

Журнал для руководителей предприятий и специалистов отрасли безопасности

№3 (30)
май - июнь
2013

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ



Средства и системы охраны в Республике Беларусь

Новые разработки нормативной базы
по производству, обслуживанию, технадзору ТСнСО

Организация физической безопасности
охраняемых объектов

Обзор средств и систем безопасности

выставка
форум
2013

Центр
безопасности
«Инженерно-техническая
безопасность»

Информационная безопасность

Вопросы комплексной защиты информации:
современный подход

Основные тренды развития телекоммуникаций,
информационного пространства и ЗИ в РБ





Не требует доказательств



Оборудование видеонаблюдения

ОДО "Сфератрэйд"
ул. Машиностроителей 29-117, Минск 220118 Беларусь
www.axiom.by

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

НОВОСТИ ОТРАСЛИ

Выставка-форум «Центр безопасности 2013: инженерно-техническая безопасность»4

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ И СИСТЕМ ОХРАНЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Новые разработки нормативной базы по производству, обслуживанию, технадзору технических средств и систем охраны6
Саков Евгений Евгеньевич, заместитель начальника отдела, начальник отделения эксплуатации управления средств и систем охраны Департамента охраны МВД Республики Беларусь

Организация физической безопасности охраняемых объектов8
Щипакин Артем Федорович, старший инспектор по особым поручениям отделения организации физической охраны объектов

Перспективы развития средств передачи извещений охранной сигнализацией для работы по сетям Ethernet 11
Шелютю Дмитрий Эдуардович, зам. гл. конструктора «АЛАРМ» НТ ЗАО

ОБЗОР СРЕДСТВ И СИСТЕМ

Реализация проектных решений на базе оборудования «Болид» 14
ЗАО НВП «Болид»

Активная система безопасности на воде E-Rescue 16
ООО «Инновационная компания «INTES»

Интеграция системы видеонаблюдения и системы контроля доступа на примере TRASSIR и СФИНКС 18
ООО «Совершенные системы»

Требования к совершенной системе видеонаблюдения. 21
Гапошин Валерий, инженер техподдержки, MICRODIGITAL Inc.

Компания ITV | АххонSoft представляет новые версии программного продукта АххонNext 23
ООО «АксонСофт»

Новые технологии компании Hikvision Digital Technology – обзор новинок 2013 года. 24
Сергей Чень, ведущий технический специалист Hikvision Digital Technology

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Вопросы комплексной защиты информации: современный подход 27
Барановский Олег Константинович, заместитель начальника по науке центра испытаний средств защиты информации и аттестации объектов информатизации Государственного предприятия «НИИ ТЗИ»

Цифры конференции, перспективные направления докладов XVIII научно-практической конференции «Комплексная защита информации» 29
Маликов Владимир Викторович, начальник цикла технических и специальных дисциплин УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь, к.т.н., подполковник милиции.

Основные тренды развития телекоммуникаций, информационного пространства и защиты информации в Республике Беларусь 31
Капариха Сергей Николаевич, Оперативно-аналитический центр при Президенте Республики Беларусь, заместитель начальника центра

Значение и результаты развития информационно-коммуникационных технологий в Беларуси 33
Капариха Сергей Николаевич, Оперативно-аналитический центр при Президенте Республики Беларусь, заместитель начальника центра

Symantec Technology Day 2013 35
Кочнев Алексей Михайлович, менеджер по развитию бизнеса корпорации Symantec в Республике Беларусь

СПРАВОЧНАЯ ИНФОРМАЦИЯ

Информация о компаниях. 37

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»

Производственно-практический журнал
№3 (30), май-июнь, 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) (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 59500 бел. руб. без НДС,
на основании п. 3.12 ст. 286
Особенной части Налогового Кодекса
Республики Беларусь

Подписано в печать — 21.03.2013 г.

Формат: 60х90 1/8

Бумага офсетная

Гарнитура Myriad Pro. Печать офсетная

Усл. печ. л. 5; Уч.-издл. 5,4

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

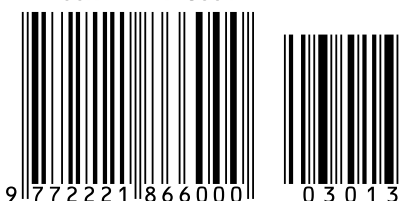
Издатель не несет ответственности за
достоверность рекламных материалов.

*Воспроизведение материалов, опубликован-
ных 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 июне состоялось знаменательное событие для нашей компании – мы открыли новую информационную площадку для специалистов отрасли безопасности Беларуси выставку-форум «Центр безопасности: инженерно-техническая безопасность, 2013».

Работая в своем информационном поле, мы прекрасно понимаем потребности в донесении актуальной информации до потребителей, ищем способы эффективно предоставить информацию пользователям. Могу с уверенностью заявить, что сегодня ни один канал коммуникации в этом деле не является основным. Продвижение должно быть комплексным и эффективным. Работает все в комплексе: и личные встречи, и интернет, и журнал. Теперь к эффективным средствам продвижения продуктов по безопасности в Беларуси добавилась выставка-форум.

Сегодня мало продать продукт, рынок требует технической поддержки, системы становятся более сложными. Поэтому на первый план выходят компетенции и уровень знаний, как продавца, так и проектировщика, инсталлятора. Одна из заявленных задач прошедшего мероприятия – повышение профессиональной квалификации специалистов отрасли безопасности посредством формирования качественной деловой программы. Видео выступлений и докладов будет размещено на сайте aercom.by

Судя по отзывам участников и посетителей выставки, задачи по продвижению и информационному насыщению решены эффективно и качественно. Началась подготовка следующей выставки-форума «Центр безопасности: инженерно-техническая безопасность, 2014». Задачи следующего года: больше новых технологий, решений, больше уникальных экспертных выступлений.

Благодарим всех участников за интерес, проявленный к мероприятию. Спасибо специалистам Департамента охраны за программную поддержку выставки-форума.

Мы продолжаем работу над созданием национальных информационных площадок. Под брэндом «Центр безопасности» в ноябре 2013 г. состоится выставка-форум «Методы и системы защиты информации, информационная безопасность – 2013».

Основная тематика выставки-форума связана с рассмотрением вопросов нормативно-правового, организационного и технического обеспечения информационной безопасности по разделам: техническая, криптографическая защита информации, разработка, внедрение, аттестация систем безопасности и систем защиты информации, обеспечение информационной безопасности банковско-финансовой сферы. Приглашаем к участию профильные компании и специалистов.

Главные темы следующего номера журнала «Технологии безопасности» №4(31), июль-август, 2013 «Пожарная безопасность. Системы видеонаблюдения».

В номере:

- Технические регламенты Таможенного союза;
- Взрывозащита – классификация, новые методы определения категорий объектов по взрывопожарной и пожарной опасности при проектировании, с учётом нового ТКП 474-2012;
- Обзор средств и систем противопожарной безопасности;
- Обзор средств и систем сегмента СВН.

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

**СПЕЦИАЛИЗИРОВАННАЯ СЕКЦИЯ
В РАМКАХ КРУПНЕЙШЕЙ ВЫСТАВКИ
ПО БЕЗОПАСНОСТИ В РОССИИ И СНГ!**

15 – 18 апреля 2013 года

Москва, ВВЦ, 75 павильон

ufi
Approved
Event

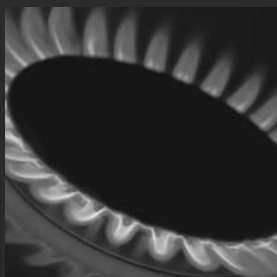
Mips
O S C O W

с 2013 года на ВВЦ!



**ПОЖАРНАЯ БЕЗОПАСНОСТЬ.
АВАРИЙНО-СПАСАТЕЛЬНАЯ ТЕХНИКА.
ОХРАНА ТРУДА**

1010010111110101010010101010
0101111111010100101010101010010100101111101010100101010
111111101010100101010101010010100101111101010100101010
10101000010101010010101010101001000001011111010100101010101001001001001010101010
0010111110101010010101010101001010010000010111110101001010101010010100101111101010100101010



- системы аварийно-пожарного оповещения
- автоматические системы пожаротушения
- системы жизнеобеспечения
- приборы приемно-контрольные пожарные
- извещатели пожарные
- огнетушители пожарные
- огнетушащие вещества

- огнезащитные и взрывозащитные материалы
- пожарная автоматика, роботы
- пожарный инвентарь и оборудование
- аварийно-спасательное оборудование
- спецодежда

Организатор:



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

При поддержке:



МВД России

Генеральный
партнер выставки:

BOLD
СИСТЕМЫ БЕЗОПАСНОСТИ

www.mips.ru

Национальная выставка-форум «Инженерно-техническая безопасность»

5 июня, 2013



Выставка-форум «Центр безопасности 2013: инженерно-техническая безопасность»

Журнал «Технологии безопасности», при программной поддержке Департамента охраны МВД и технической поддержке инновационной компании «ИНТЕС», 5 июня 2013 г. провел 1 Национальную выставку-форум «Центр безопасности 2013: инженерно-техническая безопасность». Выставка состоялась в Национальном выставочном центре «БелЭкспо». г. Минск, ул. Я. Купалы, 27.

Говоря об итогах мероприятия можно констатировать, что в Беларуси создана новая эффективная информационная площадка для профессионалов отрасли безопасности, благодаря которой будет происходить продвижение продуктов, технологий и повышение квалификации специалистов.

Как и было запланировано, мероприятие носило сугубо деловой и практический формат. Выставка-форум структурно состоит из 2 частей – непосредственно выставки и деловой программы. В стендовой работе приняло участие 20 компаний и организаций, представляющих различные направления отрасли безопасности. Был представлен ряд новых продуктов на рынке безопасности Республики Беларусь. Производители оборудования осуществили поддержку своих представителей, дистрибьюторов в стране, получили возможность прямого общения с целевой аудиторией – ключевыми фигурами профессиональных сегментов. Одним из важных результатов участия многие дистрибьюторы отмечают получение более глубокого понимания национального рынка.

В рамках деловой программы состоялся 21 доклад с презентациями новинок оборудования или затрагивающий проблематику отрасли безопасности.

Видео выступлений и докладов будет размещено на сайте aercom.by и на сайте выставки cb.aercom.by. Таким образом, выставка-форум предоставляет самый короткий доступ к базам знаний, оказывает помощь в приобретении современных навыков в привязке к профессиональной среде, сокращает время на подбор, анализ, выбор оборудования специалистами отрасли безопасности.

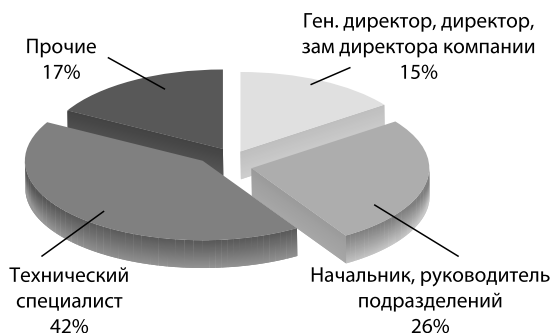
Статистика посетителей.

Выставку посетило около 500 представителей отрасли безопасности различного профессионального состава.

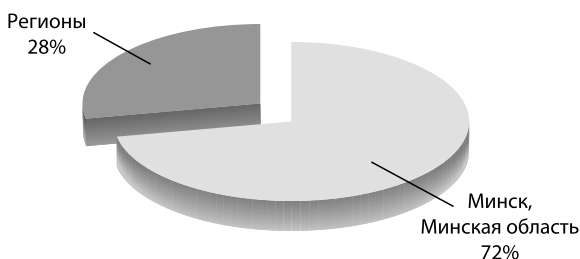
2-я выставка-форум «Центр безопасности 2014: инженерно-техническая безопасность» состоится 5 июня 2014 г.

Из планов на 2014 год. Общая тенденция – новые, проблемно-ориентированные решения. Достигнуты предварительные договоренности об участии в мероприятии представителей ведущих мировых брендов по СВН. Планируется: раздел Пожарная безопасность, создание демо-зон.

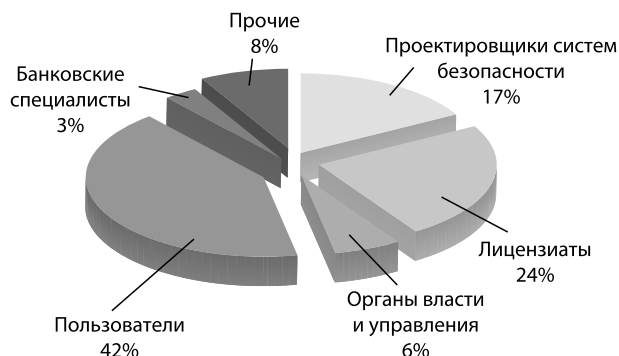
Должностной состав



Региональный состав



Профессиональная деятельность



Приглашаем экспертов в программный комитет мероприятия, ищем технических партнеров для создания демо-зон.

Благодарим всех участников и посетителей за поддержку, до встречи на следующем мероприятии!



noVus®

Профессиональные решения для систем безопасности



РЕШЕНИЯ ПРОФЕССИОНАЛЬНОГО ВИДЕОНАБЛЮДЕНИЯ ДЛЯ БАНКОВСКИХ УЧРЕЖДЕНИЙ

- Многолетний опыт в области разработки решений для банковских учреждений
- Оборудование отвечающее самым высоким требованиям безопасности
- Профессиональное программное обеспечение для мониторинга банковских филиалов
- Сертифицированное обучение операторов системы
- Оказание профессиональной технической поддержки



Дистрибьюторы оборудования NOVUS® в Беларуси:



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



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

НАДЕЖНОСТЬ И ФУНКЦИОНАЛЬНОСТЬ

RVi

НОВЫЕ IP-КАМЕРЫ RVi

Купольная
RVi-IPC33WDN



Антивандальные
RVi-IPC31VDN
RVi-IPC32VDN
RVi-IPC33WVDN



В стандартном
исполнении
RVi-IPC23WDN



Уличная
RVi-IPC43WDN



WDR

RVi-IPC33WDN, RVi-IPC33WVDN, RVi-IPC23WDN, RVi-IPC43WDN

ОБЪЕКТЫ ДЛЯ
ПРИМЕНЕНИЯ
IP-КАМЕР



12^Я МЕЖДУНАРОДНАЯ ВЫСТАВКА

HI-TECH BUILDING

www.hitechbuilding.ru

29-31 октября

2013

Экспоцентр

■ ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ:

- ВИДЕОНАБЛЮДЕНИЕ
- ОХРАННОЕ ТЕЛЕВИДЕНИЕ
- КОНТРОЛЬ, УЧЁТ И УПРАВЛЕНИЕ ДОСТУПОМ
- ОХРАННО-ПОЖАРНАЯ СИГНАЛИЗАЦИЯ
- МОНИТОРИНГ СОСТОЯНИЯ ИНЖЕНЕРНЫХ КОНСТРУКЦИЙ

■ АВТОМАТИЗАЦИЯ ЗДАНИЙ

■ СИСТЕМЫ «УМНЫЙ ДОМ»

НАЦИОНАЛЬНАЯ ПРЕМИЯ
HI-TECH BUILDING
AWARDS

www.htb-awards.ru

Организатор

MIDexpo
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И ЯРМАРКИ

При поддержке





Новые разработки нормативной базы по производству, обслуживанию, технадзору технических средств и систем охраны



Саков Евгений Евгеньевич, заместитель начальника отдела, начальник отделения эксплуатации управления средств и систем охраны Департамента охраны МВД Республики Беларусь.

ТКП 472-2013 (02010) «Правила технического обслуживания технических средств охраны»; рабочий проект ТКП xxx-2013 (02010) «Системы охранной сигнализации. Правила производства и приемки работ», планируемый к реализации проект ТКП xxx-2014 (02010) «Технический надзор за выполнением работ по оборудованию объектов системами охраны».

До 01.05.2013 года основным документом для организаций, работающих в сфере технического обслуживания средств и систем охраны, руководящим документом являлся РД 25 964-90 «Система технического обслуживания и ремонта автоматических установок пожаротушения, дымоудаления, охранной, пожарной и охранно-пожарной сигнализации. Организация и порядок проведения работ» Министерства электротехнической промышленности и приборостроения СССР и ОСТ 25 992-82 «Система технического обслуживания установок пожаротушения, охранной и охранно-пожарной сигнализации. Виды контроля. Организация контроля».

В соответствии с требованиями Закона Республики Беларусь «О техническом нормировании и стандартизации» управлением средств и систем охраны Департамента охраны МВД Республики Беларусь был разработан и введен в действие технический нормативный документ ТКП 472-2013 (02010) «Правила технического обслуживания технических средств охраны».

Документ прошел все степени согласования, утвержден и введен в действие постановлением № 10 МВД Республики Беларусь от 11.01.2013 г., внесен в реестр государственной регистрации за номером 1442 от 28.01.2013 года.

Технический кодекс установившейся практики установил требования к порядку организации и проведения технического обслуживания технических систем охраны организациями, осуществляющими данный вид деятельности по спе-

циальным разрешениям (лицензиям).

Требования технического кодекса установившейся практики не отличаются от международного стандарта МЭК 839-1-4-88 Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Руководство по проектированию, монтажу и техническому обслуживанию и российского стандарта ГОСТ Р 50776-95 (МЭК 839-1-4-88), которые в разделе 9 предписывают проводить техническое обслуживание «периодически по установленной форме организациям и физическим лицам в соответствии с действующим законодательством».

Требования технического кодекса не распространяются на техническое обслуживание средств и систем охраны индивидуального пользования, а также на юридических лиц, для которых законодательством не предусмотрено получение специального разрешения (лицензии) на осуществление охранной деятельности в части технического обслуживания средств и систем охраны.

Основными задачами технического обслуживания средств и систем охраны являются:

- контроль технического состояния средств и систем охраны, полноты блокировки уязвимых мест системами охранной сигнализации, выполнения целевых задач СОТ, предусмотренных проектной документацией;
- проверка соответствия установки и регулировки технических средств охраны, входящих в состав систем охраны, их электрических параметров требованиям нормативно-технической и (или) конструкторской (проектной) документации;
- приведение установки, настройки и регулировки технических средств охраны, входящих в состав систем охраны, их электрических параметров требованиям нормативно-технической и (или) конструкторской (проектной) документации;
- ликвидация последствий воздействия на системы охраны внешних влияющих факторов;
- выявление и устранение причин отказов, произвольных срабатываний средств и систем охраны и устранение неисправностей при ремонтах по заявкам пользователей;

ТЕХНИЧЕСКИЙ КОДЕКС
УСТАНОВИВШЕЙСЯ ПРАКТИКИ

ТКП 472-2013 (02010)

ПРАВИЛА ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ
ТЕХНИЧЕСКИХ СИСТЕМ ОХРАНЫ

ПРАВИЛЫ ТЭХНІЧНАГА АБСЛУГОВАННЯ
ТЭХНІЧНЫХ СІСТЭМ АХОВЫ

- определение предельного состояния средств и систем охраны, при котором их дальнейшая эксплуатация становится невозможной или нецелесообразной;
- анализ и обобщение информации о техническом обслуживании средств и систем охраны;
- разработка мероприятий по совершенствованию форм и методов технического обслуживания средств и систем охраны.

Приобрести ТКП 472-2013 (02010) «Правила технического обслуживания технических средств охраны» на бумажном носителе Вы можете в областных (Минском городском) управлениях Департамента охраны МВД Республики Беларусь.

Рабочий проект ТКП ххх-2013

В настоящее время Департаментом охраны МВД Республики Беларусь разрабатывается технический нормативный документ ТКП ххх-2013 (02010) «Правила охранной сигнализации. Правила производства и приемки работ». Данный документ находится в стадии утверждения МВД Республики Беларусь, прошел все необходимые согласования в заинтересованных организациях. Электронный вариант рабочего проекта размещен на сайте Департамента охраны МВД Республики Беларусь в разделе «Законодательство», а также на сайте Государственного комитета по стандартизации Республики Беларусь в разделе «Проекты ТНПА».

Монтаж и наладка систем охранной сигнализации являются видом охранной деятельности, лицензируемой Министерством внутренних дел Республики Беларусь в соответствии с Законом Республики Беларусь «Об охранной деятельности в Республике Беларусь».

Ряд положений РД 28/3.007-2001* «Технические средства и системы охраны. Системы охранной сигнализации. Правила производства и приемки работ», регламентирующего правила монтажа, наладки и приемки в эксплуатацию систем охранной сигнализации в настоящее время, в связи с изменениями в законодательстве, устарели и требуют переработки, кроме того, замена руководящих документов на технические кодексы установившейся практики предусмотрена требованиями Закона Республики Беларусь «О техническом нормировании и стандартизации».

Технический кодекс установившейся практики распространяется на производство работ по монтажу, наладке и сдаче в эксплуатацию систем охранной и ручной тревожной сигнализации (далее – систем охранной сигнализации) объектов и устанавливает правила производства и приемки работ по монтажу и наладке систем охранной сигнализации.

Технический кодекс установившейся практики отражает требования, выработанные многолетней практикой монтажа и наладки технических систем охраны с учетом норм действующего законодательства Республики Беларусь, поэтому руководством управления средств и систем охраны Департамента охраны МВД Республики Беларусь принято решение о необходимости разработки и введения в действие в 2013 году.

Технический кодекс не распространяется на производство работ по монтажу, наладке и сдаче в эксплуатацию систем охранной сигнализации, применяемых физическими лицами для индивидуального пользования, а также систем охранной сигнализации объектов Службы безопасности Президента Республики Беларусь, Министерства обороны Республики Беларусь, Комитета государственной безопасности Республики Беларусь, Государственного комитета пограничных войск Республики Беларусь.

Требования настоящего технического кодекса являются обязательными для исполнения всеми юридическими лицами, осуществляющими деятельность по монтажу и наладке

систем охранной сигнализации по специальным разрешениям (лицензиям), а также юридическими лицами, которым в соответствии с законодательством не требуется получение специальных разрешений (лицензий) на данный вид деятельности.

Работы по монтажу систем охранной сигнализации должны производиться в соответствии с согласованным с областными (Минским городским) управлениями Департамента охраны МВД Республики Беларусь и утвержденным в установленном порядке проектом или актом обследования, технической документацией предприятий-изготовителей и настоящим техническим кодексом.

Отступления от проектов при монтаже систем охранной сигнализации не допускаются без согласования с проектной организацией, разработавшей проект, и областными (Минским городским) управлениями Департамента охраны Министерства внутренних дел Республики Беларусь, согласовавшими его.

При необходимости оборудования объекта ручной системой тревожной сигнализации, одного или нескольких смежных помещений системой охранной сигнализации, доблокировки уязвимых мест допускается проводить монтажные и наладочные работы по актам обследования, разработанным подразделениями Департамента охраны или организациями, имеющими специальные разрешения (лицензии) на право проектирования систем охранной сигнализации.

Допускается проводить монтажные и наладочные работы по актам обследования, разработанным организациями, имеющими специальные разрешения (лицензии) на монтаж и наладку систем охранной сигнализации, при условии согласования актов обследования с подразделениями Департамента охраны или их совместной разработкой.

Продолжение на стр. 10 →



КОМТИД

Производство
оборудования
для охранной
и пожарной
сигнализации

ООО «Комтид»
Минск, ул. Купревича, 1-3-241.
Тел.: +375-17-211-83-24

E-mail: comtid@tut.by
<http://www.comtid.com>
<http://www.comtid.by>

УНП: 101166264



Организация физической безопасности охраняемых объектов



Щипакин Артем Федорович, старший инспектор по особым поручениям отделения организации физической охраны объектов

В нашей работе мы постоянно сталкиваемся с проблемой противоправных посягательств на различные виды собственности (квартирные кражи, разбойные нападения на объекты банковской сферы, торговые организации). Одна из причин, по которой злоумышленникам удается осуществить противоправные действия в том, что субъекты хозяйствования, пытаясь защитить свое имущество, зачастую рассчитывают только на собственные силы или ограничиваются минимальными средствами из перечня услуг, предлагаемых Департаментом. К сожалению, такие меры по обеспечению безопасности оказываются ненадежными и малоэффективными.

В соответствии с Законом Республики Беларусь от 08.11.2006 г. №175-З «Об охранной деятельности в Республике Беларусь» Департамент охраны является структурным подразделением Министерства внутренних дел и имеет полномочия осуществлять функции в сфере охранной деятельности.

В Департаменте сложилась целостная система организации охраны объектов, подкрепляемая нормативными правовыми актами, формирующая единые требования к обеспечению безопасности.

Одной из основных задач Департамента охраны является повышение уровня защищенности охраняемых объектов, а также разработка в этом направлении новых организационных и технических решений.

На сегодняшний день, кроме технических средств и систем охраны Департамент располагает возможностью для организации физической охраны объектов (имущества) юридических и физических лиц, охране общественного порядка. Данный вид услуги осуществляется на договорной основе и реализуется как аттестованными сотрудниками, так и гражданским персоналом (сторожевая и военизированная охрана).

Порядок принятия объекта под охрану

Принятие объекта под охрану, в том числе и физическую, происходит в строго установленном порядке. На начальном этапе дается оценка категории объекта, подлежащего приему под охрану (например, дипломатические представительства, объекты органов государственного управления, объекты банковской сферы, учреждения здравоохранения, торговые организации), а также определяются потенциальные формы угрозы безопасности,

причем принимаются во внимание как внешняя, так и внутренняя категории угрозы. Исходя из данной оценки, дается заключение о целесообразности использования того или иного вида охраны.

В последнее время участились случаи силового воздействия на охраняемые объекты, несмотря на их хорошую техническую оснащенность (под силовыми воздействиями имеются ввиду разбойные нападения). Наличие поста физической охраны служит своеобразным барьером для преступного проникновения на охраняемый объект.

Процесс физической охраны

Физическая охрана – охрана объектов или их частей, осуществляемая сотрудниками, гражданским персоналом военизированной либо сторожевой охраны на стационарных или обходных постах. В большинстве случаев используется смешанный вид охраны, сочетающий в себе физическую охрану (как правило, в рабочее время объекта) и техническую (вне рабочего времени).

Численность сотрудников, необходимая для осуществления охраны объекта, устанавливается Департаментом охраны в порядке, определяемом нормативными правовыми актами МВД и локальными актами Департамента охраны.

Решение о принятии объекта под физическую охрану при-

по состоянию на 1 июня 2013 г. тариф 1 часа милицейской охраны в г. Минске составляет 55 288 руб., областных центрах – 51 783 руб., в других населенных пунктах – 50 684 руб.

нимается начальником подразделения охраны после оборудования объекта техническими средствами охраны и устранения недостатков по оснащению объекта инженерно-техническими средствами защиты.

К инженерно-техническим средствам защиты относятся: защитные кабины, двери, стекла, решетки, роллеты, замки, запирающие устройства, сейфы, механические ограждения и преграды (по СТБ1250-2000 Охрана объектов и физических лиц. Термины и определения).

Стационарные и (или) обходные посты при физической охране объектов (их частей) выставляются:

- по периметру охраняемых объектов (вдоль их границы в целях недопущения проникновения на их территорию лиц вне пропускных пунктов), редко используемые;
- на отдельных охраняемых объектах (внутри их и/или вблизи от них);
- смешанным способом (по периметру охраняемых объектов, внутри их и/или вблизи от них одновременно).

Охрана объектов – совокупность правовых, организационных, охранных, режимных и технических мер, осуществляемых уполномоченными на то органами и лицами в соответствии с законодательством, обеспечивающих защиту объектов (имущества) от несанкционированного доступа и противоправных посягательств (по СТБ1250-2000 Охрана объектов и физических лиц. Термины и определения).

Впервые на рынке Беларуси

ГАРАНТИЯ НАДЕЖНОСТИ И КАЧЕСТВА!



СервисСбытАвтоматика

Мы продаем безопасность

СТРЕЛЕЦ



220024, г. Минск,
ул. Стебенева, 12, офис 6

Отдел продаж:
(017) 380 20 21,
(044) 598 09 83,
(044) 598 19 80
Факс (017) 275 61 12

www.ssa101.by

Стрелец – Надежно, Просто, Удобно, Гарантировано!

Каждый Гражданин обязан думать и заботиться о своей личной безопасности, безопасности своей семьи, своего имущества (квартиры, загородного дома, дачи).

Каждый Руководитель обязан думать и заботиться о безопасности предприятия.

Беспроводная пожарно-охранная сигнализация СТРЕЛЕЦ – это надежная защита от несанкционированных проникновений (непрошенных гостей) и возгораний.

СТРЕЛЕЦ позволяет:

- избежать укладки ненужных проводов в квартире, доме, промышленном объекте;
- контролировать систему на любом удалении от места размещения (Вы получаете информацию о состоянии системы по GSM каналу);
- контролировать утечку воды и газа;
- подключать до 400 датчиков к одной системе;
- размещать датчики на удалении до 600 метров от блока управления;
- легко работать с системой, поскольку это не требует специальных навыков и знаний, в том числе при снятии системы для транспортировки (находка для арендаторов зданий и сооружений, а также граждан – Вы переезжаете, СТРЕЛЕЦ переезжает вместе с Вами);
- интегрироваться с любой проводной системой;
- управлять системой как при помощи пульта, так и при помощи компьютера.

220024, г. Минск,
ул. Стебенева, 12, офис 6

Отдел продаж:
(017) 380 20 21,
(044) 598 09 83,
(044) 598 19 80
Факс (017) 275 61 12

www.ssa101.by

№ BY/112 03.03 023 00307 № BY/112 02.01. 033 00027

Охраняемые объекты – здания, строения, сооружения или их части, жилые дома (помещения) граждан, участки местности, транспортные средства, перемещаемые (перевозимые) грузы, денежные средства и иные материальные ценности, физические лица, личное имущество физических лиц и другое имущество, подлежащие защите от противоправных посягательств подразделением охраны, в том числе с использованием технических средств и систем охраны.

Методы физической охраны

Физическая охрана объектов может осуществляться по обычному и/или караульному расчету. При организации физической охраны по обычному расчету (в зависимости от времени охраны и особенностей охраняемого объекта) предусматриваются, как правило, двухсменные или односменные посты.

При организации физической охраны по караульному расчету, на круглосуточный пост одновременно назначаются не менее двух сотрудников, а в исключительных случаях (по согласованию с управлением Департамента охраны) – три сотрудника на два поста, расстояние между центрами которых не превышает 500 метров, если эти посты имеют общую границу и одно общее караульное помещение. При наличии двух и более постов наряжаются караулы.

В задачи постового входит:

- предупреждение, выявление и пресечение преступлений и иных правонарушений на охраняемых объектах, в границе постов и маршрутов патрулирования;
- соблюдение строгого пропускного и внутриобъектового режимов, установленных на охраняемых объектах;
- принятие мер по поиску и задержанию на территории охраняемых объектов лиц, незаконно проникших на охраняемые объекты;
- организация обороны (защиты) при нападении.

Порядок передвижения постового (пешего патрульного) по территории поста (маршрута патрулирования) определяется с учетом его обязанностей, особенностей поста (маршрута патрулирования), оперативной обстановки, времени года, суток, иных факторов и отражается в карточке поста (карточке маршрута патруля).

Организация пропускного режима

Пропускной режим на охраняемом объекте определяется инструкцией об организации пропускного режима, подписанной руководителем заказчика и начальником подразделения охраны. Инструкции по использованию должны быть краткими, ясными и не должны противоречить нормам законодательства.

Пропускной режим – порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на охраняемые объекты (с охраняемых объектов), устанавливаемый заказчиком и подразделением охраны.

Персонал охраняемого объекта должен относиться с пониманием к выполнению должностных обязанностей постовых милиционеров и понимать, что безопасность – это коллективная ответственность.

Руководство объекта обязано обучить работников основам безопасности и требовать их соблюдения, убедить работников, что физическая безопасность – ответственность каждого.

Современная охрана объектов, в т.ч. физическая, немыслима без технической оснащенности, которая используется для организации системы контроля доступа, обнаружения проникновения, оценки ситуации при поступлении сигнала тревоги, задержки нарушителя, а также своевременной связи с силами реагирования. На охраняемых объектах используются следующие виды оборудования, каждый тип технологии, используе-

Заказчик должен разработать и внедрить процедуры по обязанностям персонала в рабочее время, определить ответственных лиц по отпиранию и запираанию дверей на объекте в начале и в конце рабочего дня; по использованию тревожной сигнализации и знанию, как пользоваться тревожными кнопками; выработать культуру безопасности: сохранять бдительность, выявлять и сообщать о недостатках в проблемах физической безопасности. У всего персонала должно быть настороженное отношение к незнакомцам. Персонал должен научиться защищать свое место работы.

мой в оборудовании физической охраны, имеет свои преимущества и ограничения:

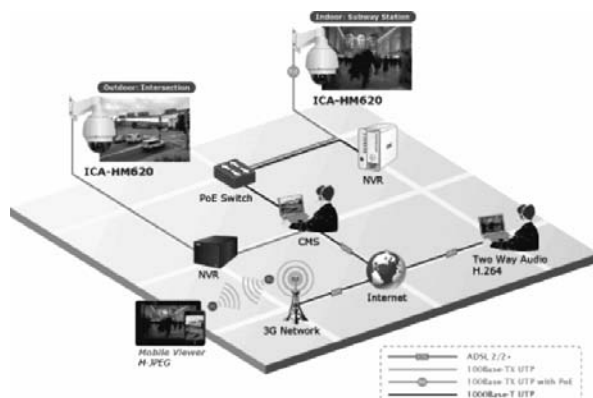
Система контроля и управления доступом (СКУД) – совокупность средств (механических, электромеханических, электрических, электронных), предназначенных для ограничения и санкционирования перемещения людей, предметов, транспорта в помещениях, зданиях и по территории охраняемых объектов (базовое оборудование – взрезные системы запирания, система навесных замков; системы контроля прохода персонала путем использования карточных ключей (магнитные замки и электромеханические защелки), биометрические системы).



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

Врезные системы запираания:

преимущество – стойкие к вмешательству, используется прочность сооружения;

недостатки – возможная сложность установки, необходимость реконструкции двери и дверной коробки, возможность изготовления дубликата ключей.

Навесные замки:

преимущество – простота установки;

недостатки – относительно легко взломать, петли должны быть не менее прочными, чем замки.

Системы контроля прохода персонала – устройства индивидуального контроля доступа:

преимущества – возможность контроля прохода в зону и выхода из зоны;

возможность интеграции нескольких устройств для повышения точности идентификации для дополнительных уровней безопасности;

недостатки – требуется детальное планирование и процедуры; необходим надежный источник питания, более дорогостоящее.

Биометрические устройства контроля доступа:

преимущества – уникальные признаки, требуется сложная техника для преодоления системы;

недостатки – возможность ошибки при идентификации; необходимость наличия соответствующих компьютерных систем для управления информацией.

Средства обнаружения – достигаются базовым оборудованием (техническими средствами, входящими в состав системы охранной сигнализации: извещатели (пассивные оптико-электронные инфракрасные извещатели, пассивные звуковые извещатели для блокировки остекленных конструкций, магнитоконтактные и электроконтактные извещатели, вибрационные, сейсмические и т.п.), приемно-контрольные приборы, оповещатели (звуковые, световые, светозвуковые);

недостатки – вероятность обнаружения, процент ложных срабатываний, уязвимость.

Средства оценки событий – (базовое оборудование – системы видеонаблюдения для мониторинга определенных зон, а также освещение).

преимущество – постоянное наблюдение за определенными зонами, визуальная оценка ситуации после сигнала тревоги;

недостатки – стационарные камеры должны быть направлены на нужные зоны; необходим активный мониторинг человеком; изображения от множества камер трудно отслеживать; оборудование может быть подвержено неблагоприятным воздействиям окружающей среды.

Средства задержки – их задача:

задержать нарушителя после его обнаружения с целью обеспечения времени для прибытия сил реагирования до совершения нарушителем противоправных действий;

сбалансировать защиту, стремясь не усложнить путь нарушителя (средства – решетки, ограничивающие устройства, укрепление дверей, окон и стен, электронные замки и пр.).

Средства связи – своевременное реагирование должно быть обеспечено разнообразными и надежными каналами связи для своевременного информирования сил реагирования о возникших проблемах;

механизмы связи должны быть настроены в соответствии с планами реагирования и процедурами (средства – радиостанции, устройства телекоммуникации).

Однако даже при наличии физической охраны необходимо минимизировать роль человеческого фактора. Для этого необходимо требовать от всех работников:

- добросовестного выполнения своих должностных обязанностей;
- строго определить категорию лиц, имеющих доступ в зоны ограничений;
- максимально ограничить посещение режимных зон лицами, не участвующими в работе;
- регламентировать порядок выдачи ключей работникам и обслуживающему персоналу;
- максимально сократить количества лиц, обладающих досмотровым иммунитетом.

Материал подготовлен на основе доклада, сделанного в ходе Первой национальной выставки-форума «Центр безопасности 2013: инженерно-техническая безопасность». ■

← Начало на стр. 7

Новые разработки нормативной базы по производству, обслуживанию, технадзору технических средств и систем охраны

Не допускается проводить работы по актам обследования на объектах:

- нового строительства;
- категории А по [1] (за исключением работ по доблокировке уязвимых мест или замене аппаратуры);
- имеющих взрывоопасные зоны.

Срок действия акта обследования, также как и проекта, – один год с даты подписания до начала производства работ по нему. Действие акта может быть продлено на тот же срок организациями, их разработавшими и согласовавшими. Акт обследования утрачивает свое действие при изменении профиля объекта и подлежит переутверждению при перемене заказчика.

Отступления от актов обследования в процессе монтажа технических средств сигнализации не допускается без согласования с заказчиком и организациями, участвовавшими в составлении акта обследования.

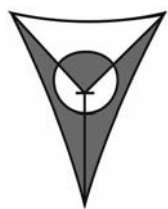
Проект ТКП xxx-2014 (02010)

Обсуждать планируемый к реализации проект ТКП xxx-2014 (02010) «Технический надзор за выполнением работ

по оборудованию объектов системами охраны» на данном этапе нет смысла. Планы по его подготовке следующие: до 15.09.2013 года утвердить техническое задание на данный технический документ, обсудить с заинтересованными организациями, одновременно разместить для обсуждения на сайте Государственного комитета по стандартизации Республики Беларусь в разделе «Проекты ТНПА». Надеюсь, что представители монтажных организаций примут участие в обсуждении данного проекта ТНПА, от этого он станет только лучше. Кто, как не Вы, сможет задать вопросы, которые следует решить в первую очередь.

В конце своего выступления хочу высказать большое спасибо от имени Департамента охраны МВД Республики Беларусь бывшему нашему сотруднику, который ушел на пенсию – Брелю Игорю Даниловичу, за оказание большой практической помощи в подготовке разработанных нормативных документов.

Материал подготовлен на основе доклада, сделанного в ходе Первой национальной выставки-форума «Центр безопасности 2013: инженерно-техническая безопасность». ■



Перспективы развития средств передачи извещений охранной сигнализацией для работы по сетям Ethernet



Шелюто Дмитрий
Эдуардович,
зам. гл. конструктора
«АЛАРМ» НТ ЗАО

Состояние и развитие технических средств и каналов связи

В настоящий момент около 90% объектов охраняются Департаментом охраны МВД Республики Беларусь по занятым телефонным линиям связи, через ретрансляторы, установленные практически на всех телефонных станциях республики. Также используются каналы GSM/GPRS, связи сотовых операторов, 7% объектов и около 3 % объектов охраняется по радиоканалам. При использовании автономных систем (предприятие, завод) каналы связи выбираются в зависимости от функциональных требований, предъявляемых к охране и защите объектов – это как занятые телефонные линии, так и сети, построенные по каналам RS485 либо Ethernet.

Однако активное внедрение цифровых технологий передачи информации Министерством связи и РУП «Белтелеком» поставило как перед Департаментом охраны, так и перед разработчиками оборудования ОПС ряд серьезных задач, требующих достаточно быстрого решения.

В первую очередь РУП «Белтелеком» начал замену межстанционных кабелей на оптоволокно. Для обеспечения работоспособности существующих ретрансляторов, установленных на АТС и работающих по меди, НТ ЗАО «Аларм» в

2007 г. разработал модуль «Аларм-Ethernet» для ретранслятора «Алеся», позволяющий организовать связь по Ethernet-каналу с пультами централизованного наблюдения (ПЦН) подразделений Департамента охраны. В 2009 г. было разработано и внедрено изделие УТОИ-02 (устройство трансляции и обработки информации), позволяющее работать как по медным парам, так и по каналу Ethernet.

УТОИ-02



Коммутатор линий КЛПТ-200



Ретранслятор «Аларм»

Аларм-Ethernet



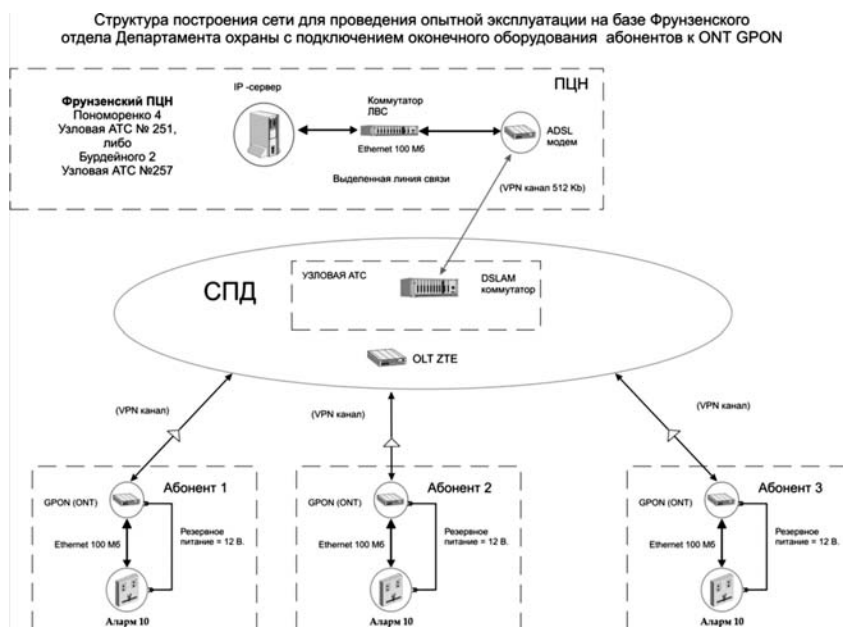
Оборудование ретрансляторов

Учитывая быстрое развитие в РБ сети Internet, а также расширение предоставляемых РУП «Белтелеком» услуг IP-сервиса (IP-телефония, Internet, IP-телевидение), встал вопрос так называемый «последней мили», т.е. максимальное сокращение длины линии связи от абонента до коммутационного оборудования узла абонентского доступа (MSAN, DSLAM) с целью увеличения пропускной способности канала. Первоначально во всех крупных городских населенных пунктах республики были установлены телекоммуникационные шкафы с оборудованием для интеграции услуг HONET ONUF01D1000 разработки

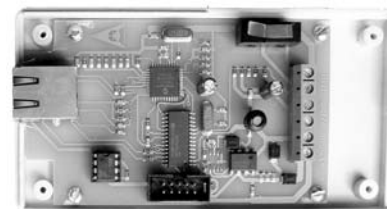
компании HUAWEI. Данные шкафы размещены в непосредственной близости от жилых домов, что обеспечивает высокоскоростную и качественную передачу данных, речи и мультимедийных сообщений. Все шкафы соединены между собой и сетью передачи данных (СПД) оптоволоконной линией связи, но между шкафом и абонентом остались медные пары, что позволяет использовать существующий парк приборов. Однако в данные телекоммуникационные шкафы не представлялось возможным разместить оборудование, разработанное ранее НТ ЗАО «Аларм» для работы по Ethernet-каналам (УТОИ-02 и модуль «Аларм-Ethernet»). Поэтому, в 2010 г. НТ ЗАО «Аларм», по согласованному проекту с РУП «Белтелеком», компанией HUAWEI и Департаментом охраны, разработал и запустил серийное производство новых ретрансляторов «Аларм», которые имеют жесткое климатическое исполнение и устанавливаются в 19" стойки телекоммуникационных шкафов. Ретранслятор имеет порт Ethernet и позволяет подключать до 200 абонентов (в телекоммуникационном шкафу – не более 120).

Внедрение GPON, переход на новые каналы связи

После запуска ретрансляторов казалось, что можно вздохнуть свободно и расслабиться, но РУП «Белтелеком» с 2011 г. начал в широком масштабе внедрять новую технологию GPON на телекоммуникационном рынке РБ. Во всех новостройках монтируются коммутационные пассивные шкафы и оптика подводится прямо к квартирам. Физические пары (медь) – отсутствуют – и соответственно, использование старого парка приборов невозможно. В квартире устанавливается абонентский терминал MT-PON-AT, обеспечивающий работу Internet, IP-телевидения и телефона. Устройство имеет один свободный Ethernet-порт, предназначенный



ППКО «Аларм-10»



БС-ППК-Ethernet

для подключения стороннего оборудования, в частности – охранно-пожарных приборов. Кроме того, с 2012 года данная технология применяется не только в новостройках, но и в существующих домах и объектах (с сохранением и без сохранения медных пар), где уже были установлены охранно-пожарные приборы. К 2015 г. планируется внедрение более 600 тыс. абонентских устройств GPON.

На момент внедрения данной технологии в Беларуси были приборы, поддерживающие работу по Ethernet-каналам через отдельный встраиваемый модуль (производитель – компания ЗАО «Ровалэнт»). Однако данные приборы работали только на пульт «Неман», который был установлен всего в 3-х подразделениях ДО МВД.

Также компания ЗАО «Новатех Системы Безопасности» разработала в 2011 году приставку МПИ-Ethernet, позволяющую подключить существующие приборы на ПЦН данной компании. Однако стоимость данного модуля оказалась сравнима со стоимостью охранного прибора.

Учитывая серьезность ситуации, специалистами НТ ЗАО «Аларм» оперативно был разработан 4-х шлейфный прибор «Аларм-10», работающий по интерфейсу Ethernet 10/100 Base-T на ПЦН СПИ «АСОС Алесь» (данный ПЦН установлен во всех подразделениях ДО МВД РБ, а также на крупнейших заводах и предприятиях Республики Беларусь).

Проведены соответствующие испытания и получен сертификат соответствия (в 2012 г.). Стоимость

прибора получилась достаточно демократичной (на сегодняшний день 996 000 руб. с НДС). Кроме того, для поддержки работы парка существующих приборов был разработан блок сопряжения «Аларм-ППК-Ethernet» (аналог МПИ-Ethernet), работающий с приборами всех производителей (от 8 до 64 ШС). В настоящий момент завершаются функциональные испытания изделия (в том числе в РУП «Белтелеком»), его примерная стоимость – 600 000 руб. с НДС.

Но внедрение данного парка оборудования (всех производителей) затянулось по вполне объективным причинам.

1. Необходимо согласовать тарифную политику стоимости трафика между РУП «Белтелеком» и ДО МВД РБ.

2. Возникли вопросы обеспечения резервного питания абонентских терминалов MT-PON-AT (данное оборудование не комплектуется резервным источником питания). Как один из вариантов решения данного вопроса – резервировать питание от охранного прибора. В частности, были проведены дополнительные испытания работы MT-PON с организацией резервного питания от ППКО «Аларм-10».

3. Наиболее серьезная проблема возникла при организации построения сети в рамках республики для обеспечения передачи информации от охранных приборов на ПЦН подразделений Департамента МВД РБ. Ранее, при организации VPN-каналов и подключении ретрансляторов на ПЦН, функции настройки

каналов брал на себя целиком РУП «Белтелеком». Однако ретрансляторов сравнительно немного, а парк объектового оборудования будет в сотни раз больше.

Кроме того, возникли технические сложности при проверке возможностей организации VPN-каналов от стационарного оборудования OLT, обслуживающего до 4 тысяч абонентов разных районов города к нескольким ПЦН одновременно. На совместном совещании представителей РУП «Белтелеком», Департамента охраны МВД и производителей средств ОПС было принято решение, что функции по обеспечению работы объектового оборудования в СПД возьмет на себя Департамент охраны. В первую очередь это касается распределения пулов IP-адресов для приборов, поддержка приборами протокола DHCP (динамическое распределение адресов), установка Департаментом охраны собственных серверов в областных городах для обеспечения динамической адресации приборов и управления. Все перечисленные меры потребуют создания в Департаменте МВД отдельной структуры.

Открывающиеся возможности при переходе на новые каналы связи

Переход на высокоскоростные каналы существенно расширит функциональные возможности ОПС:

- расширение видов событий и извещений от ППКО;
- возможность программирования приборов на расстоянии;



ПЕРВЫЙ ГИБРИДНЫЙ ОБЛАЧНЫЙ РЕГИСТРАТОР С ВИДЕОАНАЛИТИКОЙ



Новые технологии безопасности для объектов разного масштаба
- от небольших магазинов, квартир и коттеджей - до супермаркетов,
отелей, заводов и жилых комплексов.



«Proto-X» - это новое поколение высокотехнологичного оборудования, включающее самые перспективные направления профессионального видеонаблюдения: аналоговое видеонаблюдение, видеонаблюдение

высокой четкости стандарта HD-SDI, а также самое быстроразвивающееся и наиболее востребованное на рынке направление - сетевое видеонаблюдение(IP). Производство оборудования торговой марки «Proto-X» базируется на мощностях основного производственного комплекса NGTRON Limited. Высококвалифицированные специалисты осуществляют жесткий контроль всех этапов создания конечного продукта, начиная от разработки дизайна и заканчивая финальным тестированием оборудования. Именно это позволяет устанавливать на всю продукцию «Proto-X» гарантию 3 года, с возможностью моментальной замены при выявлении недочетов или заводского брака. Отличительными чертами продукции «Proto-X» являются:

- ❖ Вся продукция адаптирована специально для эксплуатации в сложных условиях (высокая разница температур, влажность, плохая освещенность и риск актов вандализма).
- ❖ Все оборудование построено на самой современной базе и DSP процессорах последнего поколения, обладает широким функционалом, а также продвинутыми техническими характеристиками.
- ❖ Продуманное программное обеспечение, разработанное собственными специалистами с учетом всех требований конечного потребителя.
- ❖ Уникальный дизайн оборудования, интерфейса и упаковки, обеспечивающий привлекательный внешний вид и позволяющий удовлетворить требования самых взыскательных клиентов.



CCTV камеры торговой марки "Proto X" созданы с применением самых современных технологий: новейшие DSP процессоры последнего поколения, светосильные мегапиксельные объективы, CCD-матрицы Sony EX-View и Sony Super HAD 2 обеспечивают кристально четкую обработку и передачу сигнала в самых сложных объективных условиях.

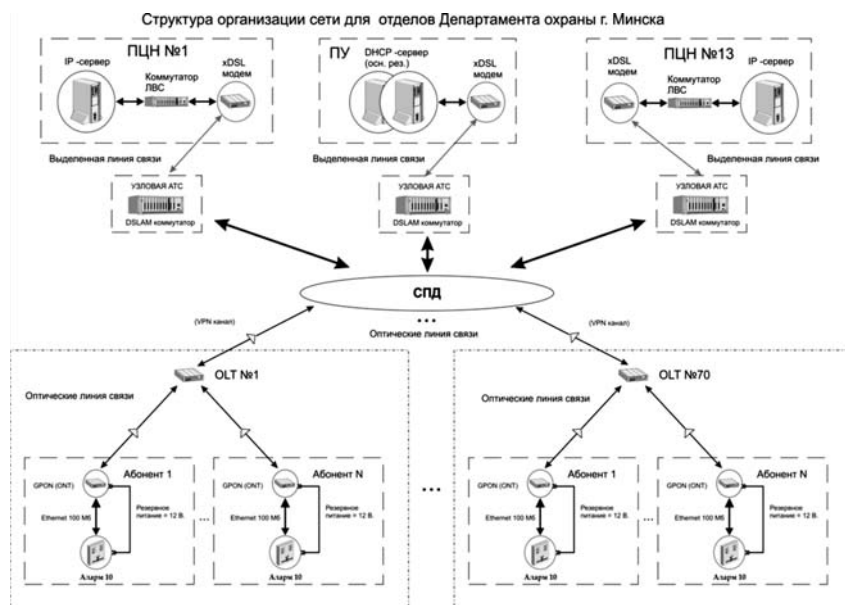


Цифровые видеорегистраторы торговой марки «Proto X» созданы с использованием уникальной технологии «Touch sensor». Данная технология

позволяет нам отказаться от привычных элементов управления на передней панели и создать неповторимый дизайн. Впервые это новшество применено именно в бюджетном сегменте, что делает видеорегистраторы «Proto X» доступными для широкого круга потребителей. Оригинальное программное обеспечение разработано российскими инженерами, имеет интуитивно понятный интерфейс и учитывает все требования современного рынка безопасности.



Официальный представитель «Proto-X» в Республике Беларусь ООО «ТеслаСистемс» тел. +375-177-927-927; факс +375-177-765-436; <http://teslasystems.by/>; mail: info@teslasystems.by



На момент написания статьи были успешно проведены испытания в РУП «Белтелеком» и ДО МВД по проверке работоспособности приборов серии «Аларм» с использованием динамической адресации, организованной на базе DHCP-сервера Департамента охраны.

- широкое использование систем видеонаблюдения (СВН) в определенных охранных СПИ;
- реализация команд управления исполнительными механизмами.

Если коснуться СВН, на сегодняшний день стоимость IP-камер еще не позволяет их использование в качестве технологического оборудования для нужд ДО МВД (просмотр объекта оперативным дежурным ПЦО при получении сигнала «Тревога»), но в перспективе – после снижения цен – это станет возможно, особенно по Ethernet-каналам связи.

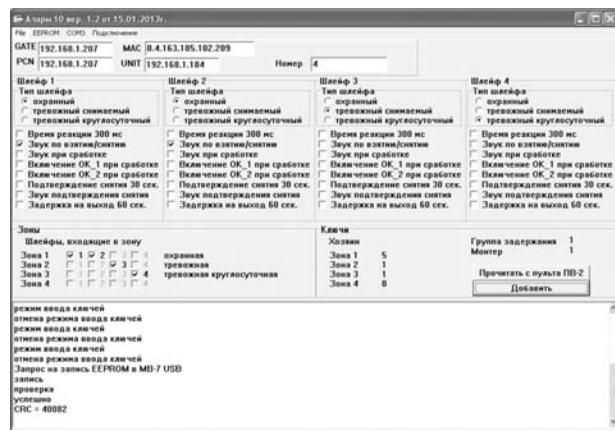
Необходимо только решить юри-

дическую сторону вопроса: согласование с собственником объекта режима видеонаблюдения, т.е. работы СВН только в режиме, когда объект находится под охраной и получен на ПЦН сигнал о проникновении на объект. Техническая сторона этого вопроса уже решена специалистами нашего предприятия: ПО ПЦН «АСОС «Алеся» позволяет непосредственно в программе оператора просматривать и сохранять видеоданные с ряда IP-камер: Vivotek FD, Axis, V10xx, в настоящий момент ведется доработка ПО под другие типы IP-камер. Данные на ПЦН с объекта могут передаваться как по Ethernet-каналам (оптические линии, через модемы

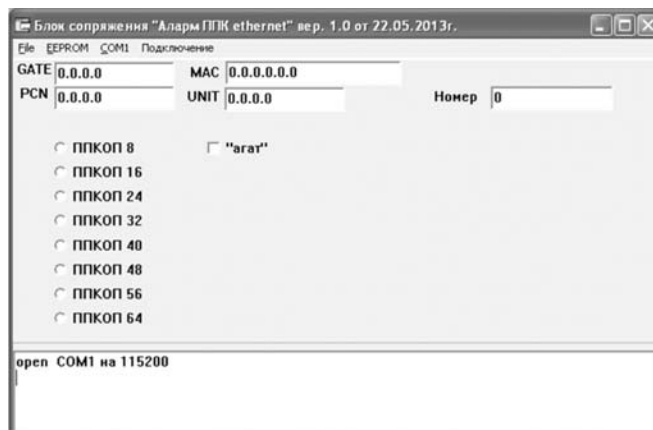
xDSL, GPON), так и по каналам сотовой связи 3G/4G – сразу же после получения сигнала «Тревога».

Надо учитывать тот факт, что СПИ «АСОС Алеся» является, прежде всего, системой охранной и пожарной сигнализации. Функция работы с видеоданными является для нее сервисной и позволяет определить: является ли «Тревога» ложной, или это реальное проникновение, а также помогает дежурному и группе задержания определиться с оперативной обстановкой. Есть функции записи и хранения видеоданных. Однако полноценная система охранного видеонаблюдения – это совершенно другая система. Это поддержка работы с огромным парком видеокamer, интеллектуальное распознавание образов, мощные функции поиска и работы с архивами и т.д. Вообще любая серьезная система безопасности должна быть ориентирована на выполнение определенных функций – либо это в первую очередь охранная система, либо это система видеонаблюдения, либо система СКУД (и т.д.). Очень хорошо, когда любая из систем позволяет вводить дополнительные функции. Например, СВН дополнена охранными функциями и СКУД, это реализовано в системе видеонаблюдения комплекса «Интеллект». СПИ «АСОС Алеся» сопряжена в части видео с данной системой, но пока данный вариант нигде не устанавливался. Чем сложнее система, тем более высокие требования предъявляются к обслуживающему персоналу и к надежности работы составных частей.

Материал подготовлен на основе доклада, сделанного в ходе Первой национальной выставки-форума «Центр безопасности 2013: инженерно-техническая безопасность».



Программирование «Аларм-10»



Программирование БС-ППК-Ethernet



Реализация проектных решений на базе оборудования «Болид»

Республика Беларусь всегда была для компании Болид важным сегментом рынка для продвижения продукции. Недаром именно в Беларуси было открыто первое официальное представительство компании. Сегодня наши страны уже объединяются Таможенным союзом. Эти обстоятельства явились вескими основаниями в пользу активного участия «Болид» в новом мероприятии – выставке-форуме «Центр безопасности 2013: инженерно-техническая безопасность» в Минске.

Несмотря на то, что этот форум проводится в первый раз, он оказался весьма полезен как для посетителей, так и для участников. Нас очень порадовала активность и наполняемость аудитории, ее энергичный молодой возраст. Со своей стороны спикеры на семинарах «Болид» не стали ограничивать во времени ни себя, ни гостей. Четыре семинара фактически превратились в мероприятия формата нон-стоп.

В ходе докладов было задано много технических вопросов. В качестве информации для тех, кто не смог посетить семинары, формулируем некоторые темы, вызвавшие наибольший интерес аудитории:

Какая максимальная длина интерфейса RS-485?

Длина линии RS-485 может достигать 3 км, а использование повторителей <C2000-ПИ> позволяет увеличивать длину и обеспечивает гальваническую развязку сегментов интерфейса. При этом не стоит путать <C2000-ПИ> и <ПИ-ГР>. <C2000-ПИ> может работать как повторитель RS-485 и как преобразователь RS-485/RS-232, а <ПИ-ГР> работает только как преобразователь RS-485/RS-232 совместно с ПК. Рис. 1

Какое максимальное количество приборов и адресных извещателей может работать под управлением одного пульта <C2000>/<C2000М>?

Нужно помнить, что максимальное количество адресов, которые могут иметь приборы под управлением одного пульта, – 127, но при этом суммарное количество подключенных к ним адресных извещателей или шлейфов неадресных приборов (<Сигнал-20П>, <Сигнал-20М>, <Сигнал-10>, <C2000-4> и т.д.) не должно превышать 512 для

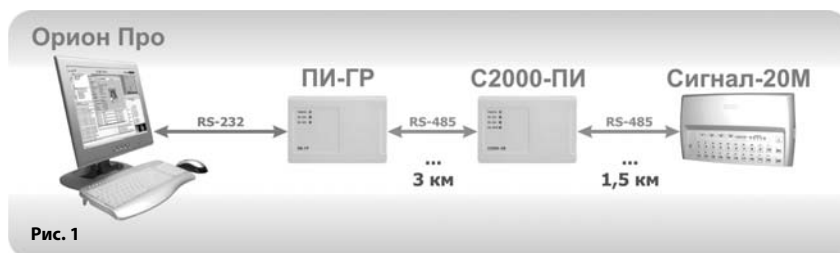


Рис. 1

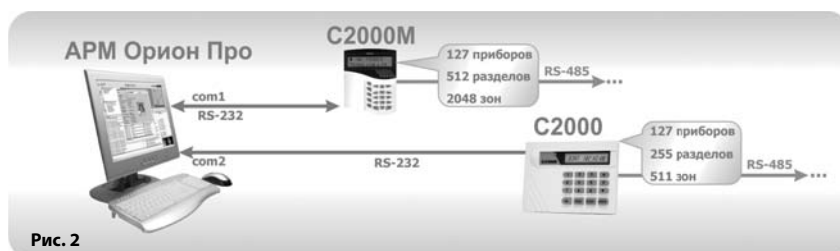


Рис. 2

пульта <C2000> и 2048 для <C2000М>. В случае применения программы АРМ <Орион Про> в системе может быть несколько подсистем под управлением пульта <C2000М> каждая, и по большому счёту, максимальное количество адресных извещателей не ограничено. Все извещатели можно нанести на планы помещений, таким образом, при сработке будет видно, какой именно

извещатель и в каком помещении сработал. Рис. 2

Как правильно объединить между собой несколько зданий, в которых установлены приборы системы <Орион>, и используется один пульт <C2000М> в комнате охраны?

В данном случае, если имеются сегменты воздушной прокладки интер-

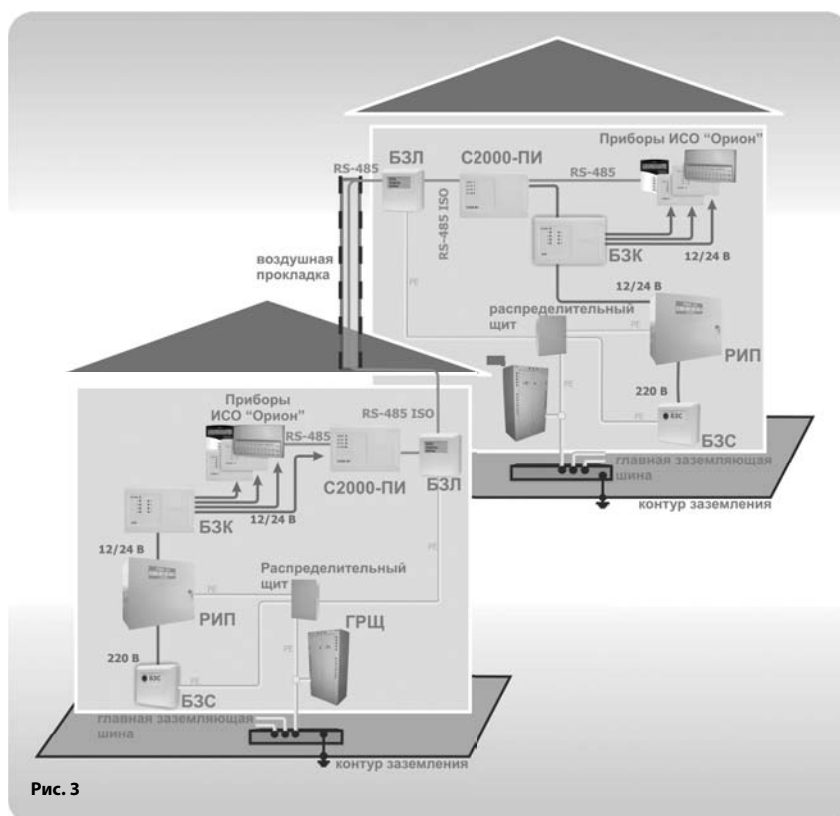
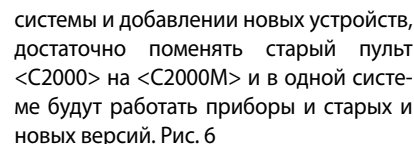
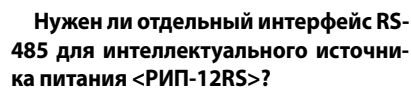


Рис. 3



Напоминаем, что пульты <C2000M> поддерживают все приборы, которые выпускались за все годы существования системы. Т.е., при расширении старой



Если на объекте функционируют две системы, каждая под управлением своего пульта <С2000М>, то они могут быть объединены в единую систему, управляемую одним ПК с АРМ <Орион Про>. Такая интеграция позволяет при пожаре осуществлять разблокировку дверей на программном уровне, с помощью механизма сценариев управления АРМ <Орион Про>. Однако, на наш взгляд, следует продублировать данный сценарий на аппаратном уровне, включив тревожное реле управляющего прибора системы пожарной сигнализации в любой шлейф системы контроля доступа, и настроив в соответствующем пульте <С2000М> запуск сценария разблокировки дверей при нарушении данного шлейфа. Это позволит системе функционировать штатным образом в случае включения или выхода из строя ПК с АРМ <Орион Про>. Рис. 7

Здесь можно отметить, что в Минске у нашей компании есть официальные представители – ЧСУП "ОрионПроект", представители и специалисты которого могут осуществлять консультации по всем интересующим вопросам, от технической поддержки и помощи при проектировании и пуско-наладке до вопросов поставок и ремонта. Также следует напомнить, что на нашем сайте www.bolid.ru выложена документация на все приборы, каталог типовых решений, справочник монтажника, демо-версии всех программ, а также записи онлайн-семинаров. Таким образом, можно довольно быстро самостоятельно разобраться в принципах работы и настройки приборов и программного обеспечения системы <Орион>. А все возникающие вопросы задать либо нашим представителям, либо нам напрямую.

УНП: 191107028

— Наша компания предоставляет клиенту не столько услуги, которые он хочет приобрести, сколько результат, который ему нужен. Ибо истинное осознание того, что нам хочется, приходит лишь с пониманием того, что нам нужно...

Валерий Коваленко директор ООО «Инновационная компания «INTES», к.э.н.



ИННОВАЦИОННАЯ КОМПАНИЯ

INTES

ООО «Инновационная компания «INTES»

Активная система безопасности на воде E-Rescue



Согласно статистическим данным

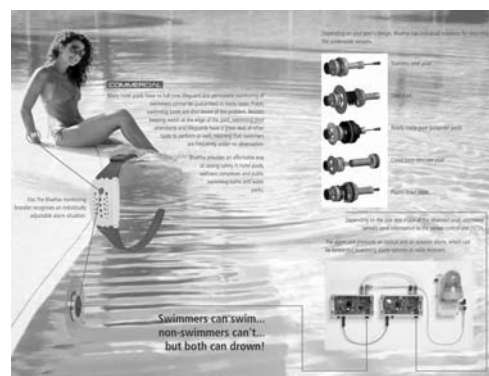
Международной федерации спасателей (www.ilsf.org) ежегодно 1,2 миллиона человек погибают от несчастных случаев на воде. Более 2 человек каждую минуту!

Жизненно важную роль в безопасности на воде играет быстрота обнаружения несчастного случая, от чего напрямую зависит возможность спасти человека. Для обеспечения максимальной скорости идентификации несчастного случая и предназначены активные средства защиты.

E-Rescue — это уникальная система безопасности нахождения на воде, позволяющая осуществлять контроль за безопасностью человека по многим параметрам, моделирующим процесс возникновения опасной ситуации на воде.

Назначение

Ключом системы является мониторинговый браслет, выдаваемый индивидуально каждому посетителю. В случае прохода предельной глубины мониторинговый браслет по истечению допустимого времени пребывания на глубине ниже предельной выдает ультразвуковой тревожный сигнал, который, поступая на приемник, формирует тревогу по системе в целом с распознаванием зоны инцидента. В роли приемника тревожного сигнала выступают подводные датчики. Система не имеет привязки к какому-то конкретному датчику системы и может быть использован в любом бассейне, оборудованном подводными датчиками.



Достоинства

Система может быть инсталлирована на любом этапе работы объекта, как на строящемся, так и работающем, и может использоваться для любого решения: от домашнего бассейна до водного центра развлечений и открытых водоемов. В этой связи могут быть использованы различные комплекты системы **E-Rescue**.

BASIC

BASIC-комплект
Предназначен для коттеджей, вилл, частных саун и т.п. В комплект входит устанавливаемый на стенке бассейна под водой датчик, блок управления с сиреной и один мониторинговый браслет. Обеспечивает **активную и пассивную** защиту бассейна (возможно использование дополнительных браслетов).

STANDARD

Standart- комплект
стационарной установки, актуальный для небольших объектов: сауна, небольшой бассейн и т.п.
в дополнение к базовым функциям, обеспечивает возможность трансляции сигнала оповещения на дублирующее устройство, размещенное в другом помещении. Ресивер дублирующего оповещателя просто вставляется в розетку.

PRO

PRO-комплект
стационарной установки, который предназначен для использования в бассейнах отелей и больших бассейнах коммерческого назначения, и водоемах **рекреационных комплексов**. Обеспечивает активную и пассивную защиту бассейнов.

MOBILE

MOBILE-мобильный
комплект, идеально подходящий для школ, детских дошкольных заведений, детских лагерей отдыха, санаториев, баз отдыха, открытых водоемов и т.д. Обеспечивает активную защиту бассейна.



СИСТЕМЫ

E-Rescue

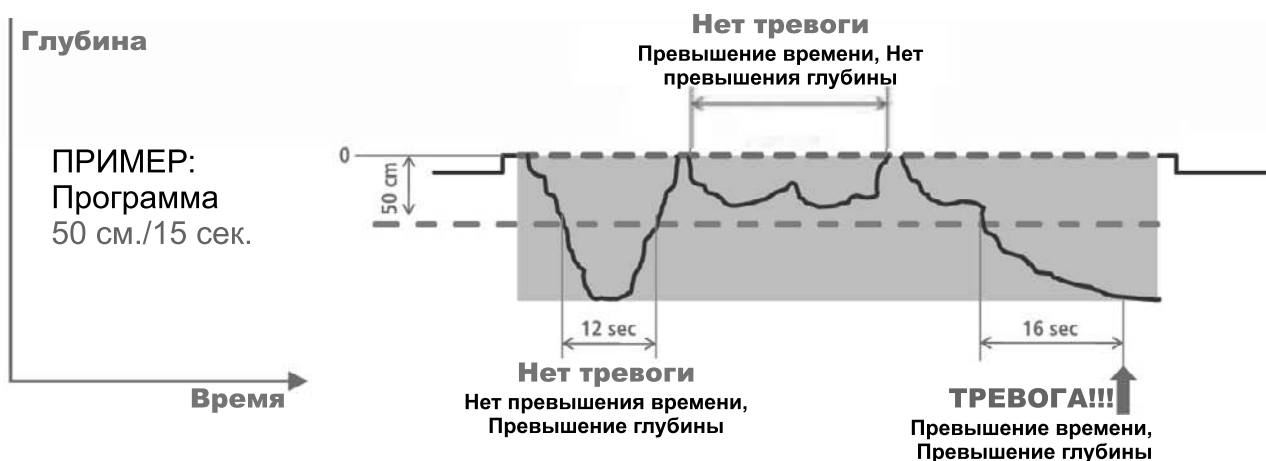
Как это работает

Активная система безопасности на воде **E-Rescue** обеспечивает **активную и пассивную** защиту пользователей общественных и частных бассейнов.

В режиме **активной** защиты система осуществляет мониторинг объема бассейна в часы работы, отслеживая данные с мониторинговых браслетов пользователей. В случае, если владелец браслета остается под водой длительное время, система выдает сигнал тревоги.

Режим **пассивной** защиты активируется в нерабочее время. Система осуществляет мониторинг объема бассейна и выдает сигнал тревоги в любом случае при попадании кого-либо в бассейн, даже если он не имеет браслета. Это обеспечивает пользователям и эксплуатирующим организациям общественных бассейнов, а также владельцам частных бассейнов и членам их семей круглосуточную безопасность.

Обычная ситуация: вы наблюдаете за резвящимися в бассейне или пруду детьми, как вдруг неожиданный звонок отвлекает вас и вы оставляете детей на некоторое время без присмотра. Чудный день в считанные секунды может обратиться чудовищным кошмаром. Этого не произойдет с системой безопасности бассейнов E-Rescue, которая никогда не утрачивает бдительности и вовремя подаст сигнал тревоги, если кто-то пробудет под водой слишком долго.



Кто проектирует, установит и наладит

РЕСПУБЛИКА БЕЛАРУСЬ и СНГ:

Инновационная компания **INTES**

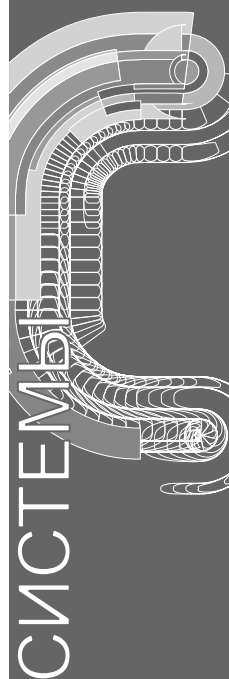
свыше 8 лет успешно работает на рынке Республики Беларусь и СНГ в областях:

- интегрированных систем безопасности (видеонаблюдение, ОС, СКУД);
- информационных технологий (ERP, SaaS и EaaS – системы, комплексные системы планирования и управления, диспетчеризации, автоматизированные билетные и платежно-пропускные системы, и др.);
- технологических решений объектов спорта, отдыха и развлечений;
- дизайна среды.

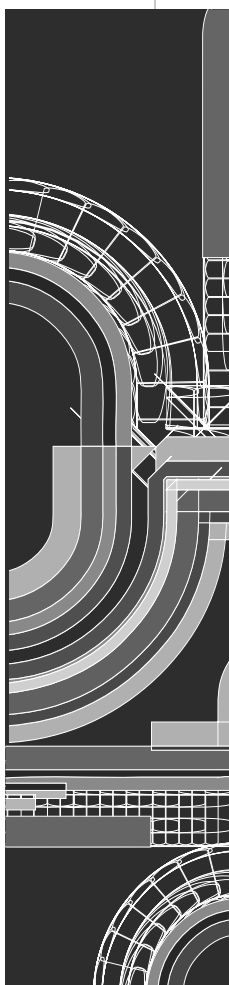
Нашими партнерами являются ведущие зарубежные и российские производители и интеграторы: ISD, UCS, DeepBlue, Kupan, ISS, RVI, PERCo, Interhotel, Axess, Cisco, Schneider Electric, Siemens, IFS, INKA, Onyti, KABA и др.

Инновационной компанией «INTES» выполняется полный комплекс работ по установке системы безопасности на водных объектах любой сложности и конфигурации «под ключ» (проектирование, поставки, монтажа и наладки) на условиях генподряда или субподряда.

Адрес:
220013, г. Минск, ул.Кульман д.2 оф.311
Тел./факс: +375 (017) 209 80 88, 209 84 84
Электронная почта: info@intes.by



E-Rescue





Интеграция системы видеонаблюдения и системы контроля доступа на примере TRASSIR и СФИНКС

ООО «Совершенные системы» работает на рынке систем безопасности с 2009 года и имеет лицензии МВД на право осуществления деятельности по обеспечению безопасности юридических и физических лиц № 02010/0649963 и лицензию МЧС на право осуществления деятельности по пожарной безопасности № 02300/2912.

С 2011 года ООО «Совершенные системы» является официальным партнером российских компаний «Промавтоматика Сервис» (торговая марка «СФИНКС») и «ДССЛ» (торговая марка «TRASSIR»).

СКУД «Сфинкс»

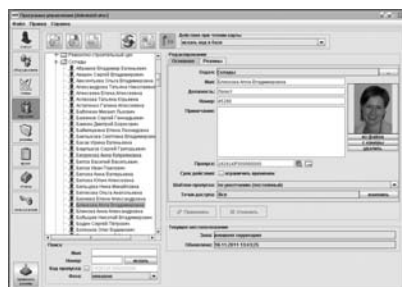


Систему контроля доступа (СКУД) «Сфинкс» можно назвать универсальной системой. Её используют для организации СКУД как в небольших офисах (на несколько дверей), так и для больших территориально-распределенных объектов (учреждения образования, заводы, фабрики, сети магазинов). СКУД «СФИНКС»

предоставляет весь необходимый функционал, который требуется от современных систем контроля доступа, а именно:

- Гибкая система контроля доступа в помещения.
- Быстрое сканирование паспортов и печать пропусков.
- Табель учета рабочего времени, интеграция с 1С:Бухгалтерией.
- Фото и видеоидентификация посетителей в системе контроля доступа.
- Гибкая система отчетов с разграничением прав доступа к информации.
- Автоматизация парковки. Распознавание номеров.
- Планы помещений с индикацией состояния компонентов системы.
- Модуль реакции на события.
- Интеграция с другими системами видеонаблюдения и ОПС
- Встроенная платежная система.

Базовый модуль



Ядро системы: обеспечивает связь с контроллерами и обмен данными в системе, ведение и резервирование базы данных.

Основные функции и особенности:

- Задание списка персонала предприятия, импорт персонала из Excel
- Задание ограничений допуска персонала предприятия по точкам прохода, по направлению и по времени
- Получение отчетов о событиях системы за любой исторический период (включая проходы, запреты доступа, действия операторов системы), экспорт персонала и режимов допуска в MS Excel

• Удаленное управление точками прохода (блокирование, разблокирование)

- Глобальный antipassback
- Зональный контроль
- Работа с графическими поэтажными планами
- Интеграция с Trassir, Domination, Ewclid, Intellect, Macroscop, VideoNet, Линия и другими системами
- Настройка прав операторов системы
- Интеграция с Active Directory
- Открытый интерфейс интеграции с любой информационной системой заказчика.

Создание и печать пропусков



Модуль необходим в тех случаях, когда необходимо персонализировать карты, выдаваемые сотрудникам.

Основные функции и особенности:

- Создание и редактирование шаблонов пропусков во встроенном редакторе
- Назначение шаблонов пропусков сотрудникам
- Печать пропусков на основании шаблонов и хранящихся в базе персональных данных сотрудников

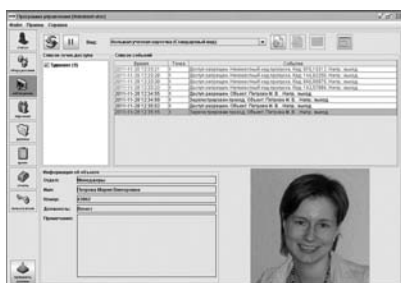
Учет рабочего времени

Модуль позволяет организовать автоматический подсчет рабочего времени сотрудников с учетом действующих на предприятии графиков и правил.

Основные функции и особенности:

- Графики любой сложности – недельные, «сутки через трое», и т.д.
- Любое количество исключений из графиков
- Ввод оправдательных документов
- Получение отчетов о фактической наработке и наработке по графику, отклонениях от рабочего графика, неявках
- Журнал нарушений рабочей дисциплины
- Получение стандартной формы Т-13

Наблюдение и фотоидентификация

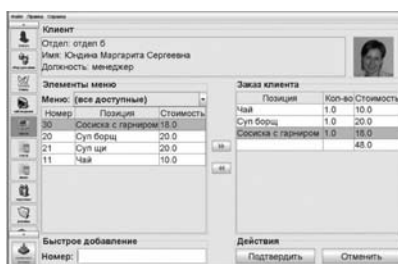


Данный модуль предоставляет обширные возможности для наблюдения за происходящими в системе событиями в режиме реального времени.

- Основные функции и особенности:
- Наблюдение за происходящими в системе событиями в реальном времени
 - Гибкое конфигурирование шаблонов интерфейсов отображения информации
 - Возможность отображения учетной карточки и фотографии сотрудника или гостя в момент прохода (фотоидентификация)
 - Возможность встраивания в единый интерфейс живого видео с камер системы видеонаблюдения
 - Автоматический выбор камеры для отображения оптимального в данный момент вида
 - Выбор набора точек доступа, за которыми осуществляется наблюдение на данном рабочем месте
 - Поддержка многомониторных конфигураций
 - Звуковое оповещение охраны о

тревожных событиях

Платежная система

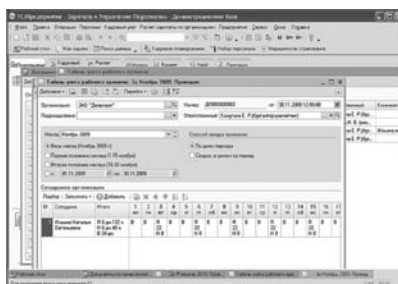


Модуль применяется для организации автоматических расчетов в столовой предприятия, а также других систем предоставления услуг и товаров с использованием карт сотрудников.

Основные функции и особенности:

- Создание и ведение виртуальных счетов сотрудников
- Создание списков товаров и услуг
- Автоматизация точек предоставления услуг и товаров
- Режим самообслуживания
- Ограничение максимального количества предоставляемых сотруднику товаров и услуг и времени реализации
- Быстрый выбор сотрудника при забытой карте
- Печать квитанций

Интеграция с 1С



- Печать квитанций

Данный модуль предназначен для автоматической передачи табеля (форма Т-13) в 1С:Предприятие.

Использование данного модуля не единственный способ взаимодействия систем Сфинкс и 1С:Предприятие.

Также возможно:

- Программное взаимодействие систем средствами встроенного языка 1С.
- Использование дополнения к конфигурации БИТ:

Управление доступом (СКУД) 8.

Данное решение позволяет управлять системой контроля доступа из интерфейса 1С, синхронизировать базы данных сотрудников, автоматически передавать данные о состояв-

шихся событиях и формировать на их основании различные отчеты, передавать в СКУД рабочие графики.

Для применения данных способов достаточно наличия только базового модуля.

Кроме того, приобретая СКУД «СФИНКС», клиенты 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.
- Полная совместимость версий.
- Поддержка интеграции с охранными, пожарными сигнализациями, видеонаблюдением, системами типа «умный дом».
- Адаптация продукта под конкретные пожелания заказчика и поддержка специальных функций.



Видеоаналитика «TRASSIR»

Российская компания DSSL – признанный лидер в области разработки и производства цифровых систем видеонаблюдения любого уровня. ПО видеоаналитики «TRASSIR», поставляемое на рынок компанией «ДССЛ», предоставляет клиентам следующие возможности:



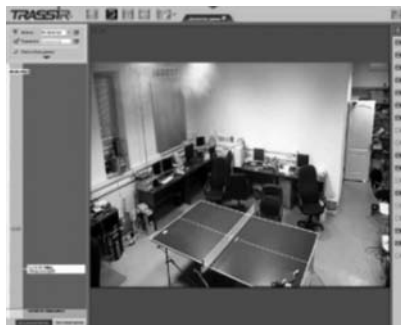
AutoTRASSIR

Определение автомобильных номеров Республики Беларусь совместно со СКУД «СФИНКС» позволяет организовать автоматизацию парковки,

предоставляя автоматический доступ номерам автомобилей из списка авторизованных. Есть функции фильтрации распознанных номеров и поиск по номерам в базе.



TRASSIR SIMT: детектор объектного трассирования SIMT эффективно фильтрует случайные шумы, селективирует объекты по размерам, направлению, скорости движения, обеспечивает детектирование только объектов с заданными параметрами и аналитическое предсказание дальнейшей траектории движения объекта с помощью вектора скорости, применяется в автоматическом режиме работы функции ActiveDome+. Также предусмотрены дополнительный детектор медленного движения и детектор оставленных предметов.



TRASSIR Detectors: детекторы дыма, огня, оставленных предметов, саботажа. Например, если камеру сдвинули, засветили и пр., то камера разворачивается на весь экран. Есть аппаратные детекторы камер, которые разработаны самим производителем. При помощи программной интеграции можно полностью управлять настройками камер (только для полностью интегрированных камер).



TRASSIR – Sphinx и TRASSIR – APM "Орион Про": интеграция с СКУДОМ и ОПС («СФИНС» и «БОЛИД»), которая позволяет управлять объектами системы ОПС и СКУД из системы видеонаблюдения, видеть их состояние

и просматривать архив видеонаблюдения в привязке к событиям из интегрированных систем.



TRASSIR ActiveDome PTZ: управление поворотной камерой при помощи обзорных камер. Позволяет позиционировать камеру без промаха и по детектору движений автоматически или можно вручную нажать кнопку управления прицелом и выделить на обзорной камере нужный сегмент, и поворотная камера спозиционируется в нужную точку.

TRASSIR ActiveSearch: поиск по движению, который позволяет найти в архиве события только в заданном участке обзора.



TRASSIR ActivePOS: контроль учета кассовых операций для банков и торговых объектов (интеграция со счетчиком банкнот). Помогает выявлять воровство на торговых объектах и определять случаи неправильного подсчета банкнот.

TRASSIR ActiveSearch+ и TRASSIR EventSearch: удобный интеллектуальный поиск по архиву по заданным критериям. В системе настраиваются общие каналы и привилегированные каналы, а также каналы низкого качества. Смотря в плохом качестве по интернету, при появлении заинтересовавшего нас события можем развернуть камеру и смотреть в хорошем качестве. Дополнительно для этого пишется поток низкого качества, что позволяет передавать по низкоскоростному каналу удаленный звук, и увеличивает длину архива. При пло-

хом качестве канала звука не слышно, если запись в высоком разрешении. Экспорт архива осуществляется в 5 раз быстрее, чем реальная запись. При экспорте сохраняется в один файл без разрывов записи, что полезно при работе с правоохранительными органами.

TRASSIR Plans: карты объектов позволяют строить иерархическую структуру помещений с указанием расположения конкретных объектов (шлагбаумы, двери, камеры, датчики) и управлять ими, нажимая на пиктограмму на карте. Активный монитор позволяет видеть одновременно и камеры и карту, разделив экран на области. Карта должна быть сохранена в любом из доступных форматов (не более 3МБ). Можно подключать много карт с переходами.

TRASSIR xScreen: подключение до 8 мониторов к одному серверу видеонаблюдения.

TRASSIR Event: система правил реакций на события, которая позволяет любое событие в системе использовать для осуществления каких-то действий.

качественную справку по всем функциональным возможностям системы.

TRASSIR Client: многопользовательский интерфейс управления.

TRASSIR Informer: индивидуальная настройка системы тревожных оповещений всех заинтересованных лиц через SMS, SMTP-почту, звуковые сообщения.

Как установить систему TRASSIR? Вы покупаете компьютер и установочный комплект TRASSIR (можно использовать сетевой видеорегистратор TRASSIR), а также лицензии на подключаемые камеры (есть модели регистраторов, в которые лицензии уже включены). В этом комплекте есть почти весь функционал за исключением распознавания автомобильных номеров, SIMP, ACTIVE DOME, контроля кассовых операций, интеграции со СКУД и ОПС.

Интеграция со СКУД «СФИНС» осуществляется как из TRASSIR, так и из СФИНС, в зависимости от функциональных обязанностей оператора системы.

Официальный партнер в Республике Беларусь компаний «Промавтоматика Сервис», ТМ «СФИНС» и «ДСЛ», ТМ «TRASSIR» «Совершенные системы», ООО
Тел./факс: (017) 294-36-45, (029) 370-20-22
E-mail: info@soversys.by
Сайт: www.soversys.by

УНП: 191152890

ВАША ПРИЯТНАЯ БЕЗОПАСНОСТЬ!



960H – это на 240 пикселей больше чем D1

Видеорегистраторы формата 960h становятся доступнее!

Модификация H.264 - High Profile - уменьшает дисковое пространство в 2 раза

Оперативная память DDR3 и процессор Dual Core - увеличивает стабильность и скорость работы

- Максимальное разрешение 944x576

- Пентаплекс

- Выходы HDMI (1920x1080p), VGA (1024x768), BNC, 3 Spot, MultiSpot

- 4 USB порта,

встроенный WEB-сервер

- Встроенные

полнофункциональные

сетевые функции

- Независимая настройка скоростей записи и передачи

по сети (DualStream)

- Архивирование данных в формате EXE через USB на Flash и HDD, DVD-RW (опция)

- Одновременная запись аудио по всем каналам

- Возможность установки до 4-х внутренних HDD, 8 внешних HDD (e-sata)

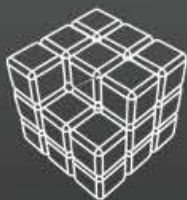
Тел.: (0162) 20-86-13
Моб. тел.: (029) 724-00-53, (029) 326-46-76
E-mail: info@microdigital.by
www.microdigital.by

MD
MICRODIGITAL

УНП: 290479641
ООО «Альда Портал»

9
64/82480

www.videonet.ru



VideoNet[®] №1
ЦИФРОВАЯ СИСТЕМА БЕЗОПАСНОСТИ

Представитель в Республике Беларусь ООО "Сталвиском"
+375 17 2054824, www.stalviscom.by

НОВЫЙ УРОВЕНЬ ВАШЕЙ БЕЗОПАСНОСТИ

Новая версия цифровой системы
безопасности №1



- Первая 64-х битная система безопасности
- Неограниченная масштабируемость системы
- Уникальные интеграционные возможности
- Возможность интеграции различных подсистем на аппаратном уровне
- Единая среда управления всеми подсистемами

- Новая среда аналитики
- Улучшенная работа детекторов
- Широкие возможности пост-анализа и интеллектуальный поиск по архиву
- Новая расширенная система реакций
- Многофункциональный интерфейс



Требования к современной системе видеонаблюдения



Валерий Гапошин,
инженер техподдержки, MICRODIGITAL Inc.

Надежность, эффективность, простота эксплуатации и доступность – все, что требуется современной системе видеонаблюдения? MICRODIGITAL Inc. известная Южно-Корейская компания, более десяти лет специализирующаяся на производстве систем видеонаблюдения, достигла больших успехов в решении этого вопроса. Наши специалисты добавили к уже названному списку универсальность, но обо всем по порядку.

MICRODIGITAL – компания с мировым именем, филиалы и партнеры которой есть практически во всех странах мира. Такому обширному распространению и развитию способствовали преимущества нашей компании. Широчайший ассортимент оборудования для видеонаблюдения позволяет реализовать проекты любой сложности в рамках одного бренда. Полная линейка включает в себя три основных направления:

- CCTV – 17 моделей регистраторов, 100 моделей видеокамер;
- IP – 58 моделей камер и расширяющийся список DVR, интеграция с различными системами;



- HD-SDI – 6 моделей регистраторов, 31 модель видеокамер.

Отдельно можно упомянуть про мониторы, объективы, пульты, тестеры и конверторы.

Квалифицированные специалисты MICRODIGITAL могут проконсультировать по вопросам подбора, совместимости, настройки и пуско-наладки оборудования, в сервис-центре осуществляется гарантийный и постгарантийный ремонт нашего оборудования. Инженеры и программисты компании обеспечили возможность интеграции и построения комплексных систем. Разработанный программный продукт сделал возможным совместную работу аналогового и цифрового оборудования.

Направление IP является одним из самых перспективных и за счет ряда преимуществ уже занимает значительную долю рынка видеонаблюдения.

- Разрешение подобного оборудования позволяет легко получать Full HD изображение и даже более того.
- Нет необходимости прокладывать отдельные кабельные трассы, поскольку можно задействовать уже существующие вычислительные сети, передавая по ним как видеопоток, так и питание в случае использования PoE.
- Масштабируемость подобной системы значительно выше, нет жестких ограничений по распределению и количеству камер.

Максимальное удобство в подключении IP-оборудования MICRODIGITAL обеспечивают: мастер пошаговой настройки и автоматическая настройка сервисов, представленные в WEB-интерфейсе. Наши IP-камеры с функцией DVR имеют возможность осуществлять запись самостоятельно по расписанию или в случае заданного события, такого, как потеря связи с сервером. Для этого предусмотрен слот под MicroSD карту на которую ведется архив. Наличие USB-интерфейса позволяет подключить Wi-Fi модуль или GSM-модем. В качестве примера подобной камеры можно назвать MDC-i4240, снабженную встроенным микрофоном. При этом для подключения не обязательно наличие внешнего IP-адреса благодаря сервису одного из наших партнеров, компании Ivideon, предоставляющей услуги облачного сервиса. Камера, подключенная подобным образом, будет доступна из любой точки, где есть интернет и одновременно возможно просматривать несколько удаленных объектов. IP-регистраторы, представляющие собой простое и эффективное решение, оснащены функцией поиска камер, что

позволяет подключить оборудование последовательностью простейших манипуляций. IP-оборудование MICRODIGITAL имеет достаточно широкий список интеграции, а поддержка стандартов ONVIF и PSIA обеспечивает еще большую универсальность и простоту эксплуатации.

Говоря о мегапиксельном изображении, следует отдельно упомянуть о направлении HD-SDI. В целом, архитектура построения такой системы подобна аналоговой. Единый интерфейс и возможность замены аналогового оборудования без дополнительных работ по прокладке кабелей позволяют легко модернизировать существующую систему, минимизировав затраты. Хотя принципиальные различия в работе следует учитывать и не пренебрегать советом квалифицированного специалиста. Важным аспектом является то, что HD-SDI камеры не сжимают изображение при передаче, обеспечивая более высокое качество видео и передачу без задержек. Подобная камера при съемке, выставленная на максимальный угол обзора, может заменить собой несколько аналоговых камер, получив преимущество в цене.

Но на данный момент поставленные задачи не всегда подразумевают требование мегапиксельного разрешения. Множество проектов по-прежнему реализуется посредством оборудования CCTV или смешанных систем. По этой причине технический прогресс и компания MICRODIGITAL не оставили без внимания данную сферу. Была представлена x900 серия регистраторов, а также камеры с горизонтальным разрешением в 960 точек. Новинки CCTV оборудования позволили несколько увеличить разрешение изображения, не требуя роста финансовых затрат. Ранее представленная технология UTC (управление по коаксиальному кабелю) была интегрирована в регистраторы. Что позволяет осуществлять управление и настройку камер непосредственно через интерфейс DVR. Установленные на борту камер DSP фирмы NextChip позволяют реализовать множество востребованных функций, таких как:

- 3DNR шумоподавление, значительно улучшавшее качество изображения и снижая при этом размер получаемого архива, за счет удаления лишней информации (шумов).
- Расширенный динамический диапазон (WDR – Wide Dynamic Range) обеспечивает четкое и максимально полное изображение в условиях резкого перепада освещенности.
- Компенсация встречной засветки (HLC – High Light Compensation) позволяет, к примеру, отчетливо разобрать номер машины, невзирая на свет фар, и в других подобных ситуациях. Функция работает независимо от движения.
- Технология цифровой стабилизации изображения (DIST), реализованная во всех CCTV камерах MICRODIGITA.

Это далеко не полный список поддерживаемых функций, обеспечивающий максимальную эффективность системы видеонаблюдения установленной на объекте. MICRODIGITAL уже реализовала множество различных решений, стараясь сделать оборудование максимально удобным и эффективным, как в монтаже, так и в эксплуатации. Программные продукты компании позволяют осуществлять работу с системой видеонаблюдения практически с любых платформ, как мобильных, так и стационарных. Сложно рассказать обо всем многообразии новинок, включающем IP DVR, бюджетные модели камер на новейших матрицах CMOS, расширяющийся ассортимент корпусов, различные варианты питания от 12V до 220V.

Необходимую информацию всегда можно найти на нашем официальном сайте www.microdigital.by, либо проконсультироваться по возникшим вопросам в службе поддержки.

Дистрибьютор MICRODIGITAL Inc. в Республике Беларусь
Альфа Портал, ООО
224014, г. Брест, ул. Писателя Сергея Смирнова, 165/1
Тел.: (0162) 20-86-13, (029) 725-45-30, (029) 326-46-76
E-mail: info@microdigital.by
Сайт: www.microdigital.by



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.

УНП:190682380

БЕЗОПАСНЫЙ ДОМ, ОДО

220094, г. Минск, 2-й Велосипедный пер., 30, комн. 402

Тел./Факс: (017) 298-38-05(15)

www.odobd.by odobd@mail.ru

Лицензии:
 №02010/6670 выдана МВД РБ от 28.01.2011г. №2км,
 действительна до 02.03.2021г;
 № 02300/1268 выдана МЧС РБ от 21.01.2011г. №3км,
 действительна до 14.03.2016г.



Компания ITV | AxxonSoft представляет новые версии программного продукта Axxon Next



Компания ITV | AxxonSoft постоянно работает над совершенствованием и развитием своего инновационного продукта **Axxon Next**. Выход новой версии продукта запланирован с периодичностью 1 раз в 3 месяца. Новые версии **Axxon Next** будут предлагать пользователям ряд соответствующих современным трендам (и при этом уникальных по возможностям) функций. Стоит отметить, что каждая версия содержит в себе значительные функциональные нововведения. На момент подготовки данного номера журнала вышла в релиз версия **Axxon Next 3.1** и параллельно ведется работа над функционалом версии 3.2. Переработанный интерфейс поиска, гибко редактируемые раскладки камер, поддержка карт Google и объектов «рыбий глаз», совершенно новый «режим погружения» для интерактивной 3D-карты – вот далеко не полный список инноваций этих двух версий.

Прежде всего хочется отметить функцию, уже доступную в релизной версии.

Это Green Stream, что означает «Зеленый поток». Как это работает?

Многие современные IP-камеры способны передавать несколько видеопотоков. В архив обычно записывается поток максимального качества, однако транслировать его на удаленного клиента не всегда представляется возможным. Для IP-камер, передающих несколько видеопотоков, **Axxon Next** автоматически выбирает наименьший поток, разрешения которого достаточно

для отображения на удаленном клиенте в зависимости от раскладки камер (а соответственно и разрешения отображаемых камер) на мониторе удаленного клиента. Если пользователь раскроет камеру на весь экран, автоматически будет выбран поток высокого разрешения, в мультикартинке – один из доступных потоков низкого разрешения. Также при настройке программы поток, передаваемый на удаленный клиент, можно зафиксировать в определенных значениях в зависимости от ширины канала передачи данных, и тогда он не будет меняться при переключении раскладки на мониторе.

Если пользователь подключает к **Axxon Next** IP-камеры, передающие один видеопоток, и для записи в архив используется поток высокого качества, то технология Green Stream позволяет при необходимости «пережать» этот поток прямо на сервере в поток необходимого разрешения, и далее передать его на клиента. Это делается с помощью кода Motion Wavelet, отличающегося высокой эффективностью сжатия при минимуме потребляемых ресурсов. Кроме того, он позволяет менять разрешение и частоту кадров видео без рекомпрессии. Это означает, что один раз упаковав видео на сервере в максимальном качестве, можно раздавать его нескольким клиентам в соответствии с их потребностями.

И, наконец, еще одна функция Green Stream – прореживание видеопотока

на детектор – помогает экономить вычислительные ресурсы сервера в том случае, если для работы видеодетектора не нужна высокая частота кадров. К таким детекторам относятся, например, детектор потери качества видеоизображения, детектор изменения фона и т.д. Для работы этих детекторов распаковывается не весь видеопоток, приходящий от камеры, а только кадры с нужной частотой. В случае применения таких кодеков, как H.264 или MPEG-4, это будут опорные кадры. А с такими кодеками, как MJPEG, кадры из потока будут выбираться и распаковываться с нужной частотой.

Таким образом, технология Green Stream делает систему видеонаблюдения на основе программного обеспечения **Axxon Next** максимально производительной. Экономия вычислительных ресурсов серверов и рабочих мест мониторинга позволяет использовать для обработки и отображения видео менее мощные компьютеры. Либо, наоборот, обрабатывать на одном компьютере большее количество видеопотоков. И то и другое позволяет сократить бюджет, выделяемый на систему видеонаблюдения.

Дистрибьютор компании ITV | AxxonSoft в Республике Беларусь

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

HIKVISION

Новые технологии компании Hikvision Digital Technology – обзор новинок 2013 года

Сергей Чень,
ведущий технический специалист

Новая линейка камер на инновационной платформе Type Raptor с применением алгоритма сжатия Hi profile H264 от компании HIKVISION.

Новая классификация

Специалисты нашей компании твердо уверены, что за IP-технологиями будущее всей сферы видеонаблюдения. Поэтому в 2013 году компания начала производство новой линейки IP-камер и провела изменения в их классификации. Новая классификация более структурирована, стала удобней и четче. Современная линейка IP-камер Hikvision состоит из следующих серий:

2 серия – оборудование для широкого применения, обладающее наилучшим соотношением цены и качества

4 серия – оборудование для профессионального применения

6 серия – оборудование для специализированных проектов, в том числе с применением функции видеоналастики.

«2 серия»

Камеры этой серии на сегодняшний день наиболее востребованы рынком, так как они недорогие и при этом в них сохраняется традиционное качество камер Hikvision.

Во «2 серии» существуют 8 видов корпусов. Корпуса камер имеют различное исполнение: цилиндрические (с классом защиты IP 66), с ИК подсветкой нового поколения – EXIR, купольные, с фиксированным объективом, мини-куб камера (со встроенным динамиком и микрофоном). Есть купольная мини-камера с ИК подсветкой – она уже продается на рынке Беларуси (модели 21 и 25).



HIKVISION

Скоро появятся модели 26 и 27 – уличные камеры с вариообъективом, разработанные по стандарту IP 66.



Технологические преимущества камер «2 серии»

Наличие моделей с «Умной» ИК подсветкой EXIR.



Технологическое преимущество ИК подсветки нового поколения EXIR базируется на 2-х моментах:

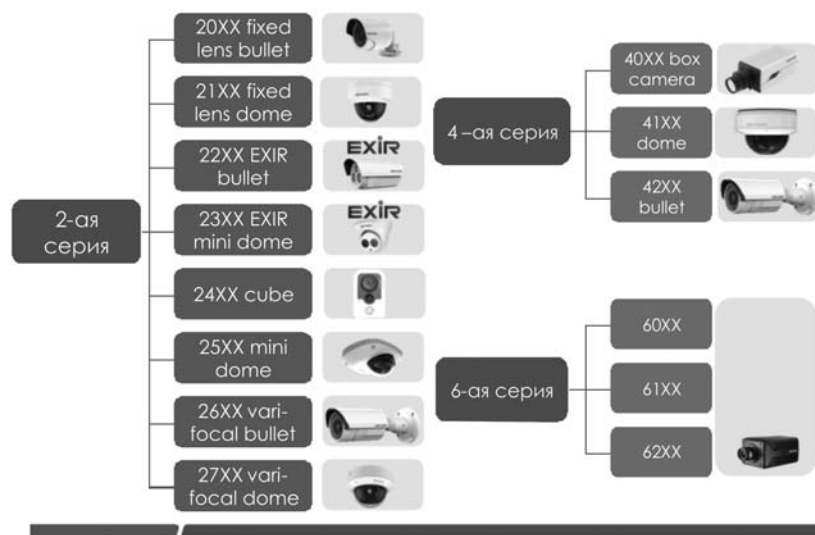
1. Применение уникальных светодиодов (закупаются у компании OSRAM в Германии). Преимущества их использования:

- более яркое, мощное и равномерное ИК освещение, только в одном направлении. Обычный светодиодный кристалл, светит в разных направлениях, а светодиод OSRAM – только в одном направлении, таким образом достигается дальность – до 50 метров.

- увеличенное время работы. Светодиод может работать непрерывно в течение 100 000 часов при температуре 250C. Эти светодиоды защищены от статического электричества.

Способ инкапсуляции – черный кристалл, благодаря этому требуется более низкая температура охлаждения.

Классификация IP камер



HIKVISION

Высокая эффективность при ночном наблюдении



Преимущества инновационной технологии Exir

**DS-2CD2312-I (1,3-Mn), DS-2CD2332-I (3-Mn)
DS-2CD2212-I (1,3-Mn), DS-2CD2232-I (3-Mn)**

Применение кристаллов с увеличенной светоизлучающей способностью
Встроенная грозозащита
Эффективная защита от перегрева
Увеличенный срок службы осветителей
Пониженное энергопотребление
Эволюционная прямоугольная форма линзы для лучшей эффективности освещения
Равномерное распределение света по всей площади кадра

Официальный представитель в Республике Беларусь – ОДО «Авант-Техно» • www.avant.by
г. Минск, ул. Короля д. 45, оф. 16В • тел.: +375 17 200 01 09 • факс: +375 17 226 43 52 • e-mail: cctv@avant.by
ОДО «Авант-Техно», УНН 190423783



Профессиональные решения в компактном исполнении



Новая серия уличных IP-камер с ИК-подсветкой

**DS-2CD2012-I (1,3-Mп), DS-2CD2032-I (3-Mп)
DS-2CD2112-I (1,3-Mп), DS-2CD2132-I (3-Mп)**

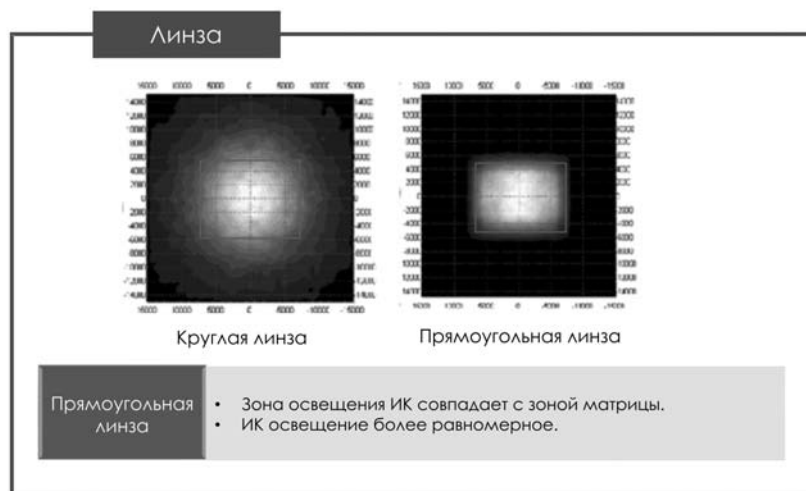
Высокое разрешение до 3 Мп
HD видео в реальном времени
Встроенная ИК подсветка до 30м
Высокоэффективный режим DWDR до 80дБ
Новейшая платформа Type Raptor
Холодный запуск при температуре до -40°C
Полная поддержка ONVIF
Вандалозащищенный корпус, степень защиты Ip66

Официальный представитель в Республике Беларусь – ОДО «Авант-Техно» • www.avant.by
г. Минск, ул. Короля д. 45, оф. 16В • тел.: +375 17 200 01 09 • факс: +375 17 226 43 52 • e-mail: cctv@avant.by
ОДО «Авант-Техно», УНН 190423783



EXIR технология

HIKVISION



2. Использование уникальной прямоугольной линзы, патент на которую принадлежит компании Hikvision.

Прямоугольная линза EXIR – зачем применена такая форма? Следует рассмотреть традиционную ИК подсветку. Круглая линза дает яркое освещение в центре, а в 4-х углах темно, получается неравномерное освещение. При использовании прямоугольных линз, ночью мы получаем более равномерное, мощное, правильно распределенное освещение в разных зонах и еще площадь нашей ИК подсветки совпадает с зоной обзора камеры. Другие компании тоже могут использовать данные светодиоды, однако у них нет такой линзы EXIR.

Умное ИК – это процесс регулирования мощности ИК излучения в зависимости от расстояния до объекта. Функцию SMART IR вы можете настроить, включить/выключить в самом интерфейсе камеры.

Наличие платформы RAPTOR. IP-камеры «2 серии» разработаны на процессорной платформе RAPTOR. RAPTOR – это процессор, разработанный американской компанией Texas Instruments, который значительно улучшил качество

кодирования. Не так давно наша компания приняла новый стандарт кодирования – H.264 hi profile. С этим стандартом мы можем лучше и эффективнее работать в сетях с низкой пропускной способностью и сохранять высокое качество изображения.

Улучшенное качество изображения. Благодаря шумоподавлению

нию и широкому цифровому динамическому диапазону получается отличное изображение. Все камеры второй серии имеют новое трехмерное шумоподавление.

«4 серия»

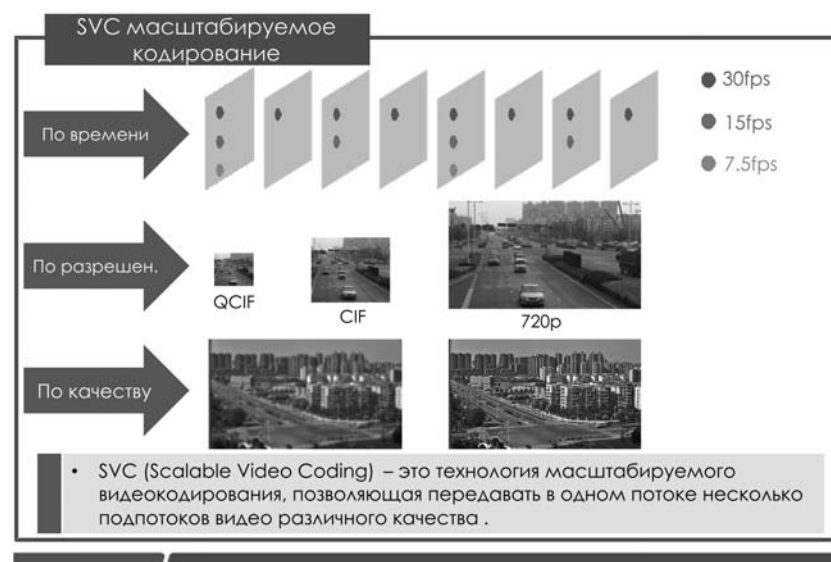
«4 серия» – IP-камеры для профессионального применения, в них Hikvision планирует использовать новые технологии, такие как AOI и SPC. Также будет реализована технология «Тройной поток» и возможность подключения до 20 клиентов к одной камере.

Технологические преимущества для IP-камер «4 серии».

Новый метод кодирования. Вся серия будет поддерживать стандарт h.264 high profile, в дальнейшем планируем перейти на стандарт h.265 – новый стандарт для кодирования видеопотоков. В этот стандарт будет добавлена функция SVC. SVC – это масштабируемое кодирование, которое позволяет передавать в одном видеопотоке несколько подпотоков видео разного качества

«Тройной поток». Многие камеры на рынке поддерживают дуальный поток. Основной поток для записи, отображения в локальной сети, а вторичный поток для отображения с мобильного устройства. В «Тройном потоке» добавлен новый поток, который сможет кодировать при таком же разрешении, как у основного потока (2-3 Мп), при этом вы можете изменить параметры потока.

HIKVISION



Функция AOI. Это алгоритм кодирования для зоны интересов. Иногда в зоне изображения нам интересна не вся информация. Например, в парке стоит автомобиль, а нас интересует только номер, тогда после настройки, для этой зоны (номерной знак) будут включены самые высокие параметры кодирования. И только четвертая серия камер сможет поддерживать эту функцию.

Сетевой доступ. К обычным камерам можно подключиться 5-6 клиентам. В «Четвертой серии», благодаря новой платформе процессора, можно подключить к камере с потоком до 60 Мб/сек и до 20 клиентов. Задержка клиента при камере 2 Мп составит 150 Мс. Если вам нужно уменьшить задержку – включите режим минимальной задержки. В этом режиме камера выключит трехмерное шумоподавление и другие OSP функции, которые не являются основными, для уменьшения задержки изображения.

Технология APN. Технология автоматического регулирования заднего фокуса. После настройки фокуса объектива мы можем изменить задний фокус, регулируя позицию сенсора.

«6 серия»

В Китае уже начата реализация этого оборудования. Позиционируется, как камеры для спецпроектов. Это интеллектуальные камеры с применением видеоаналитики (функции распознавания номеров автомобилей, лиц и пр.).

В «6 серии» будут производиться камеры с рядом эксклюзивных характеристик:

- 2 Мп камеры со скоростью записи 60 кадров в секунду (обычно применяется для наблюдения за дорогой);
- 5 Мп камера, со скоростью записи 25 кадров в секунду
- 8 Мп камера, со скоростью 15 кадров в секунду

Также будут камеры с дополнительными функциями: слежения, панорамная камера и пр.

Камеры оснащены матрицами с большими (1 или 1,8 дюймовыми) сенсорами. Благодаря такому сенсору мы в состоянии получить отличное качество изображения. При недостаточном освещении для этих камер мы можем отдельно подключить прожектор с управлением от нашей камеры.

Технологические преимущества для IP «6 серии»

В «6 серии» есть несколько образцов камер для специального применения. 5 Мп камера RealTime. Обычные камеры дают 5 кадров в секунду при 5 Мп. Камеры «6 серии» сначала делят изображение на 4 части. Затем 4 процессора и 2 чипсета, находящиеся внутри камеры, параллельно обрабатывают изображения в видеопотоки. Получается 5 Мп поток реального времени Real Time. Сегодня на рынке это первая камера, которая предлагает данную технологию.

60 кадров в секунду HD – это тоже специальная камера для серьезного проекта, что значительно увеличивает качество динамической картинки.

Общие уникальные характеристики

Благодаря использованию новейших технологий IP, вся линейка камер Hikvision обладает рядом общих уникальных характеристик:

- Камеры 2, 4 и 6 серии работают без подогрева до – 30 0С, что уже было доказано в ходе тестов и испытаний.

- Вся линейка IP-камер интегрируется в программные платформы всех известных производителей. Поддерживается ONVIF 2.2.

- В оборудовании реализована технология возобновления передачи данных.

- Реализована надежная защита от переотражения при ИК-подсветке благодаря измененной конструкции камер. Существует также защита от царапин, которые отражают ИК подсветку. Все материалы купола создаются из специального сверхпрочного пластика, который защищен от ударов и царапин.

- Высокая степень защиты оболочки. Даже в бюджетной линейке наши камеры поддерживают степень защиты IP67, хотя на спецификациях мы заявляем только IP66, однако в «4 серии» все камеры разработаны со степенью защиты IP67. Высокая степень защиты достигается рядом конструктивных особенностей, например, при изготовлении цилиндрической уличной камеры между крышкой и корпусом находится высококачественная резиновая прокладка, на всех стыках корпуса используется влагозащитный клей. При изготовлении ис-

пользуется 2 слоя стекла, которые также служат защитой. У нас на тесте есть камера, которая уже полгода находится полностью в воде, однако она превосходно работает.

Hikvision серьезно относится к вопросам безопасности: во всех камерах существует авторизация по учетным записям и цифровой водяной знак. При кодировании можно одновременно установить цифровой водяной знак на несколько камер. При воспроизведении вы можете сразу увидеть, с какой камеры и в какое время велась запись.



Клиенты Hikvision часто спрашивают, почему ваши камеры дороже, чем камеры других китайских производителей? Потому что Hikvision своими силами разрабатывает камеры для максимально простого, удобного и надежного использования. Оборудование имеет защищенный дизайн, например интерфейс питания, корпуса камер – цельные, для точной геометрии и надежности сборки и пр. В результате мы гарантируем заявленные характеристики и качество всего оборудования.

Материал подготовлен на основе доклада, сделанного в ходе Первой национальной выставки-форума «Центр безопасности 2013: инженерно-техническая безопасность».

**Официальный дистрибьютор компании
HIKVISION в Республике Беларусь
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



Вопросы комплексной защиты информации: современный подход

Барановский Олег Константинович,
заместитель начальника
по науке центра
испытаний средств защиты
информации и аттестации
объектов информатизации
Государственного
предприятия «НИИ ТЗИ»

Справка ТБ

Барановский О. К. Заместитель начальника по науке центра испытаний средств защиты информации и аттестации объектов информатизации Государственного предприятия «НИИ ТЗИ». Образование высшее, радиофизик, в 1998 г. закончил Белорусский государственный университет. Имеет академическую степень магистра естественных наук, кандидат физико-математических наук. Опыт работы в области защиты информации – с 1998 года по настоящее время.

Одним из факторов устойчивого развития личности, общества и государства является безопасность информационных отношений и поддерживающей инфраструктуры на всех уровнях взаимодействия, причем актуальность данного вопроса со временем лишь возрастает.

Информационная безопасность обеспечивается реализацией комплекса правовых, организационных и технических мер защиты информации. Глобализация информационных отношений требует согласования подходов, способов и мер защиты на межгосударственном и международном уровнях. Одной из форм сотрудничества по указанному направлению является проведение научных, научно-технических и научно-практических мероприятий.

К таковым относится научно-практическая конференция Союзного государства «Комплексная защита информации», которая прошла с 21 по 24 мая 2013 г. на базе Брестского государственного технического университета.



Организаторы мероприятия – Парламентское Собрание Союза Беларуси и России, Постоянный Комитет Союзного государства, аппарат Совета Безопасности Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Федеральная служба по техническому и экспортному контролю Российской Федерации, Межрегиональная общественная организация «Ассоциация защиты информации», Государственное предприятие «НИИ ТЗИ», Брестский областной исполнительный комитет и Брестский государственный технический университет.

информационной безопасности России и Беларуси. На пленарных и секционных заседаниях, за круглым столом заслушали и обсудили более 110 докладов.

В частности, рассмотрены вопросы создания защищенных объектов информационных технологий, технологического и нормативного обеспечения трансграничного обмена юридически значимого электронного документооборота, подготовки специалистов в области информационной безопасности в разных секторах экономики. Наиболее насыщенными стали заседания, посвященные технической и криптографической защите информации.

В ходе конференции обсудили события Союзного государства, в частности, результаты союзных программ в области безопасности информации. В рамках выполнения текущей программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011–2015 годы, утвержденной постановлением Совета Министров Союзного государства от 20 апреля 2012 г. № 6, ведутся



В работе XVIII научно-практической конференции приняли участие свыше 160 ученых, специалистов, представителей государственных органов и практических работников в сфере

научно-исследовательские и опытно-конструкторские работы по следующим направлениям:

– перспективные способы и средства защиты информации при

реализации наукоёмких технологий обработки информации, создание доверенных сред при распределённой обработке информации с использованием информационно-телекоммуникационной среды общего пользования;

- технические решения для оценки защищенности и нейтрализации угроз безопасности информации в критически важных системах информационной инфраструктуры;

- создание инфраструктуры открытых ключей для обеспечения юридически значимого обмена электронными документами между юридическими и физическими лицами Республики Беларусь и Российской Федерации;

- меры по усилению защиты платёжных систем Союзного государства за счёт использования средств высоконадежной нейросетевой биометрической аутентификации;

- меры по повышению защищенности информации, передаваемой по беспроводным каналам передачи данных, в том числе при использовании современных беспроводных технологий 3G, Wi-Fi, WiMAX, ZigBee.

обеспечения встраивания цифровых водяных знаков в графические изображения формата JPEG, в видеофайлы формата MPEG-4, аудиофайлы формата MP-3, файлы мультимедиа других форматов.

Представленные результаты определили новый круг задач для практических специалистов в части защиты информационных систем от утечки сведений конфиденциального характера. Перекрытие (снижение пропускной способности до приемлемого уровня) скрытых каналов передачи данных является необходимым условием подключения систем, обрабатывающих персональные данные, профессиональную тайну и т.п., к сетям общего пользования.

2. Новые вызовы в вопросах защиты информации от утечки за счёт побочных электромагнитных излучений.

Создание национальных и отраслевых центров обработки данных, развитие облачных вычислений позволяет существенно снизить затраты на информатизацию. Между тем, применение тонких клиентов на основе беспроводных технологий для удален-

алисты Беларуси и России.

3. Развитие методов и средств защиты от вредоносных программ и сетевых вторжений.

Современные средства защиты от вредоносных программ и сетевых вторжений реализуют две группы подходов:

- технологии сигнатурного анализа;
- технологии вероятностного анализа, включающие эвристический анализ, поведенческий анализ, анализ контрольных сумм.

Сигнатурный анализ позволяет гарантированно обнаруживать только известные вредоносные программы и сценарии атак. Ни один из применяемых подходов второй группы, ни их совместное использование не обеспечивают уверенного обнаружения неизвестных вредоносных программ и сценариев атак.

Для повышения вероятности обнаружения вредоносных программ и сетевых атак белорусскими учеными предложена система, базирующаяся на интеграции искусственных нейронных сетей и искусственных иммунных систем. Искусственная иммунная система эмулирует основные принципы и механизмы биологической иммунной системы. Нейросетевые детекторы непрерывно эволюционируют и «подстраиваются» под особенности развития вредоносных программ и сетевых атак, позволяя системе защиты адаптироваться к новым реалиям.

4. Развитие современных средств аутентификации.

Создание доверенной среды как при взаимодействии в пределах отдельно взятой организации, так и при межгосударственном информационном обмене требует применения взаимно согласованных мер и средств аутентификации.

Наряду с обсуждением общих аспектов создания и эксплуатации систем, реализующих сервисы электронной цифровой подписи и инфраструктуры открытых ключей, острую полемику вызвали доклады о новом средстве биометрической идентификации пользователя на основе сканирования сосудистого русла ладони руки, технологии аутентификации пользователей по динамике написания рукописных паролей, программно-аппаратных решениях многофакторной аутентификации в массовых технологиях.

В рамках конференции отмечен вклад заслуженных деятелей и молодых ученых в научную и организационную деятельность в сфере защиты



К актуальным вопросам защиты информации участники конференции отнесли следующее:

1. Практические методы применения стеганографии.

В противовес широко обсуждаемым на международном уровне эмпирическим подходам белорусские ученые предложили единую математическую теорию построения и анализа стеганографических алгоритмов и систем, подобную теории К.Шеннона в криптографии.

На основе марковской модели получены оценки надежности вкраплений (необнаруживаемости сообщений стегоаналитиком). Исследования направлены на разработку математических методов, алгоритмов и программного

ного запроса сведений, составляющих коммерческую и профессиональную тайну, информацию о частной жизни физических лиц и персональные данные, требует выработки новых подходов к защите и обработке информации.

Современные технологии размыывают понятие «контролируемая зона», устройства с беспроводным доступом часто используются в агрессивной окружающей среде. Выявление как побочных, так и скрытых каналов утечки информации требует пересмотра методов, показателей, норм и средств оценки защищенности в условиях увеличения полосы и верхней границы частот сигналов. О подходах к решению задач доложили ученые и специ-

Продолжение на стр. 30 →

- органы государственной власти и управления (гражданский персонал) – 20%;

Некоторые цифровые оценки критериев и показателей безопасности:

6. В Беларуси более 1 млн. \$ компании на ИБ не тратят. При этом если взять затраты на ИБ менее 0,1 млн. \$ у 56 % респондентов, то среднемесячные затраты ориентировочно составят – 8,33 тыс. \$.

1. Стеганография: компьютерная стеганография, стеганография и цифровые водяные знаки, атаки на стегосистемы и др.

- в пособии по обучению террориста «Технологич- ный муджахид, учебное пособие для джихада» присут- ствует глава, посвященная использованию стеганогра- фии;

- Так по последним аналитическим источникам информации (например, Virus Bulletin), точность вирусных детекций различными способами (сигнатурным, проактивным/поведенческим, через репутационные on-line сервисы) достигла насыщения (диаграмма 1).



Обзор подготовили:

альных дисциплин УО «Центр повышения квалификации
руководящих работников и специалистов» Департамента

Обнаружение атак

Технология	FPR, %	FNR, %	Нейросетевые подходы	FPR, %	FNR, %
Победитель KDD-99, Bagged Boosting	0,5	25,4	Модульные MLP (изв. атаки)	9	7
Правила	2	10-30	Модульные MLP (неизв. атаки)	18	14
Кластеризация	10	7	MLP	0,8	5,8
K-NN	8	9	MLP	—	0,4
SVM	10	2	Иерархия SOM	1,4	9,3
			Flexible Neural Tree	0,3	1,2

Предложенные РНС-детекторы	FPR, %	FNR, %	ACC, %
РНС-детектор аномалий	12,93	0,36	97,18
РНС-детектор злоупотреблений	0,04	2,73	97,96
Ансамбль из РНС-детекторов аномалий и злоупотреблений	0,02	1,79	98,36
Совокупный РНС-классификатор типов (23 детектора)	1,94	0,14	99,51
Совокупный РНС-классификатор классов (5 детекторов)	3,74	0,01	99,23

Диаграмма 2

охраны МВД Республики Беларусь, к.т.н., подполковник милиции.

2. Бенедиктович И.В., аспирант УО «Белорусский государственный университет информатики и радиоэлектроники», м.т.н.

Распознавание атак

Технология	CR _{det} , %	CR _{probe} , %	CR ₂₁ , %	CR ₂₂ , %
Гауссовский классификатор	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Дерево решений C4.5	97,0	80,8	4,6	1,8
Победитель KDD-99	97,1	83,3	13,2	8,4
Деревья решений	99,8	50,0	33,3	50,0
Банесовы сети	99,7	52,6	46,2	25,0
Нейросетевые подходы	CR _{det} , %	CR _{probe} , %	CR ₂₁ , %	CR ₂₂ , %
Fuzzy NN	100,0	100,0	99,8	40,0
Иерархия PCA	100,0	100,0	97,2	—
Иерархия SOM	96,9	81,3	0,0	1,1
MLP и нечеткая кластеризация	99,9	48,1	93,2	83,3
RBF	98,8	98,0	97,2	—
Flexible Neural Tree	98,8	99,3	98,8	99,9
Предложенный классификатор	CR _{det} , %	CR _{probe} , %	CR ₂₁ , %	CR ₂₂ , %
Совокупный РНС-классификатор типов (23) атак	99,78	95,18	97,60	100,00
Совокупный РНС-классификатор классов (5) атак	99,31	99,12	97,86	100,0

Диаграмма 3

3. Чурюканов С.А., аспирант УО «Белорусский государственный университет информатики и радиоэлектроники», м.т.н. ■

← Начало на стр. 28

Вопросы комплексной защиты информации: современный подход

общих информационных ресурсов Союзного государства. По решению оргкомитета конференции награждены дипломами конференции «За вклад в научную и организационную деятельность в сфере защиты общих информационных ресурсов Союзного государства» Владимир Анищенко, Александр Горбач, Геннадий Емельянов, Анатолий Куц, Юрий Харин и Юрий Язов. В завершение конференции дипломами отмечены пять победителей конкурса докладов молодых ученых.

По результатам работы конференции принята резолюция, в которой участники конференции постановили:

1. Одобрить результаты работы XVIII научно-практической конференции «Комплексная защита информации», выразить благодарность организаторам конференции за высокий уровень ее подготовки и проведения.

2. Опубликовать материалы конференции в отдельном выпуске журнала «Электроника инфо», входящего в список изданий Высшей аттестационной комиссии Республики Беларусь.

3. Провести XIX научно-практическую конференцию «Комплексная защита информации» в 2014 г. в Российской Федерации. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий.

4. Рекомендовать организаторам очередной конференции по согласованию с Постоянным комитетом Союзного государства расширить состав

ее участников и пригласить ученых и специалистов государств-участников Единого таможенного пространства и ОДКБ.

5. Проинформировать руководство Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России об итогах XVIII научно-практической конференции «Комплексная защита информации» и ее предложениях.



Предметный подход к выбору тем для обсуждения, нацеленность на рассмотрение вопросов, имеющих практическую значимость, позволили сделать конференцию «Комплексная защита информации» авторитетной площадкой для обсуждения наиболее

важных задач в области обеспечения информационной безопасности. Это особенно важно в свете анонса предстоящих событий:

- создание в Республике Беларусь так называемого «Государственного облака», которое обеспечит информационное взаимодействие государственных органов и организует работу электронного правительства;
- создание общегосударственной

системы противодействия кибератакам на фоне повышения числа зарегистрированных инцидентов, связанных с несанкционированным доступом к ресурсам государственных органов и организаций, частных компаний на территории республики. ■



Основные тренды развития телекоммуникаций, информационного пространства и защиты информации в Республике Беларусь

Капариха Сергей Николаевич,
Оперативно-аналитический центр при Президенте
Республики Беларусь, заместитель начальника центра.

Современный этап развития информационного пространства в нашей стране характеризуется активным строительством информационно-телекоммуникационных систем как межгосударственного уровня, так и между деловыми кругами Беларуси и России. В качестве примера можно привести информационные сети таможенных и налоговых органов, служб пенсионного обеспечения, МВД и пр. ведомств. Активно развивается взаимодействие банковских структур в этой сфере, более того, для ряда белорусских банков процессинговые услуги предоставляют российские банки.

Необходимо отметить устойчивый тренд российско-белорусского сотрудничества по реализации телекоммуникационных проектов в инфраструктурной области. Как пример, РУП «Национальный центр обмена трафиком» совместно с ОАО «Ростелеком», завершены работы по созданию высокоскоростной транзитной магистрали Москва–Минск–Франкфурт с пропускной способностью 1,2 Тбит/с, с возможностью расширения до 8 Тбит/с. Данная магистраль является кратчайшим путем и надежной средой для передачи трансконтинентального трафика между Европой и Азией. Все работы закончены, заключены первые договора, связанные с реализацией данного проекта.

В декабре 2012 года создано белорусско-российское предприятие СООО «Белорусские облачные технологии», которое предназначено для реализации ряда новых инновационных проектов в сфере информационно-коммуникационных технологий. Одним из реализуемых данным предприятием проектов будет построение опорной сети передачи данных для единой республиканской сети передачи данных, которая объединит в единую систему существующие сети передачи данных и позволит операторам значительно

расширить спектр оказываемых услуг на базе инфраструктуры единой республиканской сети передачи данных. Предприятие будет решать вопросы, связанные с построением сертифицированного республиканского центра обработки данных, на базе которого планируется создание т.н. «государственного облака», предназначенного обеспечить информационное взаимодействие государственных органов и иных государственных организаций, работу электронного правительства, существенно сократить расходы республиканского бюджета на модернизацию и обслуживание государственных информационных систем.

Также одним из проектов в этой области является создание единой сети сотовой подвижной электросвязи по технологии LTE, которая, используя инфраструктуру опорной сети передачи данных, обеспечит конечному рынку потребителей высокоскоростной доступ к услугам РЦОД и телекоммуникационных услугам.

Объединенные ресурсы единой сети сотовой подвижной электросвязи по технологии LTE и республиканского центра обработки данных предоставят возможность сократить не только сроки, но и капитальные и эксплуатационные затраты при создании как интеллектуальной транспортной системы г. Минска и других городов Республики Беларусь, так и системы мониторинга общественной безопасности.

Строительство участка транзитной магистрали сети электросвязи по территории Республики Беларусь, проходящего через г. Гомель и г. Брест, с высокой пропускной способностью обеспечит резервирование магистрали проходящей по маршруту г. Витебск – г. Гродно, высокую надежность и безопасность каналов доступа к международным ресурсам сети Интернет, а также выход на рынок Китая и Республики Казахстан.

Сейчас мы можем уверенно утверждать, что единое информационное пространство Беларуси и России стало реальностью, а защита пространства является одной из приоритетных задач по обеспечению безопасности государств.

Приоритетным направлением в данной области является защита информации в наиболее важных системах информационной и телекоммуникационной инфраструктурах, оказывающих существенное влияние на безопасность союзного государства в информационной сфере.

В рамках союзных программ проведены исследования и разработаны нормативно-методические документы, определяющие основные требования к организации такой деятельности. Используя эти результаты, в республике приняты акты законодательства, заложившие основы защиты критически важных объектов информатизации. Системообразующим документом в этой области является Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». Данный нормативный правовой акт определил порядок отнесения объектов информатизации к критически важным и обеспечения безопасного функционирования их.

В условиях интеграции кибернетического пространства Союзного государства в мировое информационное пространство, образуемого, в первую очередь, международной компьютерной сетью интернет, именно критически важные объекты информатизации являются объектами кибератак. Это подтверждается и результатами анализа, который проводил Оперативно-аналитический центр.

В последнее время отмечается повышение активности кибератак на информационные системы Беларуси, как государственного сектора, так и бизнес сообщества. Целью этих атак становятся информационные ресурсы в экономике, обороне, международной политике, науке, технике, а также персональные

данные граждан республики. С помощью вредоносного программного обеспечения, происходит внедрение вредоносных программ на компьютеры и предпринимаются попытки хищения информации. Центром нейтрализованы неоднократные попытки несанкционированного доступа с применением специализированного вредоносного программного обеспечения к информационным ресурсам в ряде государственных органов и организаций, в сферу компетенции которых входят различные сферы деятельности, в том числе политическая, экономическая, оборонная и научно-техническая.

Мы наладили тесное взаимодействие почти со всеми государственными органами и удаленно обеспечиваем безопасность тех ресурсов, которые находятся в информационной среде государственных структур. Результативная защита информационных систем стала возможной благодаря созданию общегосударственной системы противодействия. Данная система включает в себя механизм выявления попыток фактов несанкционированного доступа к информации. Система позволяет вести работу по оценке целевых атак на конкретные государственные органы. Обеспечивается выявление массового заражения информационных систем вредоносным ПО на ранних этапах и эффективное противодействие таким атакам. По нашему убеждению, с учетом распространенности сети интернет, любые решения по противодействию кибернападениям, ограниченные в рамках национального сегмента в данной сети, обречены на неудачу. С учетом этого Оперативно-аналитический центр организует взаимодействие с иностранными организациями, осуществляющими подобного рода противодействия информационным угрозам в различных странах мира.

Если говорить о России – это тесное взаимодействие с «Лабораторией Касперского», по расследованию функционирования международной компьютерной сети, атаки из которой как раз и были направлены на информационные системы, содержащие информацию о научно-технических разработках, анализе экономической деятельности, сферах государственного управления и банковского сектора.

Полагаем, что данное направление совместной деятельности с нашими российскими коллегами должно стать одним из приоритетных в деле обеспечения безопасности информационного пространства.

Одной из перспективных задач по защите союзного информационного пространства является создание в

сети интернет трансграничного пространства доверия РБ – РФ. Для этого в рамках совместных с Россией научно-исследовательских и опытно-конструкторских работ запланировано создание программно-аппаратных платформ удостоверяющего центра для международного взаимодействия, доверенных центров обеспечения электронного документооборота, а также разработка нормативно-правовой базы. Заказчиком проекта с Белорусской стороны является государственное предприятие «Национальный центр электронных услуг» (НЦЭУ), на базе которого будут реализовываться эти проекты.

Необходимо также отметить, что в рамках данных проектов предусматривается предоставление сервисов доверенной третьей стороны. Взаимодействие организаций Республики Беларусь и Российской Федерации не ограничивается разработкой средств защиты информации и нормативно-методической документации. Не менее важным фактором является формирование согласования вариантов и подходов к решению проблем защиты информации в сфере управленческой деятельности и развития законодательства.

В частности, опыт Российской Федерации по регулированию деятельности в области защиты информации был принят во внимание при разработке Указа Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации». Данный законодательный акт стал системным документом, который выстроил строгую систему управления в области технической и криптографической защиты информации в Республике Беларусь.

В частности, Указ определил объекты, на которых осуществляется техническая и криптографическая защита информации, а также субъектов, обязанных осуществлять ее применение. Определены порядок технической и криптографической защиты, а также полномочия Оперативно-аналитического центра по регулированию данной деятельности.

Возможно, стоит подумать над вопросом о более тесном взаимодействии между субъектами России и Беларуси по применению доверенных средств защиты информации, оцененных в рамках национальных систем подтверждения соответствия. Подобные примеры в мировой практике имеются. Например, проект по использованию международных стандартов, известных в среде специалистов по IT-безопасности как «Общие критерии». Суть данного проекта заключается в том, что страны, подписавшие соответствующее соглашение,

признают результаты оценки продуктов и систем в области IT-технологий в специально аккредитованных лабораториях (это не обязательно лаборатории этих стран) и принимают их во внимание при защите национальных информационных ресурсов. Такой проект не простой, но может оказаться весьма перспективным для Союзного государства с точки зрения создания полноценного доверенного реестра средств обеспечения информационной безопасности, позволяющего создавать системы защиты информации, учитывающие максимально широкий спектр угроз.

Важнейшим фактором успеха обеспечения информационной безопасности является наличие высококвалифицированных кадров, способных создавать системы защиты информационных ресурсов, разрабатывать современные программные и программно-технические решения, обеспечивать их грамотное применение.

Есть примеры сотрудничества заинтересованных структур Республики Беларуси и России. Мы отмечаем высокое качество учебного процесса в Российских учебных заведениях, где проходили обучение сотрудники нашего центра. Это и Московский государственный университет имени М.В.Ломоносова, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России.

В то же время в нашей стране развивается ВУЗовская система подготовки и повышения квалификации кадров в сфере информационной безопасности. Подготовка специалистов осуществляется в ряде ВУЗов страны, например в Брестском государственном техническом университете.

Приоритетным среди специальностей выделяется направление обеспечения компьютерной безопасности, в том числе криптографической защиты информации. Именно выпускники с данными специальностями сегодня востребованы в государственном управлении, финансовом секторе, промышленной сфере, сфере национальной безопасности. И наш профессорско-преподавательский состав смог бы предложить свои программы для российских слушателей. Надеюсь, что приведенные примеры по совместной деятельности по защите информационного пространства союзного государства зададут определенный настрой для участников конференции.

(материал подготовлен на основе доклада, сделанного на конференции КЗИ 26 мая 2013 года, г. Брест). ■



Значение и результаты развития информационно-коммуникационных технологий в Беларуси

Более подробно об основных тенденциях развития телекоммуникаций, информационного пространства и защиты информации в Республике Беларусь мы говорили с Капарихой Сергеем Николаевичем.

Каковы основные причины и какое значение для государства имеет создание РУП «Национальный центр обмена трафиком»?

Ранее на национальном телекоммуникационном рынке де-факто и де-юре существовало исключительное право РУП «Белтелеком» на присоединение к сетям электросвязи иностранных государств и пропуск международного трафика. Это право непосредственно влияло на условия оказания МНОГИХ востребованных услуг электросвязи, например, доступ к сети Интернет. Сравнение с передовыми странами в сфере ИКТ по скорости и стоимости доступа к Интернету было не в нашу пользу. Вот почему уход от монополии был назревшей необходимостью. Но не менее важен был и другой вопрос: как уйти от монополии? Можно было бы просто открыть рынок для всех желающих компаний из нашей страны и из-за рубежа. Но желающих могло не быть, а если бы они были, то просто бы «сняли сливки» с самого доходного рыночного сегмента, ничего не сделав для развития телекоммуникационной инфраструктуры в самой Беларуси. Вот почему в нашей стране было решено создать предприятие, сопоставимое с РУП «Белтелеком» по эксплуатируемой транспортной инфраструктуре, как на трансграничных направлениях, так и внутри государства. С этой целью и было образовано республиканское унитарное предприятие «Национальный центр обмена трафиком» (НЦОТ).

Сегодня де-юре монополии «Белтелекома» нет, но де-факто пока она остается. Связано это с тем, что становление деятель-

ности НЦОТ требовало привлечения значительного объема инвестиций. К настоящему времени эта задача решена, что позволит реализовать все направления деятельности данного предприятия, предусмотренные законодательством.

Какова роль РУП «Белтелеком» в данном проекте?

Как важнейшего участника. РУП «Белтелеком» имеет наибольшее число пользователей услуг электросвязи, крупнейшую в нашей стране быстро развивающуюся сеть, которая в соответствии с законодательством будет взаимодействовать с единой республиканской сетью передачи данных (ЕРСПД). Без такого взаимодействия задачи деятельности ЕРСПД были бы невыполнимы. Безусловно, при оказании некоторых услуг электросвязи НЦОТ будет конкурировать с национальным оператором электросвязи. Задача ОАЦ в качестве независимого регулятора в сфере информационно-коммуникационных технологий состоит в том, чтобы конкурентная борьба велась в интересах пользователей услуг и на благо развития ИКТ-сферы, а не в узко корпоративных целях.

Каковы особенности и значение проекта по созданию межнациональной скоростной магистрали Москва-Минск-Франкфурт?

Эта магистраль является кратчайшим путем и надежной средой для передачи трансконтинентального трафика между Европой и Азией. Ее пропускная способность составляет 1,2 Тбит/с с возможностью расширения до 8 Тбит/с. Создание такой оптоволоконной «трубы» позво-

ляет нашей стране использовать выгоды своего географического положения. Все работы по созданию и техническому оснащению магистральной линии связи завершены, сейчас заключаются межоператорские соглашения для обеспечения наиболее полного использования ее ресурса.

Может ли эта магистраль стимулировать создание ЦОД в стране и превратить Беларусь в поставщика «облачных услуг»?

Создание центров обработки данных, в частности республиканского центра обработки данных, ведется, в первую очередь, для удовлетворения потребностей белорусских пользователей услуг. Однако ничто не препятствует предлагать наши возможности и для нужд иностранных пользователей. Необходимые вычислительные, сетевые и кадровые ресурсы для этого будут созданы. Дело за маркетинговой политикой.

Есть ли планы и возможности по использованию «государственного облака» под требования инженерно-технических систем безопасности (охраны, видеонаблюдения, контроля доступа и пр.)?

Создание так называемого «государственного облака» начинается на базе Республиканского центра обработки данных и призвано обеспечить информационное взаимодействие государственных органов и иных государственных организаций и оказание ими электронных услуг. Реализация этого проекта поможет решению нескольких существенных задач: освободить владельцев информационных ресурсов от необходимости их

эксплуатации собственными силами, сократить государственные расходы, улучшив качество и повысив технический уровень обслуживания. Сетевая и вычислительная инфраструктуры, которые начнут создаваться в ближайшее время, безусловно, могут быть использованы и для нужд функционирования систем мониторинга общественной безопасности. Например, единая сеть сотовой подвижной электросвязи по технологии LTE прекрасно подходит для целей организации систем видеонаблюдения с удаленных объектов. Задача № 1 при проектировании Республиканского центра обработки данных – обеспечить безопасность размещаемых в нем ресурсов.

На какой структурной базе будет создаваться сеть LTE?

Предполагается, что подсистемы базовых станций, коммутации и другие элементы инфраструктуры сети LTE вторичного уровня будут создаваться в рамках инвестиционного проекта, с использованием на договорной основе сооружений действующих операторов сотовой подвижной электросвязи. В качестве транспортной сети будет использоваться инфраструктура ЕРСРД. В ближайшее время во взаимодействии с оператором «Мобильные ТелеСистемы» будет создана тестовая зона эксплуатации сети LTE, а со следующего года планируется начать коммерческое оказание услуг.

Крупнейшие мировые державы, страны СНГ заявили о создании национальных центров противодействия киберугрозам. Как вы оцениваете перспективу и необходимость появления таких центров в Республике Беларусь?

ОАЦ, в силу возложенных на него законодательством задач и функций, фактически является национальным центром противодействия киберугрозам. Дело не в официальном статусе или названии, а в эффективности работы. ОАЦ нейтрализовывал неоднократные попытки несанкционированного доступа к применению специализированного вредоносного программного обеспечения к информационным ресурсам в ряде государствен-

ных органов и организаций. Мы совершенствуем систему защиты критически важных объектов информатизации, наладили тесное взаимодействие с государственными органами и удаленно обеспечиваем безопасность тех ресурсов, которые находятся в их информационной среде. ОАЦ взаимодействует с организациями иностранных государств, ведущими борьбу с киберугрозами, без этого наша работа была бы неэффективной.

Какие новые нормативные акты, существенно влияющие на национальный сегмент информационной безопасности, можете отметить?

Назову Указ Главы государства № 196 от 16 апреля 2013 г. «О некоторых мерах по совершенствованию защиты информации», которым утверждено Положение о технической и криптографической защите информации в Республике Беларусь. Это концептуальный, всеобъемлющий документ. В нем определены либо уточнены основные термины и их определения, полномочия должностных лиц и госорганов в этой сфере, процедуры осуществления технической и криптографической защиты информации и контроля за ней.

Каковы задачи, значение для государства созданного республиканского унитарного предприятия «Национальный центр электронных услуг» (НЦЭУ)?

Деятельность НЦЭУ призвана объединить на основе Общегосударственной автоматизированной информационной системы межведомственные информационные системы, которые ранее эксплуатировались различными госорганами, что поможет к 2016 году отказаться от традиционной бумажной переписки в сфере государственного управления. Для широкого круга граждан и юридических лиц НЦЭУ через единый портал электронных услуг предоставит доступ ко всем услугам, оказываемым госорганами в электронном виде. Этот портал станет электронным «одним окном». Он освободит жителей Беларуси от необходимости посещения государственных учреждений и ожидания в очередях. Услуги, предоставляемые

через портал, будут доступны с персональных компьютеров пользователей, подключенных к сети Интернет, либо через абонентские терминалы, установленные в организациях, уполномоченных выполнять функции информационных посредников. Переход к оказанию всех услуг в электронном виде через единый портал электронных услуг, в соответствии с решением Правительства, должен быть также закончен в 2016 году.

Опыт каких стран использовался при создании белорусского НЦЭУ?

Мы рассматривали достижения в области «электронного правительства» стран почти из всех регионов мира, понимая, что просто скопировать иностранный опыт не получится. Этот опыт оказался успешнее там, где мероприятия планировались с учетом специфики функционирования системы государственных органов, особенностей социально-экономического развития страны. К нам приезжали эксперты из Республики Корея, которая в международных сравнениях занимает лидирующие позиции по уровню развития ИКТ. Данные ими оценки подтвердили, что мы находимся на верном пути. Специалисты ОАЦ знакомилась с концепцией и практикой развития «электронного правительства» в Республике Татарстан Российской Федерации, где эти процессы организовывал нынешний российский министр связи и массовых коммуникаций Никитин, Китае и Индии. Безусловно, не обошлось вниманием и опыт Европейского союза, где реализуется комплексная стратегия «цифрового» развития до 2020 года.

Каковы основные приоритеты в политике и в работе ОАЦ?

Выполнение всех доверенных Центру задач является одинаково важным для нас. Акценты по каждой из них расставил при его посещении 7 июня текущего года Глава нашего государства. Говоря о нашей деятельности в этой сфере, он напомнил о необходимости работать на опережение, а также о готовности противостоять угрозам информационной безопасности. Этим указаниям мы будем следовать в нашей работе. ■



Symantec Technology Day 2013

5 июня 2013 года корпорация Symantec при поддержке дистрибьютора Софтпром-Бел провела свою ежегодную конференцию SymantecTechnologyDay.

Открывая мероприятие, Алексей Кочнев, менеджер по развитию бизнеса Symantec в Республике Беларусь, отметил, что основными элементами успеха являются «наши заказчики, наши технологии и наши партнеры... компания Symantec будет продолжать равномерно развивать эти три составляющие». Конференция (уже второй год) становится заметным событием для отечественных специалистов в области обеспечения защиты и управления корпоративными данными. Весь день белорусские заказчики имели возможность получить достоверную информацию об актуальных технологиях лидера мирового рынка информационной безопасности и обсудить свои проекты с техническими экспертами.

По словам Андрея Вышлова, главы представительства Symantec в Рос-

сии и СНГ, Беларусь на текущий момент является самым перспективным и активно развивающимся регионом в странах СНГ, и корпорация рассчитывает на дальнейший рост своего присутствия в стране.

Актуальные тренды, технологии (информационный обзор по итогам семинара)

Группа Anonymous заявила о планах запуска 20 июня 2013 года кампании под названием OpPetrol, целью которой станут международные газовой и нефтепромышленные предприятия. Эта новость была анонсирована 11 мая 2013 года, вскоре после того, как стартовала другая кампания этой группы – OpUSA.

Специалисты группы Symantec Security Response отслеживают эти угрозы при помощи глобальной аналитической сети – Symantec Global Intelligence Network. Они обнаружи-

ли, что организованные атаки такого типа часто похожи и могут включать в себя следующие элементы:

- DDoS- атаки;
- взлом аккаунтов в социальных сетях и их порча или рассылка поддельных сообщений;
- взлом веб-сайтов организаций и их порча, кража информации и ее публикация, как доказательство взлома;
- взлом серверов организаций и попытки их саботажа, например, установка ПО, стирающего все данные.

Эксперты Symantec рекомендуют компаниям проводить мониторинг своих сетей на предмет необычного поведения, а особенно – любых попыток нарушения внешнего периметра.

Причина большинства утечек информации – сбои системы и человеческий фактор

Корпорация Symantec и институт Ponemon Institute опубликовали результаты совместного исследования 2013 года «Оценка стоимости утечки информации: глобальный анализ» (2013 Cost of Data Breach Study: Global Analysis). Данные указывают на то, что системные сбои и человеческий фактор стали причиной 2/3 всех утечек информации и подняли средний мировой показатель убытка от кражи 1 учетной записи до 136 долларов США. В список ключевых факторов вошли непонимание сотрудниками, что является конфиденциальной информацией, недостаточность системного контроля (средств управления системой), а также несоблюдение государственных и отраслевых нормативов. В таких строго регулируемых отраслях, как здравоохранение, экономика и фармацевтика, убытки от утечки информации оказались в среднем на 70% выше.

Средняя по миру убыточность скомпрометированной записи возросла, при этом цена одного инцидента утечки в США снизилась до \$5,4 млн. Такое снижение связано с распространенностью должности руководителя отдела IT-безопасности (Chief Information Security Officer, CISO), отвечающего за безопасность на уровне всей компании, а также с формированием планов реагиру-

Системные сбои и человеческий фактор стали причиной 2/3 всех утечек информации и подняли средний мировой показатель убытка от кражи 1 учетной записи до 136 долларов США.



Корпорация Symantec сообщает подробности о запуске кампании OpPetrol, которая нацелена на предприятия нефте- и газовой отрасли по всему миру. Эксперты Symantec отслеживают эти атаки и готовы ответить на вопросы, касающиеся OpPetrol и DDoS-атак в целом.

ния на инциденты и усилением программ безопасности в целом.

«И хотя злоумышленники с их новыми методами взлома могут нанести большой вред компаниям, сами сотрудники представляют угрозу, которая может оказаться столь же неожиданной и разрушительной. Восемь лет исследований убытков от утечек информации позволяют нам сделать вывод о том, что на сегодняшний день действия самих работников – одна из самых серьезных угроз безопасности компании», – сказал Ларри Панемон (Larry Ponemon), президент Ponemon Institute.

«Компании, серьезно относящиеся к безопасности и имеющие надежный план реагирования на инциденты, на 20% снижают свои убытки от утечек информации, что не оставляет сомнений в важности комплексного подхода к этому вопросу. Компании обязаны защищать конфиденциальную информацию своих клиентов вне зависимости от ее размещения, будь то ПК, мобильное устройство, корпоративная сеть или же дата-центр», – отметил Анил Чакраварти (Anil Chakravarthy), старший вице-президент подразделения Information Security Group Symantec.

Восьмой ежегодный глобальный отчет основан на данных об утечках информации у 277 компаний в 9 странах мира: США, Великобритании, Франции, Германии, Италии, Индии, Японии, Австралии и Бразилии. Отчеты по каждой из стран, а также общий отчет можно найти по ссылке. (<http://bit.ly/10FjDik>) Все рассмотренные случаи утечек случились в 2012 календарном году. Для того, чтобы избежать искажений, в исследовании не учитывались огромные утечки с кражей более 100 тыс. учетных записей.

Компании могут оценить свой собственный риск утечки при помощи нашего калькулятора риска утечки информации, который учитывает размер организации, отрасль, месторасположение, а также применяемые методы защиты и дает оценку

как в масштабе учетной записи, так и всей организации.

Основные выводы исследования:

Средняя цена утечки информации сильно различается в разных странах. Многие из этих различий связаны с типами угроз, с которыми организации приходится иметь дело, а также со спецификой законодательства по защите информации в конкретной стране. В некоторых странах, таких как Германия, Австралия и США, законодательство в области защиты потребителей более развито, что обеспечивает большую конфиденциальность данных и общую кибербезопасность.

США и Германия пока отличаются самой высокой стоимостью утечки: в среднем \$188 и \$199 за каждую скомпрометированную учетную запись и \$5,4 млн. и \$4,8 млн. соответственно за каждый инцидент утечки.

Ошибки людей и систем – главные причины утечек. Человеческий фактор и системные ошибки являются причиной 64% утечек по всему миру, при этом, как показало проведенное ранее исследование, 62% сотрудников компаний считают приемлемым перемещение корпоративных данных за пределы компании и большинство сотрудников никогда не удаляют данные, способствуя, таким образом, утечкам. Все это дает представление о том, какую роль в утечках информации играют сами сотрудники компаний, и какие убытки эти компании впоследствии несут. В наибольшей степени влиянию человеческого фактора подвержены бразильские компании. А компании в Индии чаще всего становятся жертвами утечек, связанных с системными сбоями и нарушениями бизнес-процессов. Системные сбои включают в себя сбои приложений, случайные выгрузки данных, логические ошибки при передаче данных, ошибки идентификации (неправо-

мерный доступ), ошибки восстановления данных и др.

Хакерские атаки обходятся дороже всего. Консолидированные исследования показывают, что преднамеренные атаки являются причиной 37% всех утечек информации в мире, при этом во всех исследованных странах эти утечки оказываются самыми дорогостоящими. Компаниям из США и Германии хакерские атаки обходятся дороже всего – \$277 и \$214 за каждую скомпрометированную учетную запись. В то время как в Бразилии и Индии эта цифра составляет лишь \$71 и \$46 соответственно. Помимо того, немецкие компании вместе с компаниями в Австралии и Японии больше всего подвержены риску стать жертвами хакерской атаки.

Некоторые организационные факторы приводят к снижению расходов. Компаниям в США и Великобритании удалось добиться наибольшего снижения расходов при утечках за счет сильной стратегии в

отношении информационной безопасности, наличия плана реагирования на инциденты и назначения руководителя отдела IT-безопасности. США и Франция также снизили расходы за счет привлечения сторонних консультантов по расследованию утечек.

Специалисты компании Symantec рекомендуют придерживаться лучших практик, направленных на предотвращение и снижение цены утечек:

- Обучение персонала правилам работы с конфиденциальной информацией;
- Использование системы предотвращения утечек, позволяющих распознавать конфиденциальную информацию и препятствовать ее утечке за пределы компании;
- Внедрение надежных систем шифрования и строгой аутентификации;
- Подготовка плана реагирования на инциденты, включающего адекватные шаги по оповещению клиентов. ■

Информация о компаниях

Symantec Corporation



Сайты: www.symantec.ru

Год основания: 1982 г.

Контактные лица: Кочнев Алексей Михайлович, менеджер по развитию бизнеса в Республике Беларусь.

Производство: программные средства защиты информации и обеспечения высокой доступности данных.

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 г.

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. Продукция Hikvision обеспечивает безопасность различных сфер деятельности во всем мире, включая розничную торговлю, аэродромы, железные дороги, банки, промышленные предприятия, стадионы и т.д.

Бастион – широкий ассортимент источников питания.

НВП Болид – производитель интегрированных охранных систем.

Avicam Electronics – видеокамеры, видеорегистраторы, объективы и сопутствующее оборудование.

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

Контактное лицо: Лисовский Дмитрий Васильевич, коммерческий директор.

Производство: программное обеспечение.

Поставка:

- интегрируемая платформа безопасности с распределенной архитектурой «Интеллект»;
 - модуль контроля кассовых операций POS-Интеллект;
 - модуль интеграции ОПС иСКУД;
 - 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;
 - цифровая система видеонаблюдения нового поколения: Аххон Next.
- Дистрибьютор компаний: ITV | AxxonSoft.

Аларм, НТ ЗАО



220141, г. Минск, ул. Ф.Скорины, 51 литер Ж, комн. 308а

Тел.: (017) 285-94-01, 267-47-67

Факс: (017) 285-93-59

Сайт: www.alarm.by

Год основания: 1993 г.

УНП: 100435764

Контактное лицо: Матусевич Анатолий Адамович, директор.

Сертификаты:

Сертификат работ и услуг собственного производства № 3/1221-2 от 17 марта 2009 г., выдан ТПП на выполнение монтажных и пусконаладочных работ по установке оборудования из состава ретранслятора «Алеся» (КЛТ-20) 0 (100) и УТОИ -01 на АТС; № 3/1221-3 на выполнение монтажных и пусконаладочных работ по установке оборудования из состава ПЦН «Алеся» («Алеся-01А», «Алеся-01», «Алеся-01П»).

Производство:

- приборы приемно-контрольные охранные «Аларм-3», исп. А, В, Г;
- приборы приемно-контрольные охранно-пожарные: ППКОП «Аларм-5», ППКОП «Аларм-5/4», ППКОП «Аларм-7»;
- приборы приемно-контрольные пожарные: ППКП «Аларм-8», ППКП «Аларм-8/4», «Аларм-9» (16-32 ШС);
- устройства и системы передачи извещений: система передачи извещений о проникновении и пожаре автоматизированная «АСОС Алеся»;
- ретрансляторы: Ретранслятор «Аларм»;
- модуль «Аларм-Ethernet», модуль сопряжения «Аларм GSM 2» исп. А, Б, «Аларм GSM 3» исп. А, Б;
- пультовое оборудование ПЦН для охраны объектов по каналам сотовой связи стандарта GSM.

Услуги:

Проектирование, монтаж, наладка и техническое обслуживание средств и систем охраны; монтаж, наладка и техническое обслуживание систем автоматической пожарной сигнализации; работы по установке и наладке программного обеспечения «Алеся-01 П» для организации АРМ ДПС из состава ПЦН СПИ мониторинга средств ПА. Настройка Windows Server Standard 2003 с установкой программного обеспечения «Алеся-01П» из состава ПЦН СПИ мониторинга средств ПА; гарантийный и послегарантийный ремонт приборов и систем.

Поставка:

Извещатели, аккумуляторы 1,2—18 А.ч, оповещатели (светозвуковые, звуковые), провода, короба-каналы, блок питания, блок резервного питания, сигнализаторы, оборудование видеонаблюдения, в том числе по каналам GSM.

Выполненные проекты:

Проектные, монтажные и пусконаладочные работы по установке ретрансляторов «Алеся», «Аларм», размещение оборудования СПИ «АСОС Алеся» на площадях АТС для подразделений Департамента МВД РБ и крупнейших предприятий РБ. Система передачи извещений о проникновении и пожаре на объектах РУП «Белтелеком» г. Минска с дополнительными функциями контроля показаний электросчетчиков.

Альфа Портал, ООО

224014, г. Брест, ул. Писателя Сергея Смирнова, 165/1

Тел.: (0162) 20-86-13, (029) 725-45-30, (029) 326-46-76

E-mail: info@microdigital.by

Сайт: www.microdigital.by

Год основания: 2007 г.

УНП: 290479641

Контактные лица:

- Громик Ирина, специалист по сбыту;
- Войтухович Ирина Васильевна, директор.

Производство: полный комплекс продукции для CCTV и IP-видеонаблюдения.

Услуги: прямые поставки в Республику Беларусь продукции для CCTV и IP-видеонаблюдения.

Поставка: прямые поставки в Республику Беларусь полного комплекса продукции для CCTV и IP-видеонаблюдения.

Дистрибьютор компаний: MICRODIGITAL Inc.

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 г.

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);
- Softbay Inc. (Корея);
- 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 г.

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 (СКС), компьютерных сетей с использованием витой пары и волоконно-оптического кабеля, учреждений автоматических телефонных станций (мини-АТС), систем и сетей громкоговорящей, диспетчерской связи.

Дивитек, ООО

220123, г. Минск, ул. Кропоткина, д.110, пом. №2Н

Тел.: (017) 334-40-13, (017) 334-43-36, (044) 561-21-61 Velcom

E-mail: divitec.by@gmail.com

Skype: divitec.by

Сайт: www.divitec.by

Год основания: 2013 г.

УНП: 192001897

Контактные лица:

- Корда Андрей Николаевич, директор;
- Устинов Александр Александрович, менеджер.

Услуги: подбор и продажа систем видеонаблюдения.

Поставка: видеорегистраторы, видеокамеры, сетевое оборудование, приемопередатчики

Дистрибьютор компаний: DIVITEC, HIKVISION, ActiveCam, GeoVision, SOVA, НомерОК, TWIST, SC&T, TFortis

Компания ООО «Дивитек» является авторизованным партнёром компании «Контур-КСБ» г. Москва и компании ООО «Сервис Систем Безопасности» г. Москва по оборудованию для систем видеонаблюдения и безопасности на территории Республики Беларусь.

Дополнительная информация: интернет-магазин www.divitec.by

ИНТЕС, Инновационная компания ООО

220013, г. Минск, ул. Кульман, 2-311

Тел./факс: (017) 209-80-88, 209-84-84

E-mail: its@intes.by

Сайт: www.intes.by

Год основания: 2005 г.

УНП: 190649255

Контактные лица:

- Коваленко Валерий Андреевич, директор;
- Демидов Феликс Валерьевич, руководитель службы систем безопасности.

Лицензия: № 02010/6916 до 04.05.2021 г. МВД РБ.

Услуги: проектирование, поставка, монтаж, пуско-наладочные работы, техническое обслуживание.

Поставка:

- видеонаблюдение: ООО «Торговый дом ИСС» (тм. «ISS»), ООО «ЭРВИ групп» (тм. «RVI»);
- платежно-пропускные системы: ООО «Разработка информационных систем» (тм. «ISD»), ЗАО «Интеротель Лтд.» (тм. «INTER HOTEL»);
- система контроля доступа: ООО «Завод ПЕРКО» (тм. «PERCO»);
- ERP-системы: ЗАО «ИФС СНГ» (тм. «IFS»);
- металлодетекторы: ООО «МЦБ РИМИ» (тм. «Rimi»).

Выполненные проекты: МКСК «Минск-Арена», ГКПУ «Минский зоопарк», РУП «МАЗ», ОАО «БАТЭ», Управление юстиции Мингорисполкома, ООО «Табак-Инвест» и др.

Дистрибьютор компаний: ООО «Торговый дом ИСС» (тм. «ISS»), ООО «ЭРВИ групп» (тм. «RVI»), ООО «Разработка информационных систем» (тм. «ISD»), ЗАО «Интеротель Лтд.» (тм. «INTER HOTEL»), ЗАО «ИФС СНГ» (тм. «IFS»), ООО «ООО МЦБ РИМИ» (тм. «Rimi»), ООО «Завод ПЕРКО» (тм. «PERCO»).

«PERCo») и др.

Дополнительная информация: ЕАСОП «Единая автоматизированная система оплаты проезда».

КОМТИД, ООО

ООО «КОМТИД»

220141, г. Минск, ул. Купревича, 1-3-241

Тел.: (017) 211-83-24

E-mail: comtid@tut.by

Сайт: <http://www.comtid.com>

Год основания: 1996 г.

УНП: 101166264

Контактные лица: Балахничёв Игорь Николаевич, директор.

Сертификаты:

- сертификат соответствия по ТР №С-ВУ.ПБ16.В.00121 на оповещатели звуковые ПКИ Иволга, Колибри, Бекас, Шмель, Цикада, ПКИ-2, ПКИ-3, действителен до 14.06.2015 г.;
- сертификат соответствия по ТР №С-ВУ.ПБ16.В.00122 на оповещатели ПКИ-СП12 и СП24, действителен до 14.06.2015 г.;
- сертификат соответствия по ТР №С-ВУ.ПБ16.В.00123 на оповещатели речевые ПКИ-РС1(Говорун), ПКИ-РС2, ПКИ-РО, действителен до 14.06.2015 г.;
- сертификат соответствия №ВУ/112 03.03.023 00512, на оповещатели звуковые ПКИ-1(Иволга), ПКИ-1К(Колибри), ПКИ-МБ(Бекас), ПКИ-МШ(Шмель), ПКИ-МЦ(Цикада), действителен до 17.11.2016 г.;
- сертификат соответствия №ВУ/112 03.11.033 02265, на оповещатель пожарный звуковой ПКИ-1 (Иволга), действителен до 30.10.2016 г.;
- сертификат соответствия №ВУ/112 03.11.033 02266, на оповещатели пожарные комбинированные ПКИ-СП12 и ПКИ-СМ12, действителен до 05.03.2014 г.;

Производство:

Оборудование для охранной и пожарной сигнализации:

- оповещатели звуковые;
- оповещатели речевые;
- оповещатели светозвуковые;
- оповещатели световые;
- устройства подсветки светодиодные (стробоскопические);
- извещатели пожарные дымовые;
- извещатели дымовые автономные;
- извещатели газовые.

Научно-исследовательский институт технической защиты информации, Научно-производственное республиканское унитарное предприятие



220088, г. Минск, ул. Первомайская, 26/2

Тел./факс: (017) 294 01 71, 285 31 86

E-mail: info@niitzi.by

Сайт: www.niitzi.by

Год основания: 1987 г.

УНП: 100036784

Контактные лица: Картель Владимир Федорович, директор.

Лицензии:

- Специальное разрешение (лицензия) Оперативно-аналитического центра при Президенте Республики Беларусь на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи.
- Специальное разрешение (лицензия) Комитета государственной безопасности Республики Беларусь на право осуществления деятельности, связанной с криптографической защитой информации и средствами негласного получения информации.
- Специальное разрешение (лицензия) Министерства юстиции Респу-

блики Беларусь на право осуществления деятельности по оказанию юридических услуг.

- Специальное разрешение (лицензия) Министерства внутренних дел на право осуществления охранной деятельности.
- Специальное разрешение (лицензия) Государственного военно-промышленного комитета на право осуществления деятельности, связанной с продукцией военного назначения.

Услуги:

- Аудит систем защиты информации, информационных ресурсов и систем на информационную безопасность;
- Разработка политик безопасности, заданий по безопасности, сопутствующих нормативно-методических документов;
- Подбор, сертификация, поставка и установка средств защиты информации;
- Сертификационные испытания программных и аппаратно-программных продуктов информационных технологий (ИТ), технических средств защиты информации на соответствие требованиям безопасности информации, оценка заданий по безопасности;
- Создание систем защиты информации информационных систем и автоматизированных систем в защищенном исполнении, их аттестация.
- Специальная проверка защищаемых помещений и технических средств на наличие возможно внедренных специальных технических средств негласного съема информации;
- Подготовка, аттестация объектов информатизации на соответствие требованиям руководящих и нормативных документов по безопасности информации, сопровождение и периодический инструментальный контроль аттестованных объектов информатизации;
- Проектирование и монтаж вычислительных сетей, защищенных от утечки информации по техническим каналам.

Дистрибьютор компаний: ЗАО «Конструкторское бюро «ПРИБОР».

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 г.

УНП: 190543080

Контактные лица:

- Маштакова Марина Ивановна, директор;
- Гавриловец Александр Степанович, заместитель директора по коммерческой работе;
- Игнатович Николай Федорович, руководитель проектов;
- Ковчур Лидия Владимировна, начальник отдела продаж;
- Пузанов Юрий Васильевич, начальник отдела сервиса.

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:

Dallmeier

Представитель Dallmeier electronic в Республике Беларусь.

NOVUS

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

Сайт: www.orionproject.by

E-mail: info@orionproject.by

Skype: orionproject_support

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.

Рамок, Производственно-торговое частное унитарное предприятие



220036, г. Минск, ул. Лермонтова, 29

Тел./факс: (017) 210-22-80, (017) 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

Год основания: 30.12.1992 г.

УНП: 100001879

Контактное лицо: Яско Владимир Федорович, директор.

Лицензии:

- Лицензия на право осуществления деятельности по обеспечению безопасности юридических и физических лиц №02010/0444764, выдана 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, 20.07.11 г., LucatronAG (Германия); Сертификат №2011-QC, 03.12.2012 г., SMART-Home(США), BiampSystems (США).

Производство: торговое оборудование, витрины, 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, торговое оборудование, этикет-пистолеты, принтеры этикеток, программное обеспечение для автоматизации торговли и сферы услуг, оборудование для автоматизации дома, гостиницы, офиса.

Дистрибьютор компаний: LucatronAG (Германия), SMART-Home (США), GoDEX (Тайвань), CapherLab (Тайвань), Vangold (Китай),

ZKSoftwera (Китай), Protech (Тайвань), Planet (Тайвань), ОАО «КЗТА» (РФ).

Дополнительная информация: участие в выставках Tibo, HoReCa&RetailTech и др.

СервисСбытАвтоматика, Частное торговое унитарное предприятие



220024, г. Минск, ул. Стебенева, 12 офис 6-7

Юр. адрес: 223062, Минская обл., Минский р-н, Луговослободской с/с (р-н д. Прилесье), М4, 17-й км, здание ООО «Спелпайс-Плюс», 2, каб. 23

Телефон/факс: (017) 275 61 12, (017) 380 20 21,

(044) 5980 983, (044) 5981 980

Почта: info@ssa101.by

Сайт: www.ssa101.by

Год основания: 2012 г.

УНП: 691430930

Контактные лица: Жихарев Александр Станиславович, руководитель отдела продаж, (017) 380 20 21, (044) 5980 983

Лицензия:

№02300/2709, решение МЧС РБ от 02.04.2012 г. №15км, срок действия – 5 лет.

Сертификаты:

№0128571 от 05.10.2012 г., срок действия – 5 лет (ОАО «Завод Спецавтоматика»)

№0210454 от 10.08.2010 г., срок действия – 5 лет (СЗАО «Аргус-Спецавтоматика»)

Производство:

«СервисСбытАвтоматика» – только продажа оборудования.

Пожарная и охранная сигнализация, оборудование и материалы охранной и пожарной сигнализации (СЗАО «Аргус-Спецавтоматика», ОАО «Завод Спецавтоматика»).

Услуги:

Проектирование, монтаж, пуск-наладка, сервисные и гарантийные услуги, обслуживание систем (ОАО «Завод Спецавтоматика»).

Поставка:

Охранные и пожарные материалы и оборудование любого производителя.

Объекты, на которых установлена радиосистема СТРЕЛЕЦ:

Червенский рынок в Лошице (г. Минск), Архикафедральный собор Святого Имени Пресвятой Девы Марии (г. Минск), складские помещения УП «Элос» (г. Минск).

Дистрибьютор компаний:

СЗАО «Аргус-Спецавтоматика», ОАО «Завод Спецавтоматика».

СмартПроект, ООО



220073, г. Минск, ул. Гусовского, 6-2.6

Тел./факс: (017) 290-84-48 (многоканальный),

(029) 752-39-09 Velcom, (044) 752-39-09 MTC

E-mail: info@smartproekt.by

Сайт: www.smartproekt.by

Год основания: 2008 г.

УНП: 190982560

Контактные лица:

- Сергей Викторович Волнистый, управляющий;
- Михаил Владимирович Данилов, коммерческий директор.

Услуги: консультирование, подбор и поставка оборудования для создания комплексных систем безопасности и систем «интеллектуальное здание».

Поставка: системы видеонаблюдения, системы охранно-пожарной сигнализации, системы звуковой трансляции и аварийного оповещения, системы защиты от краж, системы «интеллектуальное здание»,

оборудование для автоматизации, расходные и сопутствующие материалы для производства монтажных работ.

Торговые марки:

- «АМС», Литва. Оборудование для построения систем звуковой трансляции.
- «NOVUS», Польша. Системы видеонаблюдения.

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 г.

УНП: 191152890

Контактные лица:

- Рябов Павел Анатольевич, зам. директора;
- Каравай Андрей Сергеевич, ГИП.

Лицензии: лицензия МВД на право осуществления деятельности по обеспечению безопасности юридических и физических лиц № 02010/12812 сроком действия до 15 июля 2015 г.

лицензия МЧС на право осуществления деятельности по пожарной безопасности № 02300/2912 сроком до 27.01.2018

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 (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: БРУСП «Белгосстрах», РУП «Аэропорт Минск-1», ЗАО «Банк ВТБ (Беларусь)», ИП «ЛУКОЙЛ-БЕЛОРУССИЯ», РУП «Белоруснефть-Минскавтозаправка», СООО «БМЕ Бизнес Центр», ИООО «Бел-Прибалт», СЗАО «ПИНСКДРЕВ-ПИНВУД», ОАО «Белшина», ЗАО «Выставочный центр АКВАБЕЛ», СООО «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, Белорусский народный банк.

Дистрибьютор компаний: ACTi, Pelko, Сфинкс, Trassir, Hawell.

Сталвиском, ООО



220007, г. Минск, ул. Володько, 12-102

Тел./факс: (017) 205-48-24

E-mail: sale@stalviscom.by

Сайт: www.stalviscom.by

УНП: 191194104

Контактные лица: Стабровский Александр Леонидович, заместитель директора по общим вопросам.

Поставка:

- цифровые системы безопасности;
- системы видеонаблюдения;
- системы контроля и управления доступом;
- домофоны;
- переговорные устройства;
- замки, доводчики;
- шлагбаумы, приводы для ворот;

- турникеты, ограждения, металлодетекторы;
- системы оповещения.

Дистрибьютор компаний: официальный представитель «Skyros», VideoNet, PandaCCTV, Microdigital Inc., NSGate.

Сфератрэйд, ОДО



220118, г. Минск, ул. Машиностроителей, 29-117

Тел: (017) 341-50-50, (029) 641-50-50 Velcom, (029) 541-50-50 MTC

E-mail: info@secur.by

Сайт: www.secur.by

Год основания: 1995 г.

УНП: 100972915

Контактное лицо: 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 (Испания), Truen (Корея), ZAVIO (Тайвань), NUUO (Тайвань), Roger (Польша), KT&C (Южная Корея), Fujinon (Япония), Pinetron (Южная Корея), GSN Electronic (Израиль), Rielta (РФ), LOB (Польша), Elmes (Польша), QUIKO (Италия), JIS (Испания), Kenwei (Китай), Seoul Commtech Co. (Южная Корея), PERCo (РФ), ITV (РФ), JSB Systems (РФ), AccordTec (РФ), Elesta (РФ), Bolid (РФ) и др.

ТеслаСистемс, ООО



222518, г. Борисов, ул. Демина, 5-39

E-mail: info@teslasystems.by

Сайт: teslasystems.by

Региональные офисы: во всех областных центрах.

Год основания: 2011 г.

УНП: 691379914

Контактные лица:

- Слижевский Владимир Иванович, заместитель директора;
- Овечкин Эдуард Анатольевич, начальник отдела продаж;
- Петракович Петр Петрович, начальник отдела технической поддержки.

Услуги:

Консультации, продажа, профессиональная установка и обслуживание:

- систем видеонаблюдения (аналоговое и IP) и аксессуаров к ним;
- систем контроля доступа, видео- и аудиодомофоны, видеоглазки;
- шлагбаумы, турникеты, замки, доводчики.

Поставка:

Первый поставщик IP (ONVIF) и CCTV систем видеонаблюдения от бюджетного до профессионального уровней – 3 года гарантии на поставляемое оборудование, видеодомофоны, системы контроля и управления доступом, сопутствующих материалов.

Дистрибьютор компаний: Протокам (торговая марка ProtoX), Sewin, Тору, Macroscop.

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 г.
УНП: 100834637

Контактное лицо: 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 синхроперевода, видеонаблюдения, контроля доступа, пожаротушения, профессионального озвучивания, охраны периметра, мультимедийных систем, локально-вычислительных сетей, охранной сигнализации, противокражной системы, системы диспетчеризации, телефона, часофикации, радиофикация, система автоматизации, комплексные интегрированные системы безопасности, системы управления и контроля инженерными сетями зданий.

Дистрибьютор: Arecont Vision (США), Cisa (Италия), Технос-М+ (Россия), СЕМ Systems Great (Северная Ирландия), Autec (Германия), Openers&Closers (Испания), Airphone (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), Etrvision (Тайвань), ТД «Паритет» (Россия), Полисервис НПФ ООО (Россия), РостЕвроСтрой (Россия), Риэлта (Россия), ТЕКО (Россия).

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.ru

Год основания: 2007 г.

ОГРН: 1086454000643

ИНН: 6454088952

КПП: 772901001

Контактные лица:

- Рыжков Алексей Владимирович, директор;
- Шайдулов Рустам, руководитель дилерского отдела;
- Голубев Антон, руководитель направления IP-видео;
- Колоскова Олеся, старший менеджер отдела продаж.

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) продукции, монтаж, демонтаж, эксплуатация, 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;
- Безопасный автобус, г. Москва («Мосгортранс», более 4000 автобусов);
- Безопасная школа: 1570 школ по Москве;
- 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 автозаканов;
- 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», представляет из себя группу 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-е полугодие 2013г.

Счет-подписка на журнал «Технологии безопасности», 2-е полугодие 2013г.

Подписные индексы РУП «Белпочта»:
01248 - для индивидуальных лиц, **012482** - ведомственная подписка

www.aercom.by

Адрес: 220072, г. Минск, ул. Гусовского, 6, оф. 2.15.2. Тел./ф.: +375 17 290-84-05, 256-10-47(35). ООО «АЭРКОМБел»;
 Р/с 3012007960018 в Отделение 526, г. Минск, ОАО «Белинвестбанк», код 739,
 220013, г. Минск, пр. Независимости, 77; УНП 190970885; ОКПО 377800425000

**ТЕХНОЛОГИИ
БЕЗОПАСНОСТИ**

журнал для руководителей предприятий
и специалистов отрасли безопасности

СЧЕТ-ФАКТУРА б/н от 1 июня 2013 г.

Название	Единица измерен.	Количество	Отпускная цена, руб	Сумма руб.
Подписка на журнал «Технологии безопасности» № 4-6, 2013г.	шт.	3	77 500	232 500

Цена согласно прейскуранта № 2 от 21.02.2013 г.

Всего к оплате без НДС: Двести тридцать две тысячи пятьсот 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

ООО «АэркомБел» является издателем настоящего журнала. Периодичность выхода 1 раз в 2 месяца.



[Подпись]
 Руководитель предприятия
 Драгун С.А.

FOR A GOOD **REASON**
GRUNDIG

Инновационные системы видеонаблюдения от немецкого производителя



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

UNEX

системы видеонаблюдения

www.unexpro.ru

3 МЕГАПИКСЕЛЯ

WDR

Преодолевающая контрастность освещения

Исключительная четкость и яркость изображения даже в условиях высокой контрастности

Мегapixelные камеры **UIP-E** D-серии сочетают в одном изображении светлые зоны, снятые с высокой скоростью затвора, и темные зоны, снятые с низкой скоростью затвора. Встроенный режим **sens-up** обеспечивает четкое изображение даже при низкой освещенности

До 3 мегапикселей

Работа при низкой освещенности

Двойная скорость затвора при WDR

WDR до 120 дБ



УИП 100834637

Onvif

UNEX
системы видеонаблюдения

СП «Унибелус» 000, г. Минск, ул. Нахимова, 17, Тел.: +375 (17) 291 15 05
info@unibelus.com www.unibelus.by