприятия, банки
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/ч ток нагрузки, А)**	Электронные наклейки/электронные замки: батареи AAA	Есть, 7 А/ч, 12 В
Наличие в СКУД беспроводных электронных устройств*	электронные замки; электронные наклейки на механический замок; электронные цилиндры	нет
Каналы передачи данных (считыватель-контроллер-сервер)*	выделенные линии связи	выделенные линии связи
Канал передачи данных (электронное устройство-сервер)*	- перезаписываемая память идентификатора и/или радио-канал	нет
Контроллеры		
Объем энергонезависимой памяти (кол-во событий), шт.**	3 000	32 000/256 000 при использовании в системе концентратора CPR32SE
Кол-во пользователей в системе (max), шт.**	64 000 в ПО гостиничного СКУД 4 000 000 в ПО классического СКУД	4 000
Вид*	автономные; сетевые	автономные; сетевые
Интерфейс подключения считывателей (протокол)*	SALTO	Wiegand 26, 33, 34, 40, 42; Magstripe; RACS
Кол-во исполнительных устройств управляемых одним контроллером, шт.**	2	2
Интерфейс связи контроллера с сервером	Ethernet	Ethernet; RS 485
Кол-во контроллеров в системе / доплата за доп. контроллер	Не ограничено	320
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – от типа ИУ. Счит. устр-ва от контр-ра -100 Контр-ра от устр./сервера хран. данных – ограничено топологией сети Ethernet	Исполнит-го устр-ва от контр-ра – от типа ИУ Счит. устр-ва от контр-ра – 150 Контр-ра от устр./сервера хран. данных – 1200 (RS 485), ограничено топологией сети Ethernet
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	Замки (мех., эл. мех., эл. магн.), турникеты, калитки (по-ясные/полнорост, для аварийных выходов), ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции и пр.	Замки (эл. мех., эл. магн.), турникеты, калитки (по-ясные/полнорост, для аварийных выходов), ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы, подъемные цепи, секции и пр.
Предельные температурные условия эксплуатации (min/max), С**	-	-
Кол-во ИУ(max), шт.**	Неограниченное кол-во ИУ, управляемых контроллерами;	
Неограниченное кол-во беспроводных электронных устройств.	640	
Считыватели		
Поддерживаемые типы считывателей*	контактные, бесконтактные до 10 см	контактные, бесконтактные до 15 см, бесконтактные увеличенной дальности – до 60 см, биометрические
Класс климатического исполнения (IP)**	IP 65	IP 65
Формат обмена с идентификатором *	i-Button; Proximity Picopass; Proximity LEGIC; DESfire/Mifare; HID i-Class	Em Marine; Mifare; HID; ISO 15693
Возможность реализации*	- 2-х факторная аутентификация	- 2-х факторная аутентификация
Программное обеспечение (ПО)		
Требование к ОС	Windows 2000, NT 4.0, XP, Vista, Windows 7, Windows 8; требует MS-SQL Express, MS-SQL 2005, 2008 или 2012	Windows 2000, NT 4.0, XP, Vista, Windows 7, Windows Server 2003, 2008
Кол-во клиентских мест в системе, шт./доплата за доп. место**	Не ограничено/без доплаты	ПО для конфигурации: не ограничено/ПО бесплатное ПО для UPB: не ограничено
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK
Модули (функционал ПО)*	ПО SALTO (низкоуровневый протокол), интерфейс передачи стороннему ПО. Интеграция: СВН/COT, ОС и ПС, с периметральной ОС (объединения в ПО Интеллект), с гостиничными системами автоматизации, с системами автоматизации зданий	-

Характеристики	 CEM SYSTEMS A Tyco International Company	 CEM SYSTEMS A Tyco International Company
Общая информация		
Наименование СКУД	AC2000SE	AC2000 Lite
Представитель в РБ (компания)	СП Унибелус ООО	СП Унибелус ООО
Страна происхождения/год появления на рынке/ориентир. стоимость	Великобритания/1988 г.	Великобритания/1988 г.
Срок гарантийных обязательств, мес.**	24	24
Авторизованная (сервисная) поддержка в РБ	СП «Унибелус» ООО	СП «Унибелус» ООО
Склад в РБ. ЗИП	Да	Да
Категория объектов	Средние и крупные объекты	Малые и средние объекты
Наличие встроенного/внешнего ИБП/БРП (емкость АКБ А/ч ток нагрузки, А)**	–	–
Наличие в СКУД беспроводных электронных устройств*	электронные накладки на механический замок; электронные цилиндры; портативные мультиформатные считыватели	электронные накладки на механический замок; электронные цилиндры; портативные мультиформатные считыватели
Каналы передачи данных (считыватель-контроллер-сервер)*	- выделенные линии связи и/или радиоканал	- выделенные линии связи и/или радиоканал
Канал передачи данных (электронное устройство-сервер)*	- Secure AES128bit encrypted 802.11g 2.4GHz WiFi	- Secure AES128bit encrypted 802.11g2.4GHz WiFi
Контроллеры		
Объем энергонезависимой памяти (кол-во событий), шт. **	8000	8000
Кол-во пользователей в системе (max), шт.**	200000	200000
Вид*	сетевые	сетевые
Интерфейс подключения считывателей (протокол)*	Wiegand 26, 33, 34,40,42; USB; RS 485	Wiegand 26, 33, 34,40,42; USB; RS 485
Кол-во исполнительных устройств управляемых одним контроллером, шт.**	2	2
Интерфейс связи контроллера с сервером	Ethernet, RS 485	Ethernet, RS 485
Кол-во контроллеров в системе / доплата за доп. контроллер	Не ограничено	128
Максимальная удаленность, м**	Исполнит-го устр-ва от контр-ра – 150 Счит. устр-ва от контр-ра – 150 Контр-ра от устр./сервера хран. данных – определяется типом кабеля и топологией сети ПД	Исполнит-го устр-ва от контр-ра – 150 Счит. устр-ва от контр-ра – 150 Контр-ра от устр./сервера хран. данных – определяется типом кабеля и топологией сети ПД
Исполнительные устройства (ИУ)		
Виды исполнительных устройств (ИУ), которыми может управлять СКУД*	электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы	электромеханические замки, электромагнитные замки, турникеты, поясные/полноростовые калитки, калитки для аварийных выходов, ворота (распашные/подъемно-секционные/откатные), шлюзы (автомат./полуавтомат.), шлагбаумы, болларды, антипарковочные модули, дорожные блокираторы
Предельные температурные условия эксплуатации (min/max), С**	от -40 °С до +40 °С	от -40 °С до +40 °С
Кол-во ИУ(max), шт. **	Не ограничено	128
Считыватели		
Поддерживаемые типы считывателей*	- бесконтактные (0,1–10 м) - биометрические	- бесконтактные, с указание дальности (0,1–10 м) - биометрические
Класс климатического исполнения (IP)**	IP 66	IP 66
Формат обмена с идентификатором *	Em Marine; Mifare; HID; Indala; DESFire; PicoPass	Em Marine; Mifare; HID; Indala; DESFire; PicoPass
Возможность реализации*	3-х факторная аутентификация	3-х факторная аутентификация
Программное обеспечение (ПО)		
Требование к ОС	Intel Core i3, 4GB RAM, 250GB SATA, 10/100 Ethernet	Intel Core i3, 4GB RAM, 250GB SATA, 10/100 Ethernet
Кол-во клиентских мест в системе, шт./доплата за доп. место**	172	5
Возможности ПО*	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK	Резервирование, архивирование, интеллектуальный поиск по архиву, доработка SDK
Модули (функционал ПО)*	Интеграция: 1:C, CBH/COT (American Dynamics, IndigoVision, Bosch, GenetecOmnicast, Milestone, MatriVideo, Mobotix), ОС и ПС, с периметральной ОС	Интеграция: 1:C, CBH/COT (AmericanDynamics), ОС и ПС, периметральной ОС

HIKVISION

Мегапиксельное качество аналогового видео. Технология 960Н от HIKVISION

(конфиденциально – только для тех, кто считает деньги)

История развития технологии 960Н:

- 2009 г. Компания SONY выпустила первый процессор «Effio-E» и новые ПЗС матрицы «Super HAD CCD II» – матрицы 960Н;
- 2010 г. Выпущены обновленные и улучшенные версии «Effio-E», а также начато производство ПЗС матриц 960Н повышенной чувствительности в инфракрасном (ИК) диапазоне – «EXview HAD CCD II», что позволяет строить камеры видеонаблюдения разрешения до 700 ТВЛ, эффективно работающими в ИК-подсветке;
- 2011 г. На Токийской выставке Tokyo Big Sight корпорация Sony презентовала новые процессоры «Effio-P» и «Effio-S», которые стали дальнейшим усовершенствованием «Effio-E», а также продемонстрировала работу камеры видеонаблюдения разрешения 700 ТВЛ на их основе;
- 2012 г. Компания HIKVISION на международной выставке Security China 2012 предоставила первый в мире серийный видеорегистратор, разработанный по технологии 960Н на новом процессоре от компании Texas Instruments на платформе NETRA;
- 2013 г. Компания HIKVISION приступила к серийному производству видеокамер на платформе собственной разработки PICADIS с повышенным разрешением до 720 Твл.

Комплексное решение

Сегодня компания HIKVISION предлагает законченные системы, способные в полной мере реализовать технологию 960Н. Данная технология позволяет формировать и записывать видеоизображение с разрешением до 720 Твл – это самое высокое качество для аналоговой системы на сегодняшний день. Также технология 960Н обеспечивает 30% увеличение разрешения по сравнению с разрешением D1. Чем больше разрешение, тем выше четкость и распознаваемость видеоизображения.

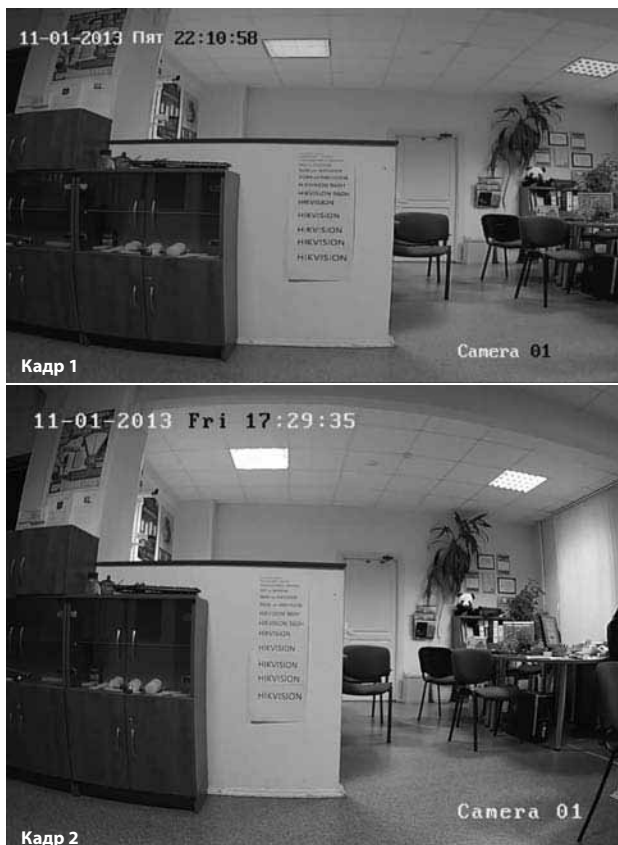
Самое главное в системах, использующих технологию 960Н, – это необходимость совместного использования камер 960Н и DVR 960Н для полной реализации качества высокого разрешения. В старых системах, работающих с видеорегистратором разрешения D1, даже если вы имеете аналоговые камеры 650-700 ТВЛ, вы можете наблюдать и записывать изображение только с разрешением D1, которое соответствует четкости до 520 Твл.

С новым DVR 960Н от Hikvision можно не только реально наблюдать высокое разрешение камер до 720 Твл, но и получить высокое качество записи с полным разрешением до 720 Твл.

Сравнение стоимости систем

Запись (Кадр 1) выполнена IP-камерой с разрешением 1.3 Мп. Ориентировочная стоимость камеры на рынке Беларуси 2 300 000 руб., полная стоимость системы из четырех камер и устройства записи с диском 1Тб – ориентировочно составит 15 000 000 руб. (без монитора).

Запись (Кадр 2) выполнена камерой PICADIS от Hikvision (технология 960Н). Ориентировочная стоимость камеры 700 000 руб., полная стоимость системы из четырех камер и устройства записи с диском 1Тб – ориентировочно 5 000 000 руб. (без монитора).



Ключевые моменты технологии 960Н:

1. Увеличение количества пикселей почти на 30%, в результате чего значительно улучшается качество изображения, как в записи, так и в наблюдении;
2. Легкая замена существующего оборудования аналоговых систем;
3. Системы 960Н не требуют увеличения затрат на оборудование.

Технология 960Н – новый стандарт в записи цифровых видеоданных

На текущий момент существует множество работающих систем видеонаблюдения с камерами, формирующими цветное изображение с разрешением до 700 Твл, однако запись ведется устаревшими цифровыми видеорегистраторами, которые воспроизводят изображение с максимальным разрешением до 520 Твл.

Преимущество технологии 960Н в том, что

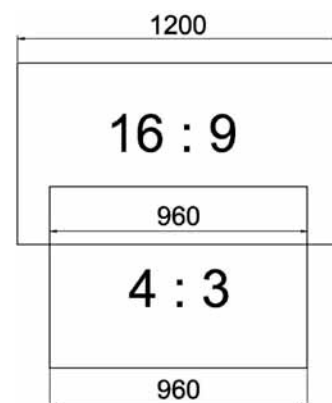


Рис. 1



Бюджетные IP регистраторы с поддержкой ONVIF



Новая серия IP регистраторов DS- 7600 NI-SE

Полный функционал – запись, наблюдение, просмотр архивов, мониторинг и др.
Запись с разрешением до 5 Мп
HDMI видеовыход с разрешением до 1920x1080p
Инновационная платформа от Texas Instruments - NETRA
Совместимость с видекамерами сторонних производителей по стандарту ONVIF
Plug-and-Play – включил и работай
Поддержка удаленного просмотра Android и iOS
Управление квотами дискового пространства



Второе рождение аналогового видеонаблюдения



Видеорегистраторы стандарта 960H серий DS-7200HWI-SH, DS-7300HWI-SH

- Увеличение четкости записи на 40%
- Сверхвысокое разрешение WD1 (960H)
- Запись в реальном времени
- Оптимизирован для работы с видеокамерами 720твл
- Поддержка протокола SNMP
- Поддержка Internet Explorer, Firefox, Google Chrome, Safari, и др.
- Поддержка бесплатного DNS сервиса от Hikvision

просто заменив старый видеорегистратор на модель с технологией 960Н, пользователь сразу же получает более высокое разрешение записи с качеством до 720 Твл. Соответственно, запись можно будет просматривать на мониторе с высоким разрешением и увидеть разницу в четкости изображения. По мнению специалистов, в ближайшее время такой способ модернизации существующей аналоговой системы станет крайне популярным среди клиентов, у которых нет физической необходимости переходить на IP-видео или инвестировать средства в HD-камеры последнего поколения.

Данная схема (Рис. 1) наглядно демонстрирует идентичность горизонтального разрешения сопоставляемых зон кадров изображений 1.3Мп (16:9) и 960Н (4:3).

Модельный ряд видеорегистраторов 960Н Hikvision

В 2013 г. компания Hikvision начала серийное производство полного спектра видеорегистраторов, спроектированных по технологии 960Н.

Базовая серия DS-7200HVI-SV – несмотря на средние показатели по скорости записи, данная серия по качеству изображения абсолютно не уступает моделям профессиональных серий.



Базовая серия DS-7200HWI-SH – серия видеорегистраторов реального времени со скоростью записи 25 к/с на каждый канал при качестве записи 960Н (WD1).



Серия стандарт DS-73XXHWI-SH – видеорегистраторы, способные удовлетворить самые серьезные требования и задачи, построены на платформе NETRA от Texas Instruments.



Профессиональная серия DS-81XXHWI-SH – самая мощная серия, емкость архива до 32Тб, исходящий поток встроенного IP-сервера до 160 мегабит.



Камеры 720 Твл

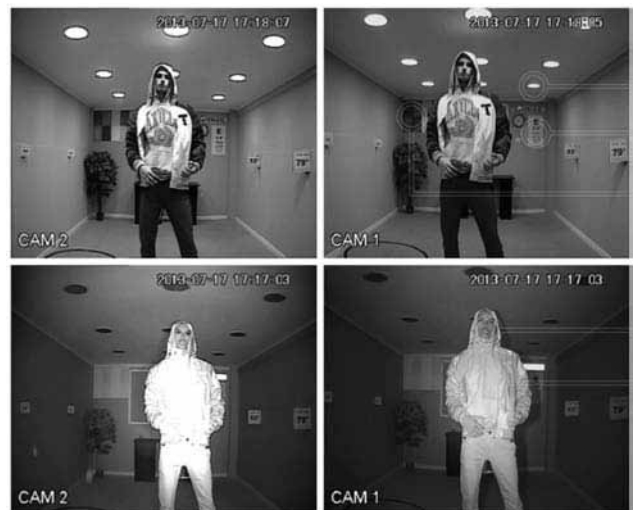
Компания Hikvision с гордостью объявила о начале производства новой серии 720Твл аналоговых камер для реализации всех технических возможностей видеорегистраторов Hikvision 960Н.

Серия построена по технической концепции PICADIS – «передовая цифровая обработка изображений» и предназначена для расширения возможностей аналогового наблюдения, позволяя пользователям достичь самого высокого уровня качества изображения в мире аналоговых систем. Международный директор по маркетингу компании Hikvision Кин Яо сказал: «Hikvision стремится быть в авангарде отрасли видеонаблюдения, и преданность нашей компании собственным научным разработкам является доказательством этого идеала. Серии камер 720Твл PICADIS поднимут качество изображения на новую высоту».

Таблица сравнительных характеристик регистраторов с технологией 960Н

Модель	Кол-во каналов видео	Скорость записи в формате WD1 (960Н)	Максимальная емкость архива	Кол-во подключаемых жестких дисков
Базовая серия				
DS-7204HVI-SV	4	12 к/с	4 Тб	1
DS-7208HVI-SV	8	8 к/с	4 Тб	1
DS-7208HVI-SV	16	6.5 к/с	4 Тб	1
Базовая серия реал тайм				
DS-7204HWI-SH	4	25 к/с	4 Тб	2
DS-7208HWI-SH	8	25 к/с	8 Тб	2
DS-7216HWI-SH	16	25 к/с	8 Тб	2
Серия стандарт				
DS-7304HWI-SH	4	25 к/с	16 Тб	4
DS-7308HWI-SH	8	25 к/с	16 Тб	4
DS-7316HWI-SH	16	25 к/с	16 Тб	4
DS-7324HWI-SH	24	25 к/с	16 Тб	4
DS-7332HWI-SH	32	25 к/с	16 Тб	4
Профессиональная серия				
DS-8108HWI-SH	8	25 к/с	32 Тб	8
DS-8116HWI-SH	16	25 к/с	32 Тб	8
DS-8124HWI-SH	24	25 к/с	32 Тб	8
DS-8132HWI-SH	35	25 к/с	32 Тб	8

для аналоговых решений в видеонаблюдении и позволят идти в ногу со временем к новым инновациям».

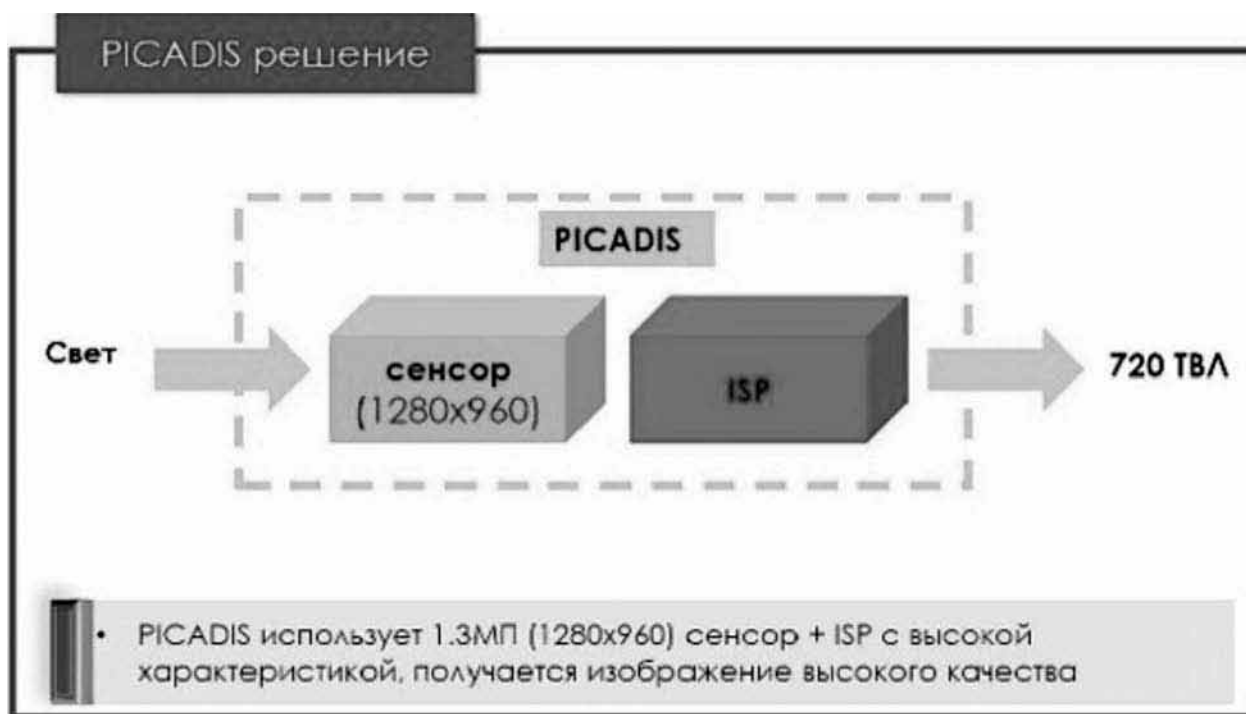


Новая серия PICADIS аналоговых камер 720Твл состоит (Рис. 1):

- из купольных камер, DS- 2CE55C2P;
- из купольных камер с ИК, DS- 2CE55C2P IR;
- из цилиндрических камер с ИК, DS- 2CE15C2P.



Рис. 1. Новая серия аналоговых камер



Каждая модель обладает сверхвысоким разрешением 720Твл благодаря использованию 1,3-мегапиксельной (1280x960) матрицы. Эти камеры имеют вдвое больше эффективных пикселей, чем у предыдущих камер 960Н (976x582), что помогает намного лучше захватить детальные изображения с целью идентификации.

Сформированные изображения подвергаются дальнейшей оптимизации – HDR (High Dynamic Range), которая помогает зафиксировать самые критические подробности, в том числе такие основные моменты, как затененные области при смешанном освещении – в любой момент времени и без ущерба для качества изображения или точности цветопередачи. Также имеется алгоритм адаптивного локального отображения цветовых оттенков (ALTM), чтобы максимизировать производительность визуализации.

Отличные показатели минимальной освещенности – еще одна достопримечательность камер 720Твл PICADIS. Скорость затвора этих камер может достигать до 40 мс при самом низком освещении. Это в два раза лучше по сравнению с обычными аналоговыми камерами. Все эти усовершенствования, в конечном счете, приводят к значительному улучшению светочувствительности камер. Если учесть цифровое шумоподавление, то можно с уверенностью заявить, что пользователи имеют возможность лучше различать формы, размеры, и, конечно, движение при помощи этих камер.

Возможность работы в полной темноте – купольные камеры DS-2CE55C2P, ИК купольные камеры DS-2CE55C2P-IRP и DS-2CE15C2P-ИК цилиндрические камеры поддерживают также функцию «интеллектуальное ИК» для решения таких проблем как частичные засветки кадра, обеспечивая четкое и резкое изображение. Кроме того, аналоговая серия камер 720TVL PICADIS эффективно работает в широком диапазоне погодных условий, в том числе при температуре от -40°C до 60°C (-40 °F до 140 °F), а также уровне влажности вплоть до 90%. Модели для наружного наблюдения DS-2CE55C2P IR и DS-2CE15C2P-IR поддерживают класс защиты корпуса IP66.

Эти функции камер формируют непревзойденное качество изображения. Аналоговые серии 720TVL от Hikvision могут удовлетворить потребности в области безопасности



практически любого бизнеса и организации, в том числе гостиниц, офисных зданий, промышленных парков и других объектов, где применимы подобные сценарии. Кроме того, Hikvision также производит DS-2CE16C2P-IT3/IT5 ИК-камеры и DS-2CE56C2P – IT3 ИК купольные камеры. Обе модели Hikvision оснащены самой передовой инфракрасной технологией Exir и оснащены лучшими в своем классе осветителями для работы в полной темноте, как в помещении, так и на улице.

Все преимущества технологии 960Н реализованы в сочетании с отличной линейкой DVR продуктов Hikvision и камер 720TVL PICADIS. Сопряжение этих продуктов создает по-настоящему самые яркие и точные изображения в формате 960Н в мире!

АВАНТ-ТЕХНО

системы безопасности

Авант-Техно, ОДО
220004, г. Минск, ул. Короля, 45-16в
Тел./факс: (017) 200-01-09, 226-43-52, 200-08-22, 200-44-83
E-mail: info@avant.by
Сайт: www.avant.by

УНП: 190423783



Лучше гор только горы!
Или альпийские технологии на отечественном рынке пожарных систем

Опыт применения оборудования системы «ИНТЕГРАЛ» (практика применения в Республике Беларусь)

STRABAG

КЛАСКОМ

SCHRACK
SECONET

Продолжаем разговор, начатый в предыдущем номере журнала (ТБ, №4, 2013). Сегодня мы хотим рассказать Вам о нашем опыте применения оборудования системы «ИНТЕГРАЛ» на вновь строящемся объекте КПУП «Брестский мусороперерабатывающий завод».

Проект реализован знаменитым австрийским концерном «STRABAG» в 2009-2011 году. Согласно Указу Президента Республики Беларусь проект был объявлен инвестиционным, что позволило концерну «STRABAG» применять на территории Республики Беларусь европейские технологии и оборудование без наличия отечественного сертификата.

Особенности проекта

Компания «КЛАСКОМ» (давний партнер компании производителя «SCHRACK Seconet, AG») осуществила инсталляцию и оказала помощь концерну «STRABAG Umweltanlagen GmbH» в реализации типового для нашей страны проекта на базе оборудования системы пожарной безопасности «ИНТЕГРАЛ». К моменту внедрения уже было принято намерение сертифицировать данную систему в нашей стране, что только ускорило принятие нашего решения участвовать в данном проекте. Заказчик проекта –

Брестский облисполком. Генпроектировщик и Генподрядчик – концерн «STRABAG Umweltanlagen GmbH». Эксплуатирующая организация – Коммунальное унитарное многопрофильное предприятие КУМПП «Брестское городское жилищно-коммунальное хозяйство» в г. Бресте.

Цель реализации проекта – Создать на 2-ой очереди строительства объекта Автоматизированную систему пожарной сигнализации для раннего обнаружения пожара в зоне приема, сортировки и переработки твердых бытовых отходов мусора.

Проект обладал рядом особенностей:

1. Проект – инвестиционный в Республике Беларусь;
2. Генподрядчик – иностранное предприятие с льготами по налогообложению и широкими полномочиями по Указу Президента Республики Беларусь;
3. Предусмотренные проектом уникальные пожарные технологии являются для Беларуси новыми, аналоги и разрешения МЧС РБ на их применение в стране отсутствовали;
4. Работы по проектированию, монтажу, наладке и техническому обслуживанию пожарного оборудования должны выполняться резидентами Беларуси, имеющими специальную лицензию МЧС РБ. Согласно условиям лицензионного соглашения недопустимо производство работ с применением пожарного оборудования, не имеющего разрешения МЧС РБ. Поэтому реализация проекта происходила параллельно с организацией процедур по легализации применяемого уникального пожарного оборудования в МЧС РБ;
5. Условия применения средств обнаружения факторов пожара – боль-

шой уровень запыленности производственных помещений;

6. Монтаж воздушного трубопровода аспирационных извещателей (газоанализаторов) должен осуществляться внутри технологического оборудования и на высотах более 9 м.

Состав, структура оборудования

В составе проекта применялись (до сего никому не известные) аспирационные извещатели, в использовании которых настаивал концерн «STRABAG» для защиты своего дорогостоящего технологического оборудования. У них уже имелся успешный опыт применения таких пожарных систем в условиях запыленных производственных помещений. В таких условиях, как правило, согласно практики нашего рынка, вообще не применяются никакие дымовые извещатели из-за высоких рисков ложного срабатывания на мелкодисперсные частицы пыли (особенно строительной).

Система аспирационных извещателей, совместно с их «ноу-хау» – системой автоматической «самоочистки», позволяет в запыленных условиях производственных помещений обнаруживать реальные факторы пожара, не только по объему защищаемых помещений, но и внутри технологического оборудования на ранней стадии его возгорания. Такой метод защиты позволяет оперативно остановить работу механизмов технологической линии, локализовать область возгорания при помощи противопожарных заслонок и применить локальное пожаротушение. Разветвленная топология тонких пластиковых трубок аспирационной системы обнаружения пожара позволяет производить забор воздушной смеси непосредственно



из самой пожароопасной области функционирования дорогостоящего технологического оборудования для последующего анализа высокочувствительным газоанализатором. Во взаимодействии с приемно-контрольным оборудованием пожарной системы сигнализации «Интеграл IP» происходит не только оперативное оповещение дежурного персонала, но и локализация пожароопасной зоны с возможностью применения автоматизированных средств локального пожаротушения.

Сроки, объем работ

Проект был реализован в июне 2011 года компанией НПО «КЛАССКОМ», совместно с концерном «STRABAG», при непосредственном содействии МЧС РБ в нереально короткие сроки – менее 1 месяца – за 20 календарных дней с момента подписания договора подряда на выполнение работ.

Для быстрой реализации объема работ была проведена большая подготовительная работа специалистов нашего предприятия, которые совместно с представителями концерна и МЧС РБ разработали программу испытаний, программу управления средствами автоматики, разработали и изготовили нестандартное оборудование и необходимую техническую документацию для технологической «самоочистки» аспирационной системы обнаружения пожара. На все подготовительные работы ушло около года.



Рис. 1. Изображение мнемонического табло для ситуационного контроля за средствами противопожарной защиты завода

В ходе реализации проекта компания «КЛАССКОМ» выполнила следующие виды работ с использованием оборудования системы «ИНТЕГРАЛ IP»:

1. Разработана проектно-сметная документация в двух разделах: установка автоматизированной пожарной сигнализации и системы продувки воздушных трубопроводов аспирационных извещателей;
2. Поставлен специализированный комплект технических средств пожарной сигнализации фирмы SCHRACK Seconet AG (Австрия);
3. Произведена комплектация проекта необходимым сырьем, материалами и покупными комплектующими изделиями;
4. Разработано и изготовлено нестандартное заказное оборудование:
 - Шкаф пожарной автоматики ARC – 2 шт.;
 - Шкаф аспирационный – 12 шт.;
 - Шкаф управления системой продувки – 12 шт.;
 - Щит информационный (мнемо-табло) – 1 шт.;
5. Произведен монтаж воздушного трубопровода на высоте 9 метров и внутри технологического оборудования;
6. Произведен монтаж заказного и специализированного оборудования;
7. Произведены пуско-наладочные работы;
8. Произведены межведомственные испытания с целью проверки выполнения требований ТНПА с участием представителей МЧС РБ с целью получения заключения на право применения зарубежных технологий на отечественных промышленных объектах;
9. Обеспечен ввод в эксплуатацию

завода в декларативные сроки строительства 21 июня 2011 года по Указу Президента РБ.

Еще одной не менее интересной особенностью реализации данного проекта явилось применение панорамного светодинамического мнемо-табло (Рис. 1), для быстрой ситуационной оценки состояния всех средств пожарной безопасности на территории всего завода.

Каналы связи

Обмен данными производится по резервированным цифровым линиям связи, приборы могут работать независимо от места установки и в любых комбинациях. По соображениям надежности предусмотрено резервированное исполнение, как линии передачи данных, так и питающих линий, причем они должны прокладываться отдельно.

Для реализации ввода/вывода информации предусмотрен специальный универсальный модуль ВЗ-UIO (Рис. 3) для запуска табло общего плана и параллельного индикаторного табло. Узел используется в качестве выносного модуля ввода/вывода с целью опроса контактов с нулевым потенциалом (спринклерные установки), а также для управления неконтролируемыми сиренами, лампами, реле и т.д. В зависимости от обстоятельств, узел встраивается или непосредственно в соответствующее табло или в ответительные коробки.

Обеспечена постоянная интеллектуальная связь между периферийными элементами и подсистемами с высочайшей степенью надежности (код Хэмминга, дистанция 4). Благодаря этому отфильтровываются ложные тревоги, вызванные такими электро-

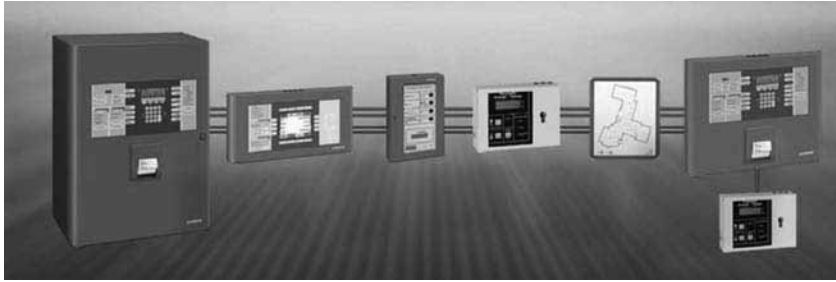


Рис. 2. Пример организации шины для обмена данными между устройствами индикации системы «ИНТЕГРАЛ IP»

магнитными помехами, как направленная радиопередача, перенапряжение, паразитные импульсы и т.п.

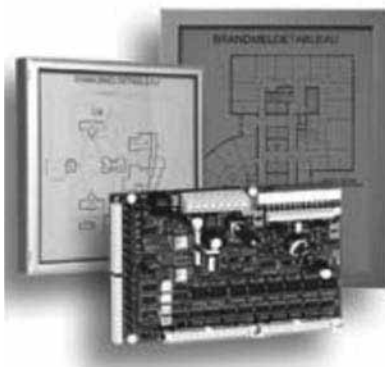
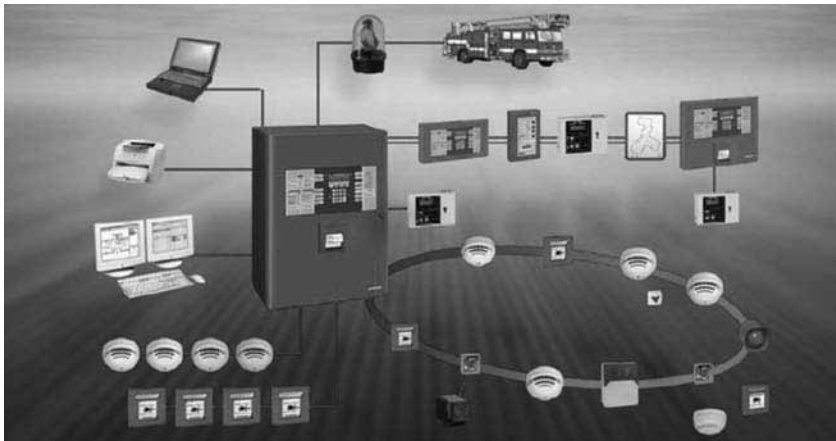


Рис. 3. Универсальный, выносной модуль ввода-вывода ВЗ-UIO

Общая структурная схема реализованного проекта



В состав создаваемой системы пожарной безопасности могут входить:

- Станции пожарной сигнализации и управления пожаротушением;
- Универсальные мультисенсорные извещатели: работа в режиме дымового, теплового или комбинированного, два уровня предтревоги, четыре уровня чувствительности дымового сенсора, девять режимов теплового сенсора, просмотр уровня загрязнения, времени работы, теку-

щих уровней задымления и температуры в помещении;

- Модули ввода/вывода для управления противопожарным оборудованием;
- Ручные извещатели для установки внутри помещений и на улице;
- Извещатели специального назначения – для взрывоопасных зон;
- Линейные и аспираторные извещатели;
- Компьютерная система мониторинга и управления, несколько рабочих мест, подключаемых по стандартной сети.

Концепция системы

В основе концепции созданной системы пожарной безопасности «ИНТЕГРАЛ» – ДОСТУПНОСТЬ для разработчиков, ЭКСПЛУАТАЦИОННАЯ НАДЕЖНОСТЬ и НЕМЕЦКОЕ КАЧЕСТВО!

магнитных помех, однако в каждое новое поколение непременно вносятся улучшения, расширяющие технические возможности и повышающие эксплуатационную надежность оборудования.

В ЦСПС Интеграл реализована тщательно разработанная интегрированная концепция защиты от перенапряжения, которая распространяется на все периферийные устройства, включая систему сетевого питания, и соответствует требованиям стандартов EN50130-4 (электромагнитная совместимость) и EN50082-2 (помехоустойчивость в промышленной зоне).

Концепция отказов в европейском стандарте EN 54-2

Евростандарт EN 54 / часть 2 (п. 13.7) допускает «отказ не более 512 извещателей и соответствующих функций» в случае появления помехи в системе.

Однако эта модель отказов, рассчитанная на 512 извещателей, не признается многими экспертами, поскольку 80% действующих систем пожарной сигнализации включают в себя менее 512 извещателей, и простая ошибка в системе приводит к ее полному отказу, включая выходы управления. Кроме того, выходят из строя системы оповещения и информации о виде и причинах повреждения оборудования.

В связи с этим, компания SCHRACK Seconet AG (начиная с конца 80-х годов) перешла к производству систем пожарной сигнализации, в которых реализуется принцип 100% горячего резервирования.

Резервирование предусматривает наличие в системе дополнительных технических ресурсов, которые в штатном режиме не используются, а вступают в работу в случае выхода из строя основных компонентов.

Термин «резервирование» (от лат. redundare – иметься в избытке) обычно характеризует наличие нескольких объектов, одинаковых по своему назначению, содержанию и сути.

Каждый модуль, установленный в станцию «ИНТЕГРАЛ», имеет на плате два контроллера: основной (сторона «А») и резервный (сторона «В»).

При нормальном функционировании системы обработка данных происходит на стороне «А», сторона «В» находится в режиме горячего резерва.

В случае возникновения неисправности какого-либо контроллера стороны «А», в работу вступает сторона «В».

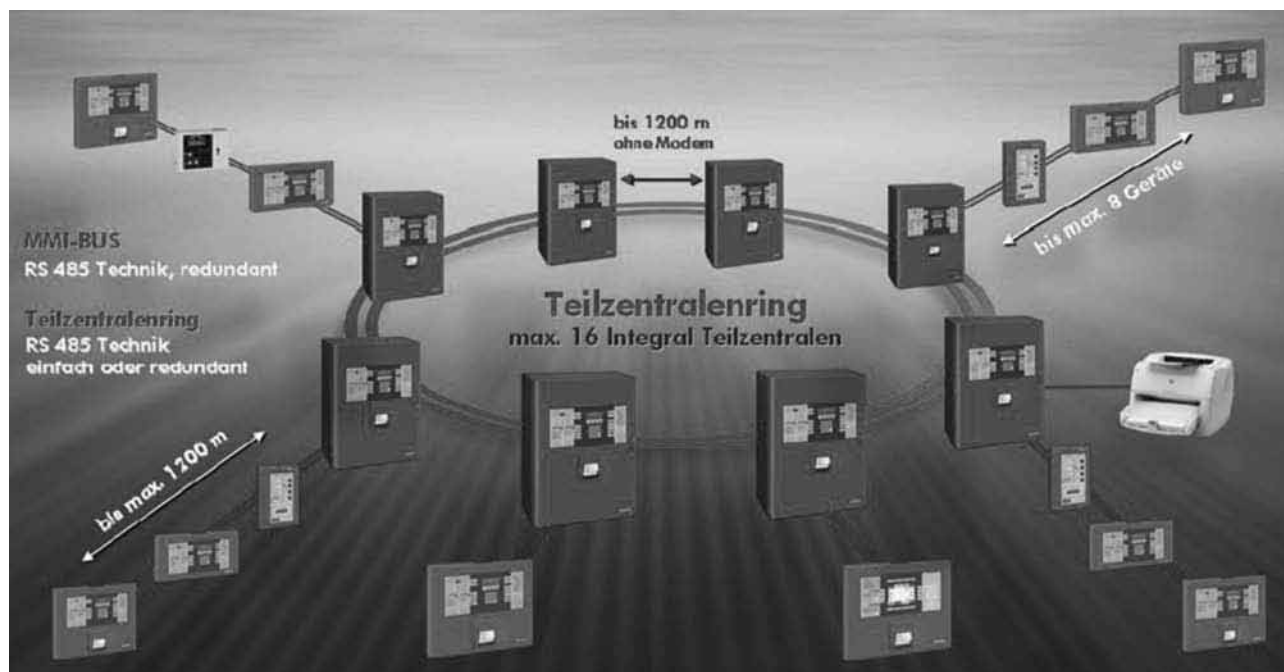


Рис. 4. Кольцевая топология построения системы пожарной безопасности на базе системы «ИНТЕГРАЛ IP»

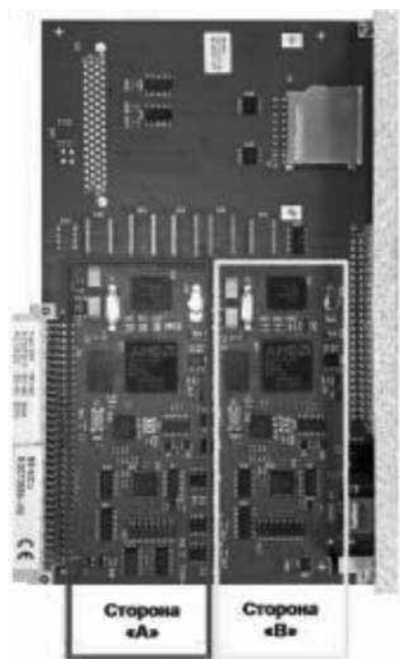


Рис. 5. Контроллер

Переключение на резервную сторону осуществляется автоматически, нет необходимости перезагружать станцию, переставлять платы и т.п.

Без каких-либо ограничений сохраняются все функции системы: обмен данными с периферийным оборудованием, выдача информации на дисплей, управление противопожарными системами и т.п.

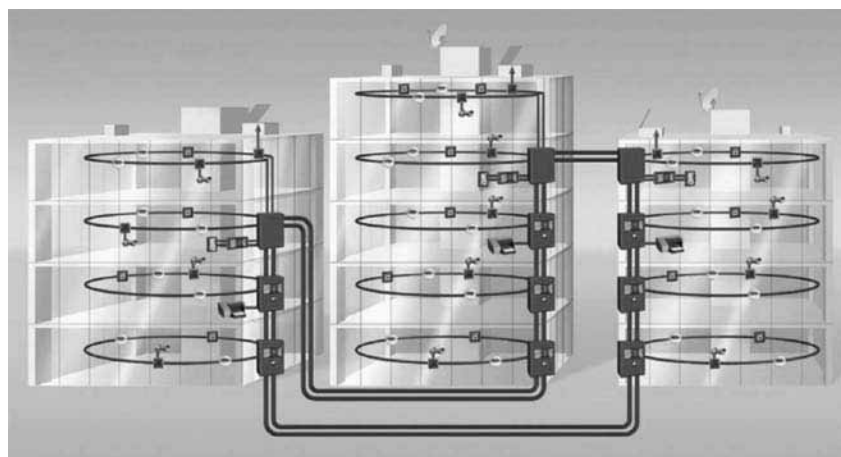
Кроме того, дублируются линии передачи данных на внешние пульта управления, а также провода, соединяющие между собой функциональные модули и приемно-контрольное

оборудование в кольце между собой, что позволяет сохранять целостность системы в случае обрыва участка линии или появления помехи.

Дополнительное образование кольцевых шлейфов гарантирует в итоге 100% работоспособность системы даже при тройной ошибке.

ким ассортиментом функциональных устройств, включая и аспирационные и взрывозащищенные извещатели.

НПООО «КЛАССКОМ» является авторизованным представителем системы INTEGRAL IP в Республике Беларусь. Специалисты компании оказывают услуги по обучению и консультиро-



В завершение начатого разговора, хотим сообщить, что в настоящий момент реализованный в Бресте, проект на мусороперерабатывающем заводе успешно эксплуатируется. В ходе эксплуатации системы на сегодняшний день неоднократно были обнаружены очаги возгорания в привозимом для переработки мусоре аспирационными средствами сигнализации.

Начиная с 12 апреля 2013 года Адресная система пожарной сигнализации «Интеграл IP» сертифицирована в Республике Беларусь с широ-

ванию специалистов в области проектирования, монтажа и обслуживания оборудования системы INTEGRAL IP.

КЛАССКОМ

Приглашаем к сотрудничеству всех заинтересованных специалистов
НПООО «КЛАССКОМ»

Тел./факс: +375 29 501-55-02

E-mail: integral-ip@tut.by

УНП: 190268725

Обеспечение комплексной информационной безопасности АСУ ТП: опыт российских компаний



Тимошенко Андрей
Борисович

Справка ТБ

Тимошенко Андрей Борисович, окончил факультет Кибернетики НИЯУ МИФИ и Финансово-юридический факультет МФЮА. В настоящий момент является начальником отдела консалтинга департамента консалтинга и аудита компании «Информзащита». Г-н Тимошенко специализируется на приведении к соответствию требованиям 152-ФЗ «О персональных данных», стандарту ISO 27001, а также на оценке бизнес-рисков и рисков ИБ, внедрению режима коммерческой тайны, противодействию мошенничеству и обеспечении безопасности АСУ ТП. В личном портфолио более 30 успешных проектов в области ИБ в компаниях различных отраслей экономики. В свободное время предпочитает заниматься спортом (йога, сноуборд) и путешествовать.

Что нужно для того, чтобы построить эффективную защиту АСУ ТП?

Этим вопросом задается каждый специалист, ответственный за АСУ ТП и ее информационную безопасность. Отвечая на него, важно понимать, что внедрение системы защиты АСУ ТП при неправильном подходе может стоить очень дорого: и на этапе внедрения самой защиты, и при возникновении проблем на этапе эксплуатации АСУ ТП.

Для того чтобы построить эффективную защиту АСУ ТП нужно, прежде всего, адекватно оценивать последствия, связанные с выходом АСУ

ТП из строя. К примеру, остановка технологического процесса на АЗС просто заставит автомобили заправляться на другой АЗС, и компания понесет финансовые потери. В то время как остановка технологических процессов на НПЗ может привести с существенным убытком не только для предприятия, но и для экономики региона или даже страны.

Помимо оценки последствий, необходимо оценивать вероятность инцидента, связанного с безопасностью АСУ ТП. Этот процесс, безусловно, сложнее, и в некоторых случаях может привести к пониманию, что снижение вероятности до нуля возможно только при полном отказе от использования технологического процесса или технологии. К примеру, к такому выводу пришли власти Германии, приняв программу отказа от использования АЭС, чтобы абсолютно исключить риск аварий на атомных электростанциях.

Другими словами, первым шагом в процессе построения эффективной защиты АСУ ТП является категоризация объектов с точки зрения их опасности и критичности.

Примером такого подхода в РФ является отнесение объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации. Вместе с тем критерии отнесения объектов к различным категориям опасности и установление требований к системам безопасности этих объектов вскоре планируется закрепить на законодательном уровне. Такие изменения предусматривает разрабатываемый в настоящее время ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Кто реально является нарушителем безопасности АСУ ТП: внутренний пользователь или внешнее лицо?

На следующем этапе подготовки к защите АСУ ТП следует определить источники угроз безопасности. Су-

ществует мнение, что основной угрозой всех информационных систем, в том числе и SCADA-систем, являются хакеры. Они, подключаясь удаленно через интернет, взламывают системы и получают над ними контроль. Такое действительно происходит, о чем свидетельствуют периодические публикации в прессе.

Но, по экспертным оценкам, на текущий момент внешние злоумышленники не являются основными источниками угроз АСУ ТП в РФ. Ими являются внутренние пользователи АСУ ТП, которые допускают ошибки при администрировании SCADA-систем, используют слабые пароли или подключают к терминалам SCADA съемные носители.

В качестве хорошей иллюстрации можно привести следующий пример. Администратор системы SCADA решил произвести настройку компонентов системы удаленно. Он подключился по протоколу RDP, и во время подключения на его компьютере произошло зависание операционной системы Windows. Попробовав реанимировать свой компьютер, он стал нажимать на разные кнопки. В конечном счете, система «отвисла», но хаотичное нажатие кнопок привело к выбросу в атмосферу большого количества метана. А поскольку факельное хозяйство было построено неправильно, то метан не сгорел, а в чистом виде попал в атмосферу.

Таких примеров много. В результате преднамеренных и непреднамеренных действий пользователей происходит большая часть инцидентов безопасности АСУ ТП. Причины могут быть разными: несоблюдение правил информационной безопасности, ошибки при администрировании АСУ ТП, низкая осведомленность пользователей АСУ ТП в вопросах ИБ и т.д.

Поскольку построение комплексной системы защиты должно учитывать все угрозы, а не только внутренние, то важно правильно оценивать риски и расставлять приоритеты.

На что ориентироваться при

обеспечении безопасности АСУ ТП?

Наиболее известные и практически значимые подходы к обеспечению безопасности АСУ ТП изложены в нормативных документах в области обеспечения ИБ АСУ ТП, разработанных основными международными организациями:

- ISA (Комитет ISA99), Международное общество автоматизации (Комитет по разработке стандартов безопасности АСУ ТП);
- NIST, Национальный институт стандартов и технологий США;
- IEC, Международная электротехническая комиссия, МЭК.

Среди всех стандартов, разработанных этими организациями, выделяют следующие основные документы, посвященные безопасности АСУ ТП:

- 13 документов серии ISA/IEC 62443;
- NIST SP800-82 «Guide to Industrial Control Systems (ICS) Security», June 2011.

В РФ нормотворчество в этой области только набирает свои обороты. Но это не мешает российским компаниям разрабатывать свои внутренние стандарты, которые в первую очередь учитывают международный опыт и лучшие практики по ИБ АСУ ТП.

План защиты АСУ ТП: с чего начать, какие этапы и работы нужно выполнить?

После того, как проведена категоризация объектов АСУ ТП по степени их опасности и критичности и решено, для каких объектов необходимо обеспечивать безопасность в первую очередь, можно приступать к разработке плана защиты АСУ ТП. Первым делом необходимо провести обследование и анализ текущего состояния защищенности АСУ ТП. В ходе обследования необходимо выявить критичные объекты и установить, защиту которых необходимо обеспечить, определить и описать технологические процессы, выявить архитектуру АСУ ТП, все ее ключевые элементы. Далее необходимо определить используемые меры и способы защиты, оценить их эффективность.

После составления картины текущей защищенности АСУ ТП необходимо определить требования к системе защиты с учетом структурно-функциональных характеристик АСУ ТП, информационных технологий,

особенностей функционирования и угроз безопасности АСУ ТП.

Основным источником требований по ИБ АСУ ТП в условиях слабого законодательного регулирования является модель угроз безопасности АСУ ТП. Другим – выбранные международные стандарты по ИБ АСУ ТП.

Эти требования формулируются в виде технического задания, на основе которого осуществляется проектирование системы защиты АСУ ТП. Технический проект на создание системы защиты обязательно согласовывается со всеми лицами, ответственными за АСУ ТП, и ее разработчиками. После того, как согласованный проект готов, следует провести опытную эксплуатацию необходимых к внедрению средств защиты. Тестирование осуществляется в заранее подготовленной тестовой среде, которая должна повторять основные элементы существующей системы.

Важно учитывать, что тестирование может являться одной из основных проблем, если на объекте используется несколько SCADA-систем. Создание нескольких тестовых сред может быть очень затратным.

После того, как все средства защиты протестированы и установлены, а все организационные мероприятия регламентированы и реализованы, наступает период промышленной эксплуатации системы защиты и ее совершенствования.

Процесс модернизации и улучшения системы защиты должен быть непрерывным и состоять из четырех основных стадий, которые циклически следуют одна за другой. Это планирование, реализация, контроль и оптимизация. Эти процессы должны покрывать все элементы системы защиты, в том числе методы и способы защиты АСУ ТП.

Как защищать АСУ ТП: методы и способы защиты?

Защита элементов и сети АСУ ТП имеет много общего с защитой корпоративных систем и сетей. Разница состоит в том, что технологическая информация не является конфиденциальной, а технологический процесс должен быть непрерывным. В связи с этим появляются ключевые особенности:

- необходимость ограничения взаимодействия сети АСУ ТП с корпоративной сетью;
- обязательный контроль и ограничение подключений съемных носителей к элементам АСУ ТП;

- возможность установки обновлений только в жестко отведенные интервалы технологических пауз;

- необходимость тестирования обновлений перед установкой, необходимость поиска компенсирующих мер в случае несовместимости средств защиты со SCADA-системами;

- необходимость выявления уязвимостей и недокументированных возможностей в АСУ ТП.

Для того, чтобы учесть эти особенности, рекомендуется использовать межсетевое экранирование на границе сети АСУ ТП или технологию дата-диодов, когда информация физически может передаваться только из сети АСУ ТП в корпоративную сеть. Другими эффективными мерами являются: блокирование внешних портов на терминалах пользователей SCADA-систем, разработка плана и регламента проверки обновлений и их тестирование в заранее подготовленной тестовой среде, анализ уязвимостей элементов SCADA-системы также в тестовой среде. Физическое разделение системных блоков и интерфейсов ввода/вывода (монитор, мышь, клавиатура) для ограничения подключения внешних устройств, когда системные блоки находятся в отдельном помещении, является хорошим примером компенсирующих мер.

Опыт российских компаний по защите АСУ ТП: как делают другие

Одной из лучших практик, применяемых российскими компаниями, является типизация и стандартизация. Типизация означает выделение типовых объектов АСУ ТП для того, чтобы выдвигать индивидуальные требования по защите к различным объектам. Стандартизация – не только учет отраслевой специфики, но и разработку стандартов безопасности внутри группы компаний. Это оправдано, когда группа компаний реализует полный цикл производства (например, начиная с добычи полезных ископаемых и заканчивая розничной реализацией топлива или электроэнергии).

Еще одной хорошей практикой является обращение за помощью в компании-интеграторы, если организация не имеет своих достаточно квалифицированных специалистов по ИБ. Такие компании за последнее время накопили богатый опыт в обеспечении безопасности АСУ ТП и знают типовые проблемы, с которыми сталкиваются почти все технологические предприятия.

Справка ТБ:

В октябре 2013 года вирус Stuxnet заразил российскую АЭС. Об этом рассказал эксперт в области компьютерной безопасности Евгений Касперский, выступая на мероприятии Канберре. Компьютерный червь Stuxnet, предположительно использовавшийся для атак на иранские ядерные объекты, проник и на российскую АЭС. Внутренняя сеть пострадавшей станции не имела выхода в интернет, однако вредоносное ПО попало на ее компьютеры с зараженной USB-флеш-карты.

Stuxnet принадлежит к семье вирусов, используемых для шпионажа и диверсий против Ирана. В нее также входят программы Duqu, Flame, Red October и Gauss. Касперский также объяснил принцип работы вирусной программы. По его словам, Stuxnet отдает команды автоматизированной системе управления центрифугами, в результате чего они выходят из-под контроля и повреждают оборудование. В это же время программа создает ложный набор данных, вводя в заблуждение обслуживающий персонал.

Касперский не первый раз предупреждает об опасностях кибервойн. В июне 2012 года на конференции в Израиле он говорил о том, что вирус Flame – это «только начало», «боюсь, это станет концом мира, как мы его знали».

Типовые проблемы защиты АСУ ТП и их решения

Многие компании уже научились решать такие типовые задачи, как установка межсетевого экрана на границе сети АСУ ТП, ограничение и контроль физического доступа, блокировка подключения внешних устройств и т.д. В то же время существуют некоторые нестандартные задачи, над которыми до сих пор ломают голову многие «безопасники».

К таким проблемам можно отнести выбор совместимых с АСУ ТП средств защиты, конфликт интересов сотрудников, отвечающих за ИБ АСУ ТП, и сотрудников, отвечающих за саму АСУ ТП, обновление программного обеспечения (ПО) и взаимодействие с разработчиками АСУ ТП.

Зачастую выбор и установка совместимых с АСУ ТП средств защиты является непростой задачей. Это связано с тем, что производитель АСУ ТП не дает никаких гарантий того, что АСУ ТП будет правильно работать. Доходит до абсурда, когда официальные рекомендации производителя на установку конкретного антивируса не дают никаких гарантий бесперебойной работы АСУ ТП с этим антивирусом.

Конфликт интересов заключается в том, что специалисты по ИБ не осознают до конца специфику АСУ ТП, которая заключается в обеспечении непрерывности технологических процессов. Сотрудники, отвечающие за АСУ ТП, обычно не понимают, какие угрозы и уязвимости есть в их системе, и не принимают в расчет всю важность и необходимость обеспечения безопасности АСУ ТП. Они также часто ошибаются, думая, что их система уже изначально защищена. Наша компания столкнулась с похожей проблемой несколько лет назад. Она была решена, когда мы взяли в свой штат квалифицированного специалиста по АСУ ТП, который помог нам разобраться

в специфике АСУ ТП и наладить конструктивный диалог с заказчиком.

Обновления ПО АСУ ТП являются серьезной проблемой, когда нет понимания принципов, на основе которых должны строиться такие процедуры. Это часто приводит к тому, что в АСУ ТП используется устаревшее ПО с большим количеством уязвимостей, которые могут быть использованы злоумышленниками или вредоносным ПО.

И наконец, неверно выстроенные отношения с разработчиками АСУ ТП приводят к тому, что после сдачи АСУ ТП в промышленную эксплуатацию разработчики теряют интерес к компании. Становится невозможным привлечь их к решению проблем, связанных, в том числе, с безопасностью АСУ ТП. Поэтому очень важно привлекать специалистов по ИБ еще на стадии разработки АСУ ТП и заключения договоров с производителями, чтобы в договорах были прописаны все необходимые положения, предусматривающие сопровождение АСУ ТП на всех этапах жизненного цикла.

Вопрос ребром: а нужно ли вообще защищать АСУ ТП?

Некоторые главные инженеры и метрологи, с которыми приходилось беседовать на проектах по защите АСУ ТП, считают, что АСУ ТП защищать не нужно: «работает, и не трогай». В этих словах есть лишь часть правды: при защите АСУ ТП нужно всегда учитывать необходимость обеспечения непрерывности технологического процесса. Но они ошибаются, считая, что эта непрерывность может быть обеспечена без создания адекватной системы защиты.

Является ли система защиты адекватной, говорит статистика, подготовленная по результатам значительного количества проектов по защите АСУ ТП, выполненных нашей компанией.

Специалистами «Информзащиты» на основе международных стандартов и отечественных нормативно-методических документов были разработаны 25 ключевых групп требований по обеспечению безопасности АСУ ТП (Рис 1).

Требования, раскрашенные серым, не выполняются практически ни в одной компании, в которой мы проводили аудит безопасности АСУ ТП.

Практически у всех компаний отсутствует управление инцидентами ИБ

Это значит, что не проводится их анализ, отсутствуют процессы управления инцидентами, не ведется база данных инцидентов и т.д. Компании лишь всячески скрывают факты, связанные с произошедшими инцидентами и авариями. В качестве примера можно привести то, что в глобальной сети сейчас гуляет несколько миллионов вирусов и электронных червей. Но при этом находятся компании, которые до сих пор не используют антивирусное ПО. Был случай, когда в сети АСУ ТП одной такой компании произошло заражение очень старым вирусом. С ним успешно справились, но при этом никто не проводил никаких исследований на тему того, как он смог попасть в сеть. А значит, все может повториться с более негативными последствиями.

Не проводится анализ защищенности

На проектах по защите АСУ ТП специалисты «Информзащиты» создают стенд, который повторяет архитектуру сети АСУ ТП. Чаще всего, им удается взломать сеть и получить полный контроль над серверами, сетевым оборудованием и даже контроллерами, которые используются на установках: например, на установках, управляющих каткрекингом нефти, и установках, которые отвечают за распределение теплотенергии. А это значит, что злоумышленники могут сделать то же самое.

Не используются системы обнаружения вторжений и выявления сетевых аномалий

Хотя наши коллеги из других компаний отмечают положительную динамику выполнения этой группы требований.

Не проводится аудит ИБ

Аудит – это анализ соответствия заранее определенным требованиям. Если эти требования не определены, например, в политике или в стандарте, то и провести аудит не представляется возможным.

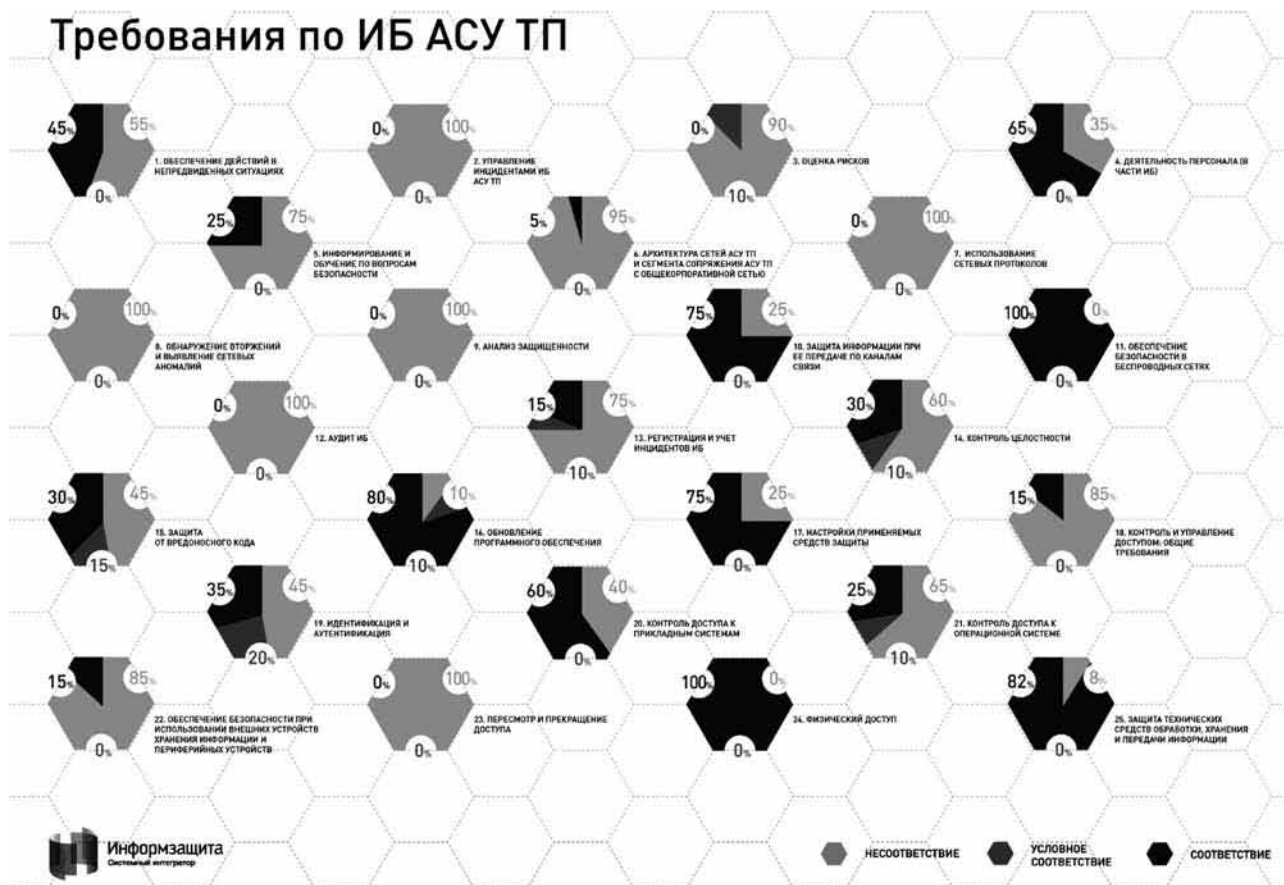


Рис.1. 25 ключевых групп требований по обеспечению безопасности АСУ ТП

Полностью отсутствует процесс пересмотра и прекращения доступа

Зачастую доступ предоставляется интуитивно и не контролируется в полной мере. Практически никогда не используются персонализированные учетные записи, а только групповые, которые защиты в систему. В связи с этим возникают проблемы при расследовании инцидентов и поиске виновных. Также

не осуществляется пересмотр и прекращение доступа. Например, после увольнения инженера АСУ ТП его учетной записью могут воспользоваться злоумышленники, если ее не заблокировать.

Зато во всех обследованных компаниях есть контроль физического доступа: охранники с автоматами, стальные двери и видеонаблюдение. Это действенные меры, но во времена высоких

скоростей развития информационных технологий они не гарантируют полную безопасность. Хакеру, который сидит дома и пьет кофе, эти меры не преграда, он вполне может подключиться удаленно.

Если более внимательно изучить остальные требования, то можно сделать вывод, сколько еще предстоит сделать для обеспечения ИБ АСУ ТП. ■

Национальная выставка-форум
«Информационная безопасность. Телекоммуникации»
2-3 декабря, 2013

**Центр
безопасности**

Более 40 уникальных докладов
по тематикам информационной безопасности
и телекоммуникаций

сформирована по итогам мероприятия
состоит из видеороликов докладов, круглых столов и
презентаций, размещена

на сайте **IS.AERCOM.BY**

Полную версию выступлений можно получить по
предварительной заявке, запросы произвольной формы
отправлять на ящик: is@aercom.by

База знаний

 **Symantec.**
Генеральный партнер

 **Fima**
Партнер семинара ЦОД

Новинки рынка

Hikvision DS-7204HVI-SV



Цифровой видеорегистратор с технологией 960H DS-7204HVI-SV

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 4 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: до 100 к/сек (12 к/сек на канал с наивысшим качеством WD1);
- жесткий диск: 1 SATA (до 4 Тб);
- интерфейсы: 4xRCA (аудио вход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;
- питание: внешний БП в комплекте DC 12V (потребляемая мощность до 20 Вт);
- размеры: 315*230*45 мм;
- вес: 2 кг.

Цена на 01.11.2013: 1 260 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Hikvision DS-7208HVI-SV



Цифровой видеорегистратор с технологией 960H DS-7208HVI-SV

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 8 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: до 200 к/сек (8 к/сек на канал с наивысшим качеством WD1);
- жесткий диск: 1 SATA (до 4 Тб);
- интерфейсы: 4xRCA (аудиовход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;

- питание: внешний БП в комплекте DC 12V (потребляемая мощность до 40 Вт);
- размеры: 315*230*45 мм;
- вес: 2 кг.

Цена на 01.11.2013: 1 890 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Hikvision DS-7216HVI-SV

Цифровой видеорегистратор с технологией 960H DS-7216HVI-SV

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 16 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: до 400 к/сек (6,5 к/сек на канал с наивысшим качеством WD1);
- жесткий диск: 1 SATA (до 4 Тб);
- интерфейсы: 4xRCA (аудиовход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;
- питание: внешний БП в комплекте DC 12 V (потребляемая мощность до 40 Вт);
- размеры: 315*230*45 мм;
- вес: 2 кг.

Цена на 01.11.2013: 2 490 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Hikvision DS-7204HWI-SH



Цифровой видеорегистратор с технологией 960H DS-7204HWI-SH

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- запись 25 к/сек на каждый во всех режимах;
- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 4 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: 100 к/сек (25 к/сек на канал с наивысшим качеством WD1);

высшим качеством WD1);

- жесткий диск: 1 SATA (до 4 Тб);
- интерфейсы: 4xRCA (аудиовход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;
- питание: внешний БП в комплекте DC 12 V (потребляемая мощность до 20 Вт);
- размеры: 315*230*45 мм;
- вес: 2 кг.

Цена на 01.11.2013: 1 380 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Hikvision DS-7208HWI-SH



Цифровой видеорегистратор с технологией 960H DS-7208HWI-SH

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- запись 25 к/сек на каждый во всех режимах;
- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 8 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: 200 к/сек (25 к/сек на канал с наивысшим качеством WD1);
- жесткий диск: 2 SATA (до 4 Тб каждый);
- интерфейсы: 4xRCA (аудиовход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;
- питание: DC 12 V (потребляемая мощность до 20 Вт);
- размеры: 445*290*45 мм
- вес: 4 кг.

Цена на 01.11.2013: 2 820 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Hikvision DS-7208HWI-SH

Цифровой видеорегистратор с технологией 960H DS-7216HWI-SH

Поставщик: ОДО «АВАНТ-ТЕХНО»

Производитель: HIKVISION

Назначение: Для записи звука и изображения.

Особенности:

- запись 25 к/сек на каждый во всех режимах;
- высокое разрешение по стандарту 960H – 960x576;
- формат сжатия H.264 High Profile;
- HDMI видеовыход Full HD 1920x1080;
- подключение к DNS серверу HIKVISION;
- двойной поток по каждому каналу;
- встроенный IP-сервер;
- удаленный просмотр с мобильных устройств.

Характеристики:

- количество каналов видео: 16 BNC;
- количество каналов аудио: 4 RCA;
- выходы: 1xBNC, 1xVGA, 1xHDMI;
- разрешение: WD1/4CIF/2CIF/CIF;
- общая скорость записи: 400 к/сек (25 к/сек на канал с наивысшим качеством WD1);
- жесткий диск: 2 SATA (до 4 Тб каждый);

- интерфейсы: 4xRCA (аудиовход), 1RJ45 10M/100M, 2xUSB 2.0, 1xRS-485;
- питание: DC 12 V (потребляемая мощность до 20 Вт);
- размеры: 445*290*45 мм;
- вес: 4 кг.

Цена на 01.11.2013: 4 080 000 бел. руб. с НДС.

Время появления на рынке: 4 квартал 2013 г.

Программное обеспечение (ПО) для построения интеллектуальных систем видеонаблюдения Axxon Next, версия 3.5



Поставщик: Частное предприятие «АксонСофт»

Производитель: ITV | AxxonSoft

Сертификат: Не подлежит.

Назначение: ПО Axxon Next предназначено для построения распределенных систем видеонаблюдения неограниченного масштаба.

Особенности: ПО Axxon Next является инновационной разработкой ведущей российской компании в области создания программных продуктов для систем видеонаблюдения.

Возможности:

Распределенная система с неограниченным количеством серверов и камер в системе.

Поддержка объективов «рыбий глаз» и паноморфных объективов ImmerVision.

Несколько методов оптимизации нагрузки на сеть, сервера и удаленные рабочие места.

Поддержка стандартов ONVIF, PCIA, потокового видео RTSP.

Интерактивная 3D-карта с режимом погружения.

Интеграция сторонних геокарт (в частности Google Maps).

Интеллектуальный поиск в архиве (по событиям, по детектору, по цвету и т.д.).

Быстрый поиск в архиве Time Compressor.

Ориентировочная цена: от 200 000 бел. руб. за канал. Бесплатно: удаленные рабочие места, звук, телеметрия, реле/лучи, видеоаналитика камер.

Время появления на рынке: ноябрь 2013 г.

Система автоматического управления шлагбаумом с функцией распознавания автомобильных номеров WaveServer A54



Поставщик: Частное предприятие «АксонСофт»

Производитель: ЗАО «Стрим-Лабс»

Сертификат: Не подлежит.

Назначение: Устройство позволяет автоматизировать управление шлагбаумом или другим исполнительным механизмом путем пропуска на территорию автомобилей из

«белого» списка, хранящегося в энергонезависимой памяти устройства.

Особенности: Встроенная SD-карта для хранения номеров и изображений, часы для фиксации времени проезда.

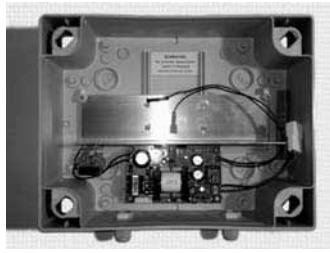
Возможности: Возможность удаленного подключения по Ethernet.

Характеристики: Подключение двух аналоговых камер для распознавания номеров. Размер устройства (117x85x35 mm)

Ориентировочная цена: 16 000 000 бел. руб.

Время появления на рынке: ноябрь 2013 г.

Источник резервированный РЕЗЕРВ-12/5У7 уличного исполнения



Поставщик: ООО «Видео-СКУД» (г. Минск)

Производитель: ООО «МикроКомСервис» (РФ)

Сертификат: РОСС RU.AB68.B041227

Назначение: Источник вторичного электропитания – резервированный импульсный РЕЗЕРВ-12/5У7 предназначен для обеспечения бесперебойного электропитания средств систем контроля и управления доступом, охранно-пожарной сигнализации, видеонаблюдения и других потребителей номинальным напряжением 12 В постоянного тока.

Особенности: Позволяет выполнять построение сложных территориально распределенных систем безопасности.

Возможности: Источник имеет герметичное исполнение и предназначен для установки на открытом воздухе для круглосуточной непрерывной эксплуатации, при температуре окружающей среды от -40°C до +40°C.

Источник обеспечивает:

- защиту АКБ от глубокого разряда при работе на резервном питании;
- защиту от короткого замыкания по выходу с отключением выходного напряжения и автоматическим восстановлением напряжения после устранения аварийного режима.

Характеристики:

- постоянное выходное напряжение, В, 13,4–14,0;
- постоянное выходное напряжение, В, 10,5–13,5 (при отсутствии напряжения сети);
- номинальный ток нагрузки при работе от сети, А, 5,0;
- диапазон входного напряжения, В, 165–275;
- габариты корпуса, мм, 254x199x102

Время появления на рынке: 2013 г.

СКУД «WEB-офис»



Поставщик: ООО «Видео-СКУД» (г. Минск)

Производитель: ООО «СКД-С» (РФ)

Сертификат: до 21.06.2015 г.

Назначение: Полнофункциональное решение СКУД для средних и малых объектов.

Особенности: Встроенный WEB-сервер на базе micro-PC с установленным ПО.

Возможности:

- проход и проезд на территорию и в помещения по предъявлению идентификаторов;
- учет рабочего времени сотрудников;
- удаленный контроль за нахождением сотрудников на объекте;
- проход посетителей (с ограничением времени действия пропуска – с точностью до 1 часа, с автоматическим запретом пропуска при входе и выходе);
- работа с различными идентификаторами (бесконтактные карты, PIN-код, штрих-код) в одной системе.

Характеристики:

- максимальное число пользователей – 20400;
- максимальное число хранимых событий – 48000;
- напряжение питания – (85...265) В, 50 Гц;

- потребляемая мощность, не более, 1,5 Вт;
- металлический корпус;
- встроенный источник бесперебойного питания.

IP-камера ICA-HM620



Поставщик: Производственно-торговое частное унитарное предприятие «Рамок»

Производитель: PLANET Technology Corporation

Сертификат: Есть.

Назначение: Скоростная купольная IP-камера предназначена для записи видеозображения.

Особенности: Широкая зона наблюдения, оптический зум до 20х, 360 градусов непрерывное панорамирование.

Возможности:

Поддержка четкого изображения 24 часа в сутки. Удаление шумов из видеосигнала.

Характеристики: 1/2.8 "Sony Progressive Scan CMOS Sensor, 1920x1080 pix, ИК-фильтр; 4.7 ~ 84.6 mm Vari-Focal, 20x оптический, 8x цифровой zoom.

Ориентировочная цена: 2176 у.е.

Время появления на рынке: 2013 г.

Видеорегистратор NVR-3210



Поставщик: Производственно-торговое частное унитарное предприятие «Рамок»

Производитель: PLANET Technology Corporation

Сертификат: Есть.

Назначение: 32-канальный сетевой видеорегистратор предназначен для построения IP систем видеонаблюдения.

Особенности: Управление до 32 IP-камерами.

Возможности: Мониторинг видеонаблюдения с мобильного телефона. Настройка посредством Web-интерфейса. Поддержка русского языка. Интеллектуальный поиск IP-камер. Функция циклической записи позволяет делать видеозапись в формате 24/7.

Характеристики: 2560*1920, H.264/MPEG4/MJPEG, 4*SATA (Support RAID 0/1/5/10), Gigabit LAN, 6*USB, eMAP, 2-way Audio, E-SATA, VGA output, Auto-Power recovery, 256-ch CMS.

Ориентировочная цена: 1130 у.е.

Время появления на рынке: 2013 г.

Коммутатор XGS3-42000R



Поставщик: Производственно-торговое частное унитарное предприятие «Рамок»

Производитель: PLANET Technology Corporation

Сертификат: Есть.

Назначение: Построение систем на больших предприятиях.

Возможности: Резервные модули управления и два блока питания обеспечивают способность безостановочной работы сети. Горячая замена модулей.

Характеристики: Управляемый 3-го уровня, модульный, стекируемый, 168 портов GbE + 156 слотов SFP + 13 слотов XFP, 336 Гбит/с.

Ориентировочная цена: 1900 у.е.

Время появления на рынке: 2013 г.

ROGER RFT1000



Поставщик: ОДО «Сфератрэйд»
Производитель: ROGER Sp.j. (Польша)

Назначение: Считыватель бесконтактных карт автономный/сетевой, с интегрированным биометрическим считывателем (оптический сканер отпечатков пальцев), внутренняя установка, TCP/IP, RS-485, Wiegand, память количества образцов отпечатков – 1900, 0...+45°C, 85x85x52 мм. Предназначен для считывания карт и/или отпечатков пальцев.

Особенности:

- оптический сканер отпечатков пальцев;
- считыватель карт ISO/IEC 14443 Mifare;
- режим работы 1:1;
- режим работы 1:N;
- до 1900 отпечатков пальцев в режиме 1:N;
- выходной интерфейс RACS CLK/DTA и Wiegand;
- интеграция с PR Master;
- протокол связи AES 128 CBC;
- настройка считывателя по RS-485 или Ethernet;
- SDK.

Характеристики:

- Напряжение питания: 12VDC;
- Потребляемый ток, не более: 130 mA;
- Диапазон рабочих температур: +5°C...+40°C;
- Относительная влажность, не более: 95 %;
- Тип монтажа: накладной;
- Габаритные размеры: 85x85x52 мм;
- Вес: 0,160 кг.

Emerald TS100



Поставщик: СП «Унибелус» ООО
Производитель: CEM Systems Ltd (Великобритания)

Сертификат: В процессе получения.

Назначение: Интеллектуальный терминал доступа.

Особенности: Скремблированная клавиатура.

Возможности: Контроллер точки прохода, встроенный считыватель iClass и iClass SE.

Характеристики: Сенсорный ЖКИ дисплей 4,3", встроенная БД, Ethernet.

Ориентировочная цена: 1 600 у.е.

Время появления на рынке: сентябрь 2013 г.

Emerald TS200



Поставщик: СП «Унибелус» ООО
Производитель: CEM Systems Ltd (Великобритания)

Сертификат: В процессе получения.

Назначение: Интеллектуальный терминал доступа.

Особенности: Скремблированная клавиатура, VOIP интерком.

Возможности: Контроллер точки прохода, встроенный считыватель iClass и iClass SE.

Характеристики: Сенсорный ЖКИ дисплей 4,3", встроенная БД, Ethernet.

Ориентировочная цена: 1 900 у.е.

Время появления на рынке: сентябрь 2013 г.

Emerald TS300



Поставщик: СП «Унибелус» ООО

Производитель: CEM Systems Ltd (Великобритания)

Сертификат: В процессе получения.

Назначение: Интеллектуальный терминал доступа.

Особенности: Скремблированная клавиатура, VOIP интерком, удаленные приложения.

Возможности: Контроллер точки прохода, встроенный считыватель iClass и iClass SE.

Характеристики: Сенсорный ЖКИ дисплей 4,3", встроенная БД, Ethernet.

Ориентировочная цена: 1 900 у.е.

Время появления на рынке: сентябрь 2013 г.

RVi-IPC32DNS



Поставщик: ООО «ЭРВИ групп»

Производитель: ООО «ЭРВИ групп»

Сертификат: Сертификат соответствия ГОСТ Р № РОСС CN.AG98.B10906

Назначение: Охранное видеонаблюдение вне помещений.

Особенности: Миниатюрные размеры, антивандальный корпус со степенью защиты IP66, ИК-подсветка, питание по стандарту

PoE (IEEE802.3af).

Возможности: Трансляция видеопотока с разрешением 1920x1080 пикселей со скоростью 25 к/с, круглосуточное видеонаблюдение.

Характеристики:

- максимальное разрешение и частота кадров 1920x1080, 25 к/с;
- объектив 3.6 мм;
- ИК-подсветка до 15 м;
- рабочая температура -40°C...+60°C;
- габаритные размеры Ø64x80 мм.

Время появления на рынке: ноябрь 2013 г.

RVi-IPC42DNS



Поставщик: ООО «ЭРВИ групп»

Производитель: ООО «ЭРВИ групп»

Сертификат: Сертификат соответствия ГОСТ Р № РОСС CN.AG98.B10906

Назначение: Уличное видеонаблюдение.

Особенности: Корпус со степенью защиты IP66, ИК-подсветка, компактные размеры, питание по стандарту PoE (IEEE802.3af).

Возможности: Трансляция видеопотока разрешением 1920x1080 пикселей со скоростью 25 к/с, круглосуточное видеонаблюдение.

Характеристики:

- максимальное разрешение и частота кадров 1920x1080, 25 к/с;
- объектив 3.6 мм;
- ИК-подсветка до 15 м;
- рабочая температура -40°C...+60°C;
- габаритные размеры Ø63.5 x 160 мм.

Ориентировочная цена: 2 821 500 бел. руб.

Время появления на рынке: октябрь 2013 г.

RVi-IPN16/2 PRO**Поставщик:** ООО «ЭРВИ групп»**Производитель:** ООО «ЭРВИ групп»**Сертификат:** Сертификат соответствия ГОСТ Р № РОСС CN.AГ98.B10905**Назначение:** Охранное IP-видеонаблюдение.**Особенности:** Запись до 16 видеопотоков разрешением до 5 МП каждый. Запись 16 FullHD видеопотоков со скоростью 25 к/с. Суммарный входящий битрейт до 160 Мбит/с.**Возможности:** Отображение видеoinформации в реальном времени. Поддержка 2-х HDD до 4 ТБ каждый. ПО для организации УРМ в комплекте. Возможность мониторинга с мобильных платформ (iOS, Android, Windows Phone).**Характеристики:**

- количество видеопотоков для записи (макс.) 16;
- суммарная скорость декодирования потоков 1920x1080 (1080p), 400 к/с;
- количество, тип, максимальный объем HDD 2, SATA3, 4 ТБ;
- видеовыходы 1 VGA / 1 HDMI (аудио/видео);
- тревожные вх./вых. 16/3;
- питание DC 12 В.

Ориентировочная цена: 7 837 500 бел. руб.**Время появления на рынке:** ноябрь 2013 г.**RVi-IPN16/8 PRO****Поставщик:** ООО «ЭРВИ групп»**Производитель:** ООО «ЭРВИ групп»**Сертификат:** Сертификат соответствия ГОСТ Р № РОСС CN.AГ98.B10905**Назначение:** Охранное IP-видеонаблюдение.**Особенности:** Запись до 16 видеопотоков разрешением до 5 Мп каждый. Запись 16 FullHD видеопотоков со скоростью 25 к/с. Суммарный входящий битрейт до 160 Мбит/с.**Возможности:** Отображение видеoinформации в реальном времени. Поддержка 8-ми HDD до 4 ТБ каждый. ПО для организации УРМ в комплекте. Возможность мониторинга с мобильных платформ (iOS, Android, Windows Phone).**Характеристики:**

- количество видеопотоков для записи (макс.) 16;
- суммарная скорость декодирования потоков 1920x1080 (1080 p), 400 к/с;
- количество, тип, максимальный объем HDD 2, SATA3, 4 ТБ;
- видеовыходы 1 VGA / 1 HDMI (аудио/видео);
- тревожные вх./вых. 16/3;
- питание AC220 В.

Ориентировочная цена: 14 701 500 бел. руб.**Время появления на рынке:** ноябрь 2013 г.**RVi-R04LA****Поставщик:** ООО «ЭРВИ групп»**Производитель:** ООО «ЭРВИ групп»**Сертификат:** Сертификат соответствия ГОСТ Р № РОСС CN.AГ98.B10905**Назначение:** Охранное видеонаблюдение на малых объектах.**Особенности:** Запись разрешения D1 (704x576) и частотой 25 к/с по каждому каналу, выполнен в пластиковом корпусе, имеет компактные размеры, широкие возможности работы по сети.**Характеристики:**

- разрешение и скорость записи 704x576 – 100 к/с;
- количество каналов – 4 (BNC);
- количество аудио вх./вых. – 2 вх./1 вых. (BNC);
- видеовыходы 1 VGA (Full HD) / 1 BNC;
- питание DC 12 В;
- габаритные размеры 200x200x45 мм.

Ориентировочная цена: 1 120 000 бел. руб.**Время появления на рынке:** октябрь 2013 г.**Счет подписка на журнал «Технологии безопасности», 1-е полугодие 2014г.**

Подписные индексы РУП «Белпочта»:

01248 - для индивидуальных лиц, 012482 - ведомственная подписка

www.aercom.by**ТЕХНОЛОГИИ
БЕЗОПАСНОСТИ**журнал для руководителей предприятий
и специалистов отрасли безопасности

Платательщик _____

Адрес: 220072, г. Минск, ул. Гусовского, 6, оф. 2.15.2. Тел./ф.: +375 17 290-84-05, 256-10-35 (47) ООО «АЭРКОМБел»;

Р/с 3012007960018 в ЦБУ №526 ОАО «Белинвестбанк», код 739

220013, г. Минск, пр. Независимости, 77; УНП 190970885; ОКПО 377800425000

СЧЕТ-ФАКТУРА 6/н 26 ноября 2013

Название	Единица измерен.	Количество	Отпускная цена, руб	Сумма руб.
Подписка на журнал «Технологии безопасности» №1-3, 2014г.	шт.	3	93000	279000

Цена согласно прейскуранта № 6, от 22.08.2013**Всего к оплате без НДС:** Двести семьдесят девять тысяч рублей**Без НДС на основании п. 3.12 ст. 286 Особенной части Налогового Кодекса РБ**

Цель приобретения: для собственного потребления

► Обязательно укажите в платежном поручении
(в назначении платежа) почтовый адрес и телефон

Руководитель
предприятия
Драгун С.А.

ООО «АэркомБел» является издателем настоящего журнала. Периодичность выхода 1 раз в 2 месяца.

Информация о компаниях

Авант-Техно, ОДО

АВАНТ-ТЕХНО системы безопасности

220004, г. Минск, ул. Короля, 45-16в

Тел./факс: (017) 200-01-09, 226-43-52, 200-08-22, 200-44-83

E-mail: info@avant.by

Сайт: www.avant.by

Год основания: 2003

УНП: 190423783

Контактные лица:

- Козодаев Руслан Валерьевич, директор;
- Новик Владимир Павлович, начальник отдела продаж;
- Красногоров Александр Михайлович, начальник отдела систем видеонаблюдения.

Производство: охранные, пожарные извещатели и оповещатели.

Услуги:

Консультации по подбору и применению охранно-пожарного оборудования и систем видеонаблюдения. Гарантийное и послегарантийное сервисное обслуживание на базе собственного авторизованного сервисного центра.

Поставка:

- технические средства охранно-пожарной сигнализации;
- системы видеонаблюдения и контроля доступа;
- IP-видеосистемы;
- сопутствующие материалы для монтажа систем.

Дистрибьютор компаний:

PARADOX (Канада) – ведущий мировой производитель охранной техники, выпускающий обширный спектр охранного оборудования и продающий свою продукцию более чем в 60 стран мира.

HIKVISION – международная компания с производством в Китае. Разработка и производство IP-видеосистем, видеокамер, видеорегистраторов и плат видеоввода. Первое место в мире по производству видеорегистраторов. Hikvision представляет самые передовые решения со сжатием в формате H.264 для индустрии цифрового видеонаблюдения на основе своих собственных запатентованных алгоритмов.

Бастион – широкий ассортимент источников питания.

НВП Болид – производитель интегрированных охранных систем.

Avicam Electronics – видеокамеры, видеорегистраторы, объективы и сопутствующее оборудование.

АДАНИ, УП



220075, г. Минск, ул. Селицкого, 7

Тел.: (017) 346-29-01, 346-29-03

Факс: (017) 346-29-02

E-mail: info@adani.by

Сайт: www.adanisystems.com

Год основания: 1991

УНП: 100054851

Контактные лица:

- Линева Елена Владимировна;
- Сосенко Константин Викторович;
- Семеников Анатолий Иванович;
- Губаревич Игорь Иванович.

Лицензии:

- № 02040/0573310 выдана МЗ РБ, действительна до 27.04.2015;
- № 02300/108-4 выдана Департаментом по ядерной и радиационной безопасности МЧС, действительна до 15.07.2015.

Сертификаты:

На предприятии внедрена международная система качества ISO 9001:2000 и ISO 13485:2003, сертифицированная организацией SGS.

Услуги: Поставка, монтаж и сервисное обслуживание производимого оборудования.

АксонСофт, Частное предприятие



220100, г. Минск, ул. Куйбышева, 40, офис 3

Тел.: (017) 292-66-11, 292-66-99

E-mail: minsk@axxonsoft.com

Сайт: www.axxonsoft.by

УНП: 191217449

Контактные лица: Лисовский Дмитрий Васильевич, коммерческий директор.

Поставка:

Программное обеспечение для построения интегрированных систем видеонаблюдения и комплексной безопасности объекта:

- система видеонаблюдения нового поколения с функциями интеллектуального поиска в архиве: Axxon Next;
- интегрируемая платформа безопасности с распределенной архитектурой «Интеллект»;
- модуль контроля кассовых операций POS-Интеллект;
- модуль интеграции ОПС и СКУД;
- модуль распознавания и поиска похожих лиц FACE-Интеллект;
- модуль распознавания автомобильных номеров АВТО-Интеллект;
- модуль распознавания номеров вагонов ЖД-Интеллект;
- модуль защиты банкоматов АТМ-Интеллект;
- модуль контроля характеристик транспортных потоков;
- модуль учета рабочего времени.

Дистрибуция оборудования для систем безопасности: Axis, Sony, Panasonic, Arecont Vision, Samsung, Vivotek, Microdigital, Wizebox, Тахион, StreamLabs.

Сервера для систем видеонаблюдения.

Система автоматического управления шлагбаумом с распознаванием автономеров WaveServer A54.

Дистрибьютор компаний: ITV | AxxonSoft, IPDrom, StreamLabs.

АльфаСистемы, ООО



220090, г. Минск, Логойский тракт, д. 22а, офис. 207

Тел.: (017) 262 84 64, 268 05 36

Факс: (017) 265 12 59

E-mail: info@cctv.by

Сайт: www.cctv.by

Год основания: 2005

УНП: 190598104

Контактные лица: Гаврютиков Александр Анатольевич, директор.

Услуги: технические консультации, гарантийное и послегарантийное обслуживание систем видеонаблюдения, систем контроля и управления доступом.

Поставка: оборудования систем видеонаблюдения, систем контроля и управления доступом.

Дистрибьютор компаний: Samsung Techwin (Корея); GRUNDIG (Германия); LevelOne (Германия); CBC Group (торговые марки Computar, GANZ); AXIS Communications (Швеция); Arecont Vision (США); IFS (США); Evidence Network; Topcam Technology (Китай); Spacocom (Япония); SC&T (Тайвань); Widearea Times Technology Co. (Китай); ITV (РФ), ISS (РФ); VideoNet (РФ).

БЕЗОПАСНЫЙ ДОМ, ОДО



220094, г. Минск, 2-й Велосипедный пер., д. 30, комн. 402

Тел./Факс: (017) 298-38-05(15), (029) 150-95-97

E-mail: odobd@mail.ru

Сайт: www.odobd.by

Год основания: 2006

УНП: 190682380

Контактные лица:

- Сидоренко Александр Владимирович, директор;
- Малец Сергей Федорович, ГИП;
- Янович Павел Станиславович, главный инженер.

Лицензии:

- лицензия №02010/6670 выдана МВД РБ от 28.01.2011 г. №2км, действительна до 02.03.2021 г.;
- лицензия № 02300/1268 выдана МЧС РБ от 21.01.2011 г. №3км, действительна до 14.03.2016 г.

Услуги:

Проектирование, монтаж, наладка и техническое обслуживание систем пожарной сигнализации, систем оповещения о пожаре, систем охранной сигнализации, систем телевизионного видеонаблюдения и контроля управления доступом, локальных вычислительных сетей (ЛВС) и структурированных кабельных сетей (КСК), компьютерных сетей с использованием витой пары и волоконно-оптического кабеля, учрежденческих автоматических телефонных станций (мини-АТС), систем и сетей громкоговорящей диспетчерской связи.

Выполненные проекты:

ИП «Велком», ЗАО «Белорусская сеть телекоммуникаций», ЗАО «Projestos projektai» (Литовская Республика), ООО «Евроторг», ООО «Златка», ОАО «Франсбанк», ОАО «Белинвестбанк», ЗАО «Дельта Банк», ОАО «Белагропромбанк», ОАО «Технобанк», ООО «Аксис на Кирова», ООО «Нестле Россия», ЗАО «Торговый дом «ЛУКБЕЛОЙЛ», ЗАО «Универсам «Юго-Запад плюс», ООО «Маттиоли», УМСР-154 ОАО «МАПИД», ООО «Орифлэйм косметикс», ООО «Белавтэкс», ИП «Ресторан Джомолунгма», ООО «ВкусСервис», ООО «СУШИ ВЕСЛА», ИП «ТА-Инжиниринг», ООО «ПРЕВАР», ООО «Лимкомсервис», СП «ВестТрансЛайн» ООО, ТПОО «Брест», ОАО «БЕЛРЫБА», ЧТУП «Ювелирная сеть 585», ЗАО «Торговый дом «ШагоВита», СП «САМБЕСТ» ООО, УП «Юнифарм», ЗАО «Федерация», ОАО «Торгодежда», КУП «Минскхлебпром», ГУ «Централизованная система детских библиотек», ЧУП «Поречье Белкоопсоюза», ГУ «НИИ онкологии и медицинской радиологии имени Н.Н.Александрова», УО «Национальный центр художественного творчества детей и молодежи» МО РБ, ТКУП «Минсктранс» филиал «Трамвайный парк», РУПС «Птицефабрика «Дружба», ЗАО «ТрестБелПСП-строй», Высший Хозяйственный Суд Республики Беларусь, КУП «Минский метрополитен».

БелГвард, ООО



220053, г.Минск, ул.Новаторская д.2А, оф.214-2

Тел.: (017) 282-90-56, (029) 6216573, +375 29 482-90-56

E-mail: info@belgvard.by

Сайт: www.belgvard.by

Год основания: 2010

УНП: 191310608

Контактные лица: Вихарев Виктор, директор.

Лицензии: МВД 02010/14251 от 14.04.2011 №7км 14.04.2021.

Услуги:

Проектирование, монтаж, техническое обслуживание:

- Архитектурная подсветка зданий и сооружений;
- Системы электропитания зданий и сооружений;
- Пультовая и GSM охранная сигнализация;
- Аналоговое видеонаблюдение;
- IP-видеонаблюдение;
- Системы контроля и управления доступом;
- Видеодомофоны;
- Спутниковое и эфирное телевидение;
- Естественная вентиляция и дымоудаление;
- Локальные вычислительные сети;
- Сети связи.

Выполненные проекты: Сеть салонов «СКВИРЕЛ» – ОС, СКУД, IP СВН;

ОАО «Щучинский МСЗ» – СКУД, СВН; Волковыское ОАО «Беллакт» – СКУД, СВН, Лвс; УП «РСР10» – СВН и др.

Биометрик Солюшнс,ООО (Biometric Solutions, LLC)



220033, г. Минск, пр. Партизанский 8, к. 28 каб.6

Тел./факс: (017) 3897212, (044) 466-36-36, (033)-366-36-36

E-mail: info@bio-system.by

Сайт: www.bio-system.by

Год основания: 2012

УНП: 192102396

Контактные лица:

- Юшин Евгений Александрович, директор;
- Асаёнок Денис Дмитриевич, отдел продаж.

Поставка: Системы безопасности: биометрические системы контроля доступа и учёта рабочего времени, видеонаблюдение (в перспективе).

Выполненные проекты по системам контроля доступа и учёта рабочего времени:

ООО «Белавтоконтинент», ООО «Трест Росспецэнергомонтаж», ООО «Экомедсервис – Медицинский центр», ОАО «Белагропромбанк», ООО «БелПрайм Солюшнс», СП «ДЖЕНТИ-СПЕДИШН», ЧП «ЭйВит», ООО «Биоком Технологии», ООО «Стройбыт-ЗОВ», ООО «Белавтоконтинент».

Дистрибьютор компаний: ANVIZ.

БиоСофтТрейд, ООО



220141, г. Минск, ул. Ф.Скорины, д.52

E-mail: info@biosofttrade.by

Сайт: www.biosofttrade.by

Год основания: 2006

УНП: 190739708

Контактные лица: Петруша Владимир Станиславович, директор.

Производство:

Биометрическая система учёта рабочего времени Bioscan ACS TT, RFID считыватель стандарта EM Marine – BioProху, системы распределённого мониторинга параметров оборудования, биометрический замок Bioscan 21, биометрический турникет.

Услуги: Автоматизация технологических процессов, пуско-наладочные работы.

Поставка: RFID карты, частотные преобразователи, аналого-цифровые преобразователи, промышленные контроллеры.

Дополнительная информация:

Готовится к выпуску биометрическая система контроля доступа.

Производим модернизацию сложного промышленного оборудования, замену двигателей постоянного тока на асинхронные двигатели переменного тока с разработкой и внедрением комплексных систем управления приводами.

Видео-СКУД, ООО



220125, г. Минск, ул. Уручская, дом 23а, оф. 1

Тел.: (017) 265-67-63, (029) 686-87-63

E-mail: info@videoskud.by

Сайт: www.videoskud.by

Год основания: 2009

УНП: 191216787

Контактные лица:

- Парсиев Дмитрий Дзантемирович, директор;
- Суцёнок Василий Михайлович, заместитель директора.

Лицензии:

- №02010/0614715 выдана МВД РБ, действительна до 14.05.15 г. На проектирование, монтаж, наладку и ТО средств и систем охраны (ООО «Невия»);
- № 02300/0565722 выдана МЧС РБ, действительна до 08.07.15 г. На монтаж, наладку и ТО АПС (ООО «Невия»).

Сертификаты: ТПГ «КОМКОМ»; ЗАО «Системы контроля доступа»; D-Link; Beward; MACROSCOP и т.д.

Услуги: проектирование, монтаж, наладка и ТО систем безопасности (совместно с ООО «Невия»).

Поставка: оборудования (первый импортёр) видеонаблюдения (IP и CCTV), СКУД, металлодетекторы, турникеты, шлагбаумы, резервные источники электропитания и т.д.

Выполненные проекты (совместно с ООО «Невия»): ПРУП «Минский завод специального инструмента и технологической оснастки» – проектирование, поставка оборудования, монтаж «Автоматизированной системы контроля и управления доступом «Кронверк» с функцией учета рабочего времени персонала завода»; ИЗАО «Пивоваренная компания «Сябар» – проектирование, поставка оборудования, монтаж и ввод в эксплуатацию Системы IP мегапиксельного видеонаблюдения и системы IP-контроля и управления доступом «Кронверк»;

за 2009-2013 гг. более 60 крупных объектов.

Дистрибьютор компаний: MACROSCOP (Интеллектуальное ПО для систем IP-видеонаблюдения); ООО «Мегабит» (СКУД «Кронверк», СКУД «Ревверс»), ТПГ «КОМКОМ» (ЦСВН «Ewclid», «Ewclid-AUTO», клиент-кассир «Digital Duplex»); НПП «Локаторная техника» (металлодетекторы «Паутина»); Brickcom (Тайвань, IP-системы видеонаблюдения); Beward, (РФ, IP-системы видеонаблюдения) и т.д.

Завод СВТ, ЧУП

220005, г. Минск, пр. Независимости, 58, корпус 30

Тел./факс: (017) 2902859, 2939792

E-mail: marketing@zsvt.by, sales@zsvt.ru

Год основания: 2006

УНП: 190737825

Контактные лица:

- Сякерский Валентин Степанович, главный инженер;
- Шлопак Людмила Васильевна, заместитель директора;

- Пономарева Елена Михайловна, и.о. начальника отдела маркетинга и продаж.

Производство:

- Радиоизмерительная техника: осциллографы, вольтметры, токоизмерительные клещи, мультиметры, генераторы, частотомеры, анализаторы шума, калибраторы.
- Вычислительная техника и средства отображения: видеомониторы "ИНФОТОН", ПЭВМ и тонкие клиенты "ИНФОТОН".
- Средства обеспечения безопасности: металлодетекторы арочные «Инфотон-1003М», металлодетекторы досмотровые «МД-1001М».
- Прочее: дозиметры, источники питания, ЖКИ-индикаторы.

Дополнительно:

Частное производственное унитарное предприятие ЧУП "Завод СВТ" образовано в 2006 г. на базе структурных подразделений ОАО "Минский приборостроительный завод". Более 30 лет основным направлением деятельности является производство изделий спецтехники по заказам Министерства обороны Российской Федерации и радиоизмерительных приборов.

Развивая традиции производства качественной технологически сложной продукции, с 2013 года специалистами предприятия освоено производство вычислительной техники, а также мониторов и средств отображения под собственной торговой маркой «ИНФОТОН».

Модельный ряд включает в себя более 100 типов мониторов с диагональю от 17 до 29 дюймов, а также ПЭВМ и тонких клиентов. Специалисты завода готовы разработать и изготовить средство отображения информации «под заказчика», включая видеостены, информационные табло, промышленные и коммерческие дисплеи любых размеров и функционального назначения.

КЛАССКОМ, Научно-производственное общество с ограниченной ответственностью**КЛАССКОМ**

220053, г. Минск, ул. Будславская, 19-407

E-mail: office@classcom.by

Сайт: www.classcom.by

Год основания: 2001

УНП: 190268725

Контактные лица: Ткаченко Сергей Александрович, директор.

Лицензии:

- №02300/679 на право осуществления деятельности по обеспечению пожарной безопасности с 21.02.2007 г. по 20.02.2017 г.;
- №02010/115 на право осуществления охранной деятельности с 28.12.2001 г. по 27.12.2021 г.

Сертификаты: № BY/112 03.0.3023 00562, с 28.02.2012 г. по 28.02.2017 г.

Производство: АСПС «ЭСТАФЕТА»; ППКП «ВЕЖА»; ИБП 12/3; ИБП 24/1,5.

Услуги:

- создание автоматизированных систем диспетчеризации и противопожарной защиты зданий и сооружений;
- разработка проектно-сметной документации для создания систем охранно-пожарной сигнализации, оповещения о пожаре, противопожарной защиты и всех видов пожаротушения;
- монтаж, наладка и техническое обслуживание систем охранно-пожарной сигнализации, оповещения о пожаре и всех видов пожаротушения;
- предоставление тренировочных курсов для специалистов подрядных и эксплуатирующих организаций по вводу в действие и техническому обслуживанию адресных систем пожарной сигнализации.

Поставка: адресная система пожарной сигнализации INTEGRAL IP (Австрия).

Выполненные проекты:

- 2001-2005 гг. внедрение АСПС «ЭСТАФЕТА» в Минском метрополитене;
- 2001-2006 гг. внедрение АСПС «ЭСТАФЕТА» на Белорусском металлургическом заводе;
- 2002-2007 гг. создание первой отечественной автоматизированной системы противопожарной защиты здания «Национальная библиотека Беларуси»;
- 2004-2005 гг. создание комплексной системы безопасности в гостинице «Лучеса» г.Витебска;
- 2004-2007 гг. создание автоматизированной системы на ТЦ «Столица»;
- 2006-2008 гг. создание комплексной системы противопожарной защиты на Мозырском подземном хранилище газа ОАО «Белтрансгаз»;
- 2010-2011 гг. создание автоматизированной системы противопожарной защиты на мусороперерабатывающем заводе в г. Бресте.

Дистрибьютор компаний:

- SCHRACK Seconet, AG (Австрия);
- HOCHIKI (Япония).

Новатех Системы Безопасности, ЗАО**НОВАТЕХ**

220125, г. Минск, ул. Городецкая, 38а, 3-й этаж

Тел.: (044) 718-53-50 Velcom, (033) 664-89-02 MTC, (017) 286-39-51 (52)

E-mail: info@novatekh.by

Сайт: www.novatekh.by

Год основания: 2006

УНП: 190543080

Лицензия: №02300/1827, выдана на основании решения от 03.06.2009 г. №10км сроком на 5 лет, действительна до 03.06.2014 г., зарегистрирована в реестре лицензий МЧС РБ за №1827.

Услуги:

Разработка, производство и продажа оборудования пожарной и охранной сигнализации, систем радио и GSM-охраны.

ЗАО «Новатех Системы Безопасности» представляет собой команду специалистов высокого уровня в области разработки, производства и реализации продукции.

ЗАО «Новатех Системы Безопасности» гарантирует комплексную сервисную поддержку. Оказывает бесплатные консультации по установке, настройке, программированию оборудования, а также услуги по шеф-монтажу систем безопасности.

Дистрибьютор компаний:



Представитель Dallmeier electronic в Республике Беларусь.

Авторизованный дистрибьютор по продаже, установке и гарантийному обслуживанию систем безопасности NOVUS® на территории Республики Беларусь.

Производитель бюджетной линейки видеонаблюдения 2х2.

Орионпроект, ЧСУП



220131, г. Минск, 1-й Измайловский пер., д. 51, оф. 4

Тел.: (017) 290-04-58, 290-04-59

E-mail: info@orionproject.by

Сайт: www.orionproject.by

Год основания: 2009 г.

УНП: 191107028

Контактные лица: Черняк Евгений Евгеньевич, заместитель директора.

Услуги:

- продвижение, разработка, техническое сопровождение, обучение, реализация, гарантийное, послегарантийное обслуживание и ремонт продукции «НВП Болид» (РФ) на рынке Республики Беларусь;
- проведение сертификационных и плановых испытаний оборудования на соответствие существующим нормам безопасности;
- проведение конференций, семинаров и обзорных лекций с проектно-монтажными и другими заинтересованными организациями на предмет популяризации применения оборудования «НВП Болид», ознакомление с новыми технологиями и тенденциями развития в области систем обеспечения безопасности, автоматизации и диспетчеризации объектов;
- оказание содействия, консультаций и помощи в решении организационных и технических вопросов поставки, применения и наладки оборудования.

Поставка: весь спектр оборудования ЗАО НВП «Болид».

Дополнительная информация: авторизованный представитель компании ЗАО НВП «Болид» на территории Республики Беларусь.

ОФИС – ТЕХНИКА, ООО



220053, г. Минск, ул. Нововиленская, д. 8, офис 47

Адрес юридический: 222310, г. Молодечно, ул. Космонавтов 13 ком. 102

Тел./факс: (017) 289-78-54, 233-23-24

E-mail: info@officetechnica.by

Сайт: www.officetechnica.by

Год основания: 1997

УНП: 600455190

Контактные лица:

- Пашковский Дмитрий Васильевич, учредитель;
- Смирнов Сергей Валентинович, коммерческий директор.

Услуги: сервисное обслуживание офисной и полиграфической техники.
Поставка: уничтожители документов (шредеры), переплетное оборудование, ламинаторы, биджи, пленка для ламинирования, резаки, полиграфическое оборудование.

Выполненные проекты: комплексное обеспечение оргтехники,

уничтожителями, полиграфическим оборудованием Совета Республики. Оснащение уничтожителями документов ГХУ УД Президента, Суда Евра3ЭС.

Дистрибьютор компаний: Mitsubishi Electric, HSM, TIKO, OPUS, CYKLOS, GMP, KW-triO.

Дополнительная информация:

Интернет – магазин «ОФИСШОП» <http://www.officeshop.by>.

Наши партнеры: ГХУ Управления делами Президента Республики Беларусь, КГБ РБ, МВД РБ, СК РБ, Беларусьбанк, Банк БелВЭБ, БПСбанк, Беларусский, БелАЗ и т.д.

Просвет, ИВООО



220013, г. Минск, ул. Кульман, 2

Тел.: (017) 292-70-52, 232-30-11, (029) 672-25-58

E-mail: prosvet@security.by

Сайт: www.securit.by

Год основания: 1992

УНП: 100151049

Контактные лица:

- Царев Андрей Владимирович, директор;
- Царева Елена Сергеевна.

Лицензии: Специальное разрешение (лицензия) № 02010/0526922 на право осуществления деятельности по обеспечению безопасности юридических и физических лиц. Выдано Министерством внутренних дел Республики Беларусь, действительно до 27.08.2014 г.

Сертификаты:

- сертификат № 0000023 «Авторизованный дилер и сервисный центр PERCo» (до 01.07.2014 г.);
- сертификат № 0000025 «Авторизованный инсталлятор PERCo» (до 27.03.2014 г.);
- сертификат «Авторизованный и сертифицированный дистрибьютор ASSA ABLOY» (до 29.08.2014 г.);
- сертификат уполномоченного дилера компании «Entromatic» (торговая марка DITEC).

Услуги: монтажные работы по установке камер видеонаблюдения, звукового оборудования, турникетов, шлагбаумов техническое и гарантийное обслуживание.

Поставка: системы видеонаблюдения, системы контроля доступа, шлагбаумы, электромеханические защелки, доводчики, испытательное оборудование.

Выполненные проекты: ОАО «ХК банк», РГЛЦ «Силичи», ООО «Трайпл», УП «Минский парниково-тепличный комбинат», Дом правосудия, ОАО «Алютерм», ПО «Беларусский», ПО «МТЗ», ПО «МАЗ», ТЭЦ-5, ЗАО «Ноябрьскгаздобыча», ЗАО «Сибнефть», БНТУ, РУП «Протезно-восстановительный центр», Национальный аэропорт Минск.

Дистрибьютор компаний: PERCo, ASSA ABLOY Sicherheitstechnik GmbH, Eff-Eff, GeoVision Inc., DITEC S.p.A.

Рамок, Производственно-торговое частное унитарное предприятие



220036, г. Минск, ул. Лермонтова, 29

Тел./факс: (017) 210-22-80, 213-67-00, (029) 613-67-00, (033) 313-67-00

E-mail: ramok@ramok.by

Сайты: www.RAMOK.by, www.BizSoft.by, www.ydom.by, www.kypi.by

Год основания: 1992

УНП: 100001879

Контактные лица: Яско Владимир Федорович, директор.

Лицензии:

- Лицензия на право осуществления деятельности по обеспечению безопасности юридических и физических лиц №02010/0444764, выда-

на Мингорисполкомом 13.03.09 г., срок действия – до 13.03.2014 г.;
 - Лицензия на право осуществления деятельности по обеспечению пожарной безопасности № 02300/2584, выдана МЧС РБ 26.07.11 г., срок действия – до 25.07.2016 г.

Сертификаты:

- Сертификат соответствия №BY/112-04.01.002 00156 от 07.10.2006 г., действителен до 7.10.2014 г., БелГИСС;
 - Сертификат №051/11Т, 20.07.11г., LucatronAG (Германия); Сертификат №2011-QC, 03.12.2012 г., SMART-Home(США), Сертификат BiampSystems (США).

Производство: торговое оборудование, витрины, прилавки, мебель под заказ клиента.

Услуги: центр обслуживания кассовых аппаратов, ремонт кассовых аппаратов, монтаж видеонаблюдения, ОПС, СКУД, автоматизация торговли и услуг, озвучивание помещений.

Поставка: системы видеонаблюдения, сканеры штрих-кода, терминалы сбора данных, противокражное оборудование, кассовое оборудование, весовое оборудование, счетчики банкнот, детекторы валют, видеодомофоны, переговорные устройства, активные микрофоны, торговое оборудование, этикет-пистолеты, принтеры этикеток, программное обеспечение для автоматизации торговли и сферы услуг, оборудование для автоматизации дома, гостиницы, офиса.

Выполненные проекты: сеть магазинов «Оптика-24», сеть магазинов «Парфюмстандарт», сеть салонов «Интеркомпьютерсервис», сеть магазинов «Парничок», автосалон «Субару», Сеть аптек по Беларуси более 26 шт., сеть магазинов «Космо», сеть салонов «Евросеть» и др.

Дистрибьютор компаний: LucatronAG (Германия), SMART-Home (США), GoDEX (Тайвань), CapherLab (Тайвань), Vangold (Китай), ZKSoftwera (Китай), Protech (Тайвань), Planet (Тайвань), ОАО «КЗТА» (РФ), Fiscat (Китай).
 Дополнительная информация: участие в выставках Tibo, HoReCa&RetailTech и др.

РОВАЛЭНТКОМПЛЕКС, ООО



223056, Минская обл., Минский район, пос. Юбилейный, ул. Луговая, 11
Тел./факс: (017) 506-21-52, 510-23-27 (сбыт), 510-23-26, (029) 777-75-90 МТС, (029) 350-17-77 VELCOM
E-mail: support@rovalant.by, support@rovalantcomplex.com
Сайт: www.rovalantcomplex.com, www.rovalant.by, www.autoparking.by
Год основания: 1994
УНП: 190832170

Контактные лица: Петлицкий Александр Вячеславович, заместитель директора по технике.

Лицензии:

- лицензия на право осуществления охранной деятельности № 02010/16668, действительна по 25 октября 2022г., выдана Министерством внутренних дел Республики Беларусь;
 - лицензия на право осуществления деятельности по обеспечению пожарной безопасности № 02300/1526, действительна по 26 декабря 2017г., выдана Министерством по чрезвычайным ситуациям Республики Беларусь.

Сертификаты:

- № BY/112 02.01. 033 00201, срок действия с 07.10.2013 по 06.10.2018, выдан Учреждением «Республиканский центр сертификации и экспертизы лицензируемых видов деятельности» Министерства по чрезвычайным ситуациям Республики Беларусь;
 - № BY/112 03.03. 023 00480, срок действия с 10.10.2011 по 10.10.2016, выдан Органом по сертификации технических средств охранно-пожарной сигнализации;
 - № BY/112 02.01. 033 00156, срок действия с 17.07.2013 по 16.07.2018, , выдан Учреждением «Республиканский центр сертификации и экспертизы лицензируемых видов деятельности» Министерства по чрезвычайным ситуациям Республики Беларусь;
 - № BY/112 03.03.033 00306, срок действия с 29.05.2009 по 29.05.2014, выдан Учреждением «Республиканский центр сертификации и экспертизы лицензируемых видов деятельности» Министерства по чрезвычайным ситуациям Республики Беларусь;

чайным ситуациям Республики Беларусь;

- № BY/112 03.03.033 01917, срок действия с 16.12.2010 по 15.12.2015, выдан Учреждением «Республиканский центр сертификации и экспертизы лицензируемых видов деятельности» Министерства по чрезвычайным ситуациям Республики Беларусь;
 - № BY/112 03.03. 023 00111, срок действия с 13.07.2009 по 09.07.2014, выдан Органом по сертификации технических средств охранно-пожарной сигнализации.

Производство:

- СИСТЕМА АВТОМАТИЗИРОВАННОЙ ПАРКОВКИ 777 «КОМПЛЕКСПАРКИНГ»;
 - ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННО-ПОЖАРНЫЕ ПРИБОРЫ СЕРИИ «А»;
 - СИСТЕМА УПРАВЛЕНИЯ ОПОВЕЩЕНИЕМ ОЗВУЧИВАНИЕМ И ЭВАКУАЦИЕЙ «ГОНГ»;
 - АДРЕСНО-АНАЛОГОВАЯ СИСТЕМА ПОЖАРНОЙ СИГНАЛИЗАЦИИ АСПС «БИРЮЗА»;
 - ИНТЕГРИРОВАННАЯ СИСТЕМА ОХРАНЫ «777».

Услуги:

- техническое обслуживание;
 - ремонт приборов.

Поставка:

- СИСТЕМА АВТОМАТИЗИРОВАННОЙ ПАРКОВКИ 777 «КОМПЛЕКСПАРКИНГ»;
 - ПРИЕМНО-КОНТРОЛЬНЫЕ ОХРАННО-ПОЖАРНЫЕ ПРИБОРЫ СЕРИИ «А»;
 - СИСТЕМА УПРАВЛЕНИЯ ОПОВЕЩЕНИЕМ ОЗВУЧИВАНИЕМ И ЭВАКУАЦИЕЙ «ГОНГ»;
 - АДРЕСНО-АНАЛОГОВАЯ СИСТЕМА ПОЖАРНОЙ СИГНАЛИЗАЦИИ АСПС «БИРЮЗА»;
 - ИНТЕГРИРОВАННАЯ СИСТЕМА ОХРАНЫ «777».

Выполненные проекты:

- РУП «НАЦИОНАЛЬНЫЙ АЭРОПОРТ МИНСК»;
 - АСБ «Беларусбанк».

Дистрибьютор компаний: ITV, Samsung.

Смарт Бизнес Технолоджи, ООО



223053, Минский р-н, д Боровая, 3 АБК
Тел./факс: (017) 510-94-09
E-mail: smartbt@mail.ru
Сайт: www.smartbt.by
Год основания: 2005
УНП: 691581574

Контактные лица: Макейчик Александр Николаевич, заместитель директора.

Услуги: обслуживание и ремонт банковского оборудования.

Поставка: банковское оборудование, одноразовые сигнальные устройства, одноразовый пломбирующий материал.

Дистрибьютор компаний: ООО «Силтек» Россия.

Совершенные системы, ООО



223051, Минский р-н, а/г Колодищи, ул. Короткая, д. 8, комн. 31
Тел./факс: (017) 508-23-33, (029) 370-20-22
E-mail: info@soversys.by
Сайт: www.soversys.by
Год основания: 2009
УНП: 191152890

Контактные лица:

- Рябов Павел Анатольевич, зам. директора;
 - Каравай Андрей Сергеевич, Главный инженер проекта.

Лицензии:

- лицензия МВД на право осуществления деятельности по обеспечению безопасности юридических и физических лиц № 02010/12812 сро-

ком действия до 15 июля 2015 г.;

- лицензия МЧС на право осуществления деятельности по пожарной безопасности № 02300/2912 сроком до 27.01.2018 г.

Услуги:

Проектирование, монтаж, наладка и техническое обслуживание средств и систем охраны и пожарной сигнализации. Поставка, проектирование и настройка оборудования для сетевой инфраструктуры предприятий.

Поставка:

- видеокамеры (Soversys, Pelko, Hikvision, ACTi, D-link);
- видеорегистраторы (Trassir, Soversys, Hawell, Hikvision, ACTi);
- аксессуары для видеонаблюдения (Hawell);
- СКУД (контроллеры и ПО «Сфинкс», турникеты «Ростов-Дон»);
- источники бесперебойного питания (APC);
- серверное оборудование (IBM, HP);
- сетевое оборудование (D-link, Cisco).

Выполненные проекты: ОАО «Белорусский Народный банк», ЗАО Банк ВТБ (Беларусь), ЗАО «БелСвиссБанк», Иностранное частное предприятие «Индастриал Транзит», Отдел образования, спорта и туризма Минского райисполкома, Управление образования администрации Октябрьского р-н г. Минска, БРУСП «Белгосстрах», РУП «Аэропорт Минск-1», ИП «ЛУКОЙЛ-БЕЛОРУССИЯ», РУП «Белоруснефть-Минскавтозаправка», ООО «БМЕ Бизнес Центр», ООО «Бел-Прибалт», СЗАО «ПИНСКДРЕВ-ПИНВУД», ОАО «Белшина», ЗАО «Выставочный центр АКВАБЕЛ», ООО «ЗАВОД ВИНОГРАДНЫХ ВИН «ДИОНИС», ООО «Нестле Россия», ИП «Интерфакс-Запад», ООО «Альторос Девелопмент», ООО «ДМИТРИЕВ КИРМАШ», ООО «МедиаСистемаИнтер», ЗАО «Универсам Первомайский», ОАО «Гипросвязь», ООО «Монлибон», ООО «Эксист», Национальная Академия Наук Беларуси, ГНУ «Институт порошковой металлургии», Юридический колледж БГУ, ОАО «СветлогорскХимволокно».

Дистрибьютор компаний: ACTi, Pelko, Сфинкс, Trassir, Hawell.

Спецэлектро Лтд, ООО



220026, г. Минск, ул. Корицкого, 3-1Н

Тел./факс: (017) 295-22-12, 295-43-34, 295-77-92

E-mail: info@spetselectro.by

Сайт: www.spetselectro.by

Год основания: 1992

УНП: 100080014

Контактные лица: Самарин Виктор Иванович, генеральный директор.

Лицензии:

- лицензия на право осуществления охранной деятельности № 02010/1968 от 27.02.2009 г., выдана Министерством внутренних дел Республики Беларусь действительна до 08.04.2014;
- лицензия на право осуществления деятельности по обеспечению пожарной безопасности № 02300/528 от 29.01.2010 г., выдана Министерством по чрезвычайным ситуациям Республики Беларусь, действительна до 26.02.2015.

Сертификаты: около 50 сертификатов (серийное производство) на поставляемую продукцию.

Производство:

- извещатель охранный оптико-электронный пассивный Vi-motion; прибор приемно-контрольный охранный «СЭТ-4АД»; адаптер «Маэстро».

Услуги:

- проектирование, монтаж, наладка, техническое обслуживание комплексных систем безопасности;
- поставка оборудования охранный, пожарной сигнализации, контроля доступа, видеонаблюдения, противокражных систем, контроля кассовых операций.

Поставка: более 100 наименований импортной продукции.

Выполненные проекты: Национальный банк Республики Беларусь, ОАО «АСБ Беларусбанк», ОАО «Приорбанк», Белбизнесбанк, банк «Зо-

лотой талер», Беларусский народный банк, РРБ-Банк, Инфобанк, Внешэкономбанк, банк «Москва-Минск», Главное управление «Дипсервис», Главное хозяйственное управление УД Президента Республики Беларусь, Национальный художественный музей Республики Беларусь, Верховный суд Республики Беларусь, БелГИЭ, Управление юстиции Мингорисполкома, Управление образования Мингорисполкома, РУП «Гомельэнерго», ТЭЦ-3, Госкомавиации, Министерство здравоохранения Республики Беларусь, Мобильная цифровая связь, фабрика «Модум», Заславский замок, СООО «Табак-инвест», ОАО «Декорум», СООО «Паркинг плюс», ТЦ «Аквабел», «Престон-маркет», универсам «Сторожевский», гипермаркеты «Простор», гипермаркеты «Гиппо» в Минске, г. Могилеве и г. Гомеле, ТЦ «Бонус» и др.

Дистрибьютор компаний: Tyco International, Visonic, Panasonic, GeoVision, Notifier Italia, by Honeywell, System Sensor, Ramcro S.r.l, Паритет.

Сфератрэйд, ОДО



220118, г. Минск, ул. Машиностроителей, 29-117

Тел: (017) 341-50-50, (029) 641-50-50 Velcom, (029) 541-50-50 МТС

E-mail: info@secur.by

Сайт: www.secur.by

Год основания: 1995

УНП: 100972915

Контактные лица: Малаховский Денис Святославович, директор.

Лицензия: № 02300/50 на право осуществления деятельности по обеспечению пожарной безопасности, выдана МЧС РБ, действительна до 10.02.2016 г.

Услуги:

- технические консультации по вопросам обеспечения безопасности любого уровня сложности;
- обследование и экспертная оценка состояния технических средств безопасности на объектах административного, производственного и других назначений;
- составление технического задания и проекта;
- поставка оборудования;
- гарантийное и послегарантийное обслуживание поставляемого оборудования.

Поставка:

- IP и CCTV-системы видеонаблюдения;
- системы контроля и управления доступом;
- системы охранно-пожарной сигнализации;
- системы защиты товаров от краж;
- системы аварийного оповещения и звуковой трансляции;
- сопутствующие материалы для монтажа и др.

Дистрибьютор компаний: AXIOM, MOBOTIX AG (Германия), SALTO Systems S.L. (Испания), LG Electronics (Южная Корея), Truen (Южная Корея), ZAVIO Inc. (Тайвань), NUUO (Тайвань), Roger (Польша), KT&C (Южная Корея), Fujifilm (Япония), Pinetron Co (Южная Корея), GSN Electronic (Израиль), Rielta (ПФ), LOB (Польша), Elmes Electronic (Польша), QUIKO (Италия), JIS (Испания), PERCo (ПФ), ITV\AxxonSoft (ПФ), JSB Systems (ПФ), AccordTec (ПФ), Elesta (ПФ), Bolid (ПФ) и др.

Техноцентр, ЗАО



220004, г. Минск, ул. Короля, д. 9, к 4 (второй этаж)

Тел./факс: (017) 299-55-55

E-mail: office@techno-centre.com

Сайт: www.techno-centre.com

Год основания: 1997

УНП: 101295470

Контактные лица: Германович Павел Сергеевич, директор.

Лицензии:

- Лицензия № 02300 849 (деятельность по обеспечению пожарной безопасности) выдана на основании решения от 9 апреля 2004 г № 2 км. Срок действия продлен на 5 лет, согласно решения от 17 марта 2009 г № 6 км. Министерство по чрезвычайным ситуациям Республики

Беларусь.

- Лицензия № 0210/0528620 (на обеспечение безопасности юридических и физических лиц). Выдана на основании решения от 15 мая 2009 г № 18 км Министерством внутренних дел Республики Беларусь, действительна до 25 июня 2014 года.

Производство: телекамеры, шлагбаумы, болларды.

Услуги: ремонт мониторов ViewSonic, поставка и монтаж систем безопасности.

Поставка: СНВ, ОПС, СКД, противокражные системы, металлодетекторы, блоки питания, домофоны, аксессуары систем безопасности.

Выполненные проекты: большое количество различных проектов в сфере обеспечения пожарной и охранной безопасности в Республике Беларусь.

Дистрибьютор компаний: Sony, AXIS, ISS.

Унибелус, СП ООО



UNIBELUS

220033, г. Минск, ул. Нахимова, 10

Тел./факс: (017) 291-15-05, 230-72-40

E-mail: info@unibelus.com

Сайт: www.unibelus.by

Год основания: 1994

УНП: 100834637

Контактные лица: Белова Ольга Владимировна, генеральный директор.

Производство: система трансляции и оповещения о пожаре «АРИЯ».

Услуги: от консультации и проектирования до пусконаладочных работ и последующего сервисного обслуживания всех слаботочных сетей.

Поставка: систем пожарной сигнализации, трансляции и оповещения, конференц-связи и синхронного перевода, видеонаблюдения, контроля доступа, пожаротушения, профессионального озвучивания, охраны периметра, мультимедийных систем, локально-вычислительных сетей, охранной сигнализации, противокражной системы, системы диспетчеризации, телефония, часофикация, радиофикация, система автоматизации, комплексные интегрированные системы безопасности, системы управления и контроля инженерными сетями зданий.

Дистрибьютор компаний: Arecont Vision (США), Cisa (Италия), Технос-М+ (Россия), CEM Systems Great (Северная Ирландия), Autec (Германия), Openers&Closers (Испания), Aiphone (Япония), Green Center (Чехия), Samsung Techwin (Ю. Корея), JVC Professional Europe (Германия), CBC (Ganz, Computar), AVerMedia Information (Тайвань), Win4net (Ю. Корея), Daiwon Optical (Ю. Корея), Тахион (Россия), TOA (Япония), Tasker (Италия), JTS (Тайвань), DNH (Норвегия), CISCO (США), SRS (Украина), Эталон (Россия), OT-Systems (Гон Конг), КОМКОМ (Россия), Girikond (Россия), Isaberg Rapid (Швеция), Lantech (Тайвань), PELCO (Россия), AV Tech Corporation (Тайвань), Cominfo A.S. (Чехия), Enhance Technology GmbH (Германия), HID Global (Великобритания), Instek Digital Co., Ltd (Тайвань), Lantech Communications Global, Inc. (Тайвань), Mattig-Schauer GmbH (Германия), BFT (Италия), Etrovision (Тайвань), ТД «Паритет» (Россия), Полисервис НПФ ООО (Россия), РостЕвроСтрой (Россия), Ризлта (Россия), ТЕКО (Россия).

Фабрика турникетов и систем, Частное Предприятие



220014, г. Минск, ул. Малая, д. 1, оф. 1

Тел./факс: (017) 508-77-88, 508-77-55

E-mail: mail@turniket.info

Сайт: www.turniket.info

УНН: 191690318

Контактные лица: Елаго Вадим Николаевич, зам. директора по маркетингу.

Производство: турникеты, системы контроля доступа и учета рабочего времени.

Услуги: Производство турникетов-триподов, ограждений, электромеханических, механических и автоматических калиток, систем контроля доступа и учета рабочего времени, разработка ПО.

Поставка: биометрические терминалы контроля доступа.

Выполненные проекты: оборудование установлено более чем на 1000 предприятиях Республики Беларусь и более чем на 300 предприятиях РФ.

ЭРВИ групп, ООО



121471, г. Москва, ул. Рябиновая, д. 45А, стр. 24

Тел./факс: (495) 735 38 47; (495) 735 38 57

Сайт: www.rvi-cctv.by

Год основания: 2007

ОГРН: 1086454000643

ИНН: 6454088952

КПП: 772901001

Контактные лица:

- Рыжков Алексей Владимирович, директор;
- Голубев Антон, руководитель отдела ВЭД.

Производство: полный комплекс продукции для CCTV и IP-видеонаблюдения:

- сетевые камеры видеонаблюдения;
- IP-видеорегистраторы (NVR);
- автономные цифровые видеорегистраторы с сетевыми возможностями;
- аналоговые видеокамеры с цифровой обработкой изображения;
- объективы для видеокамер;
- профессиональные мониторы видеонаблюдения;
- термокожухи;
- видеодомофоны;
- источники питания.

Услуги: поставка (продажа) оборудования, разработка, проектирование и послепродажное обслуживание.

Оборудование в проектах (наиболее значимые):

- Безопасный город Москва (более 40 000 видеокамер в местах массового скопления людей, дворовых территорий, подъездов, площадей, парков и т.д.);
- Государственная программа «Безопасный город»: г. Краснодар, г. Архангельск, г. Астрахань, г. Мурманск, г. Тюмень;
- Безопасный автобус, г. Москва («Мосгортранс», более 4000 автобусов);
- Безопасная школа: 1570 школ по Москве, 67 школ в Хабаровском крае, 51 школа в Сахалинской области, 37 школ в Республике Башкортостан, 50 школ в Воронежской области;
- Более 20 объектов здравоохранения г. Москвы, в том числе Московский родильный дом №17, Клинический родильный дом (г. Астрахань);
- Спецтранспорт МВД: ЦСН, ГИБДД, ППС (более 3000 автомобилей);
- более 1800 а/м инкассации Сбербанка РФ;
- ФСИН: более 400 автозак;
- более 30 отделений «Сбербанка» РФ (филиалы в городах Москва, Северо-Кавказский ФО, в Астраханской, Саратовской, Белгородской, Калужской, Брянской, Владимирской, Архангельской областях и Краснодарском крае);
- более 40 отделений «ГазЭнергоБанк» в Калужской области;
- Банк «Зенит» (обеспечение системами видеонаблюдения инкассаторских а/м);
- «Газпромбанк» (обеспечение системами видеонаблюдения инкассаторских а/м);
- «Банк Москвы» (обеспечение системами видеонаблюдения инкассаторских а/м).

Дополнительная информация:

«ЭРВИ групп» – это группа управленцев, разработчиков и технических специалистов, деятельность которых направлена на создание более совершенных и адаптированных под задачи государства продуктов, обеспечивающих безопасность, как граждан России, так и различных объектов недвижимости.

**2-х мегапиксельная уличная телекамера
с отличным соотношением цена / качество!**

GCI-K1526TH



Розничная цена 6 350 000 руб. без НДС

- цифровая система шумоподавления (3D+2D DNR)
- режим "день/ночь" (механический ИК-фильтр)
- 1/2.7" CMOS, 2 Megapixel,
- ИК подсветка до 25 м (71°);
- Full HD 1080p/ SXGA/ HD 720p/ XGA/SVGA/ 4CIF/ VGA/ CIF - 25 кадр/с;
- встроенный объектив f=3-9 мм, Auto Iris (DC);
- цифровой zoom, Баланс белого, BLC, WDR, детектор движения, Privacy Zones,
- разъем для Micro SD/SDHC карт (до 32Gb),
- 12V DC/ 24V AC/ PoE,
- IP66, -35°...+50°

Гарантия 36 месяцев

Видеонаблюдение немецкого качества - от Grundig

FOR A GOOD **REASON**
GRUNDIG



Для получения более подробной информации посетите
www.grundig-security.com

Официальный дистрибьютор в Республике Беларусь - компания «АльфаСистемы»
г. Минск, Логойский тракт 22а, офис 207
Тел./факс: (+375 17) 262 84 64, 268 05 36 / 265 12 59
info@cctv.by www.cctv.by

УНП 190598104



DIGIEVER

Все функции в одном устройстве DIGISTOR NVR

Совершенное сетевое видеонаблюдение с поддержкой разрешения Full HD и высоким качеством записи

- Поддержка функции мониторинга, удаленного мониторинга через веб-браузер и приложения на базе iOS и Android
- Разработан на базе стабильной и безопасной ОС Linux
- Интуитивно понятный интерфейс для мультиканального воспроизведения
- Быстрая настройка всего в 5 простых этапов
- Надежное управление привилегиями пользователей
- Управление различными происходящими событиями
- Продвинутое управление RAID дисками с возможностью их горячей замены
- Встроенный GPIO порт* (4 цифровых входа и 2 выхода)



УНП 100034037



СП «Унибелус» ООО официальный представитель DIGIEVER в Республике Беларусь
220033, Беларусь, г. Минск, ул. Нахимова, 10
Тел.: (017) 291 15 05, Факс: (017) 230 72 40
GSM: (029) 7777 230, (029) 608 15 05
www.unibelus.by

