Журнал для руководителей предприятий и специалистов отрасли безопасности

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

№6(33)
ноябрь-декабрь
2013

ЭКСПЕРТНЫЙ ОБЗОР

Итоги, тенденции, состояние, прогнозы развития сегментов безопасности Республики Беларусь

Министерство по чрезвычайным ситуациям Департамент охраны

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ОТРАСЛИ БЕЗОПАСНОСТИ НА 2014 ГОД

Основные тренды сегмента в 2013-14 гг.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

www.axiom.by

AXIOM

Не требует доказательств

ПРОФЕССИОНАЛЬНЫЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

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

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

УНН100972915

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, № 6 (33)–2013
В НОМЕРЕ:

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»
Производственно-практический журнал
№ 6 (33), декабрь, 2013

Периодичность выхода: 1 раз в 2 месяца

Учредитель и издатель:
ООО «АэркомБел»

Главный редактор:
Сергей Адамович Драгун

Над номером работали:
Лисенкова Анна
Карпук Мария

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

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

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

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

Подписка через РУП «Белпочта»:
01248 — для индивидуальных подписчиков;
012482 — для предприятий и организаций.

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

Подписано в печать — 21.02.2014 г.
Формат: 60x90 1/8
Бумага офсетная
Гарнитура Myriad Pro. Печать офсетная
Усл. печ. л. 6,75; Уч.-изд.л. 8
Тираж: 800 экз.
Заказ _____

Отпечатано в типографии
ООО «Юстмаж»

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

ISSN 2221-8661

СЛОВО РЕДАКТОРА

Основные тенденции, которые будут влиять на развитие отрасли безопасности в Республике Беларусь:

- Нормативные. Все ведомства, регулирующие сегменты безопасности, приняли в 2013 или планируют принять в 2014 году ряд нормативных актов, существенно влияющих на развитие сегмента и регламентирующих применение технических средств безопасности на территории страны. Более подробно см. в материалах журнала.

Можно выделить тенденцию – нормативные акты принимаются с учётом экономической интеграции с соседними странами. Функционирование национального рынка безопасности становится более открытым (хотя бы в рамках Таможенного союза). Будут существовать национальные перечни технических средств безопасности, но в будущем эксперты прогнозируют их отмену. Останется ряд позиций (например, в сегменте информационной безопасности), где будут существовать только национальные решения.

По оценкам экспертов большинство национальных производителей, существующих сегодня вне жесткой конкурентной среды (благодаря НА), не выдержат конкуренции даже в условиях действия технических регламентов Таможенного союза (в первую очередь с российскими производителями).

- Технические факторы, влияющие на развитие сегмента безопасности. Повсеместное применение IP-среды уже сегодня и полное её господство завтра. Также главный фактор – активное развитие каналов связи (ВОЛС, на подходе LTE), что скажется на тактике обеспечения безопасности. По оценке экспертов будущее за интегрированными системами и комплексным подходом к безопасности. Первой начинает подходить к обеспечению безопасности как к комплексной задаче банковская отрасль.

Готовятся новые номера журнала «Технологии безопасности»:

№1, январь-февраль, 2014. Главные темы номера: СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ. ПОЖАРНАЯ БЕЗОПАСНОСТЬ

1. Системы видеонаблюдения

- Обзор нормативных актов, регулирующих вопросы создания и эксплуатации систем видеонаблюдения в интересах обеспечения общественного порядка;
- Экспертные мнения, комментарии участников рынка (поставщиков, потребителей): влияние принятых нормативных актов на рынок СВН.

Обзор торговых марок СВН:

- Сводная таблица участников рынка Беларуси в сегменте СВН. Условия – первые поставщики, легализация оборудования на рынке Беларуси (сертификация ЕАС).

Обзор технический решений СВН (на примере схемы объекта):

- Ведущие поставщики СВН проводят расчет оборудования IP СВН для типового объекта (магазина) в соответствии с новыми нормативными требованиями.
- Обзоры новых решений СВН, тенденции. Проекты и решения.

2. Газовое тушение, комплексные системы пожарной безопасности:

- Нормативное регулирование. Переработка ТНПА, касающихся технических требований к автоматическим установкам газового пожаротушения (НПБ 60-2002, НПБ 83-2004, НПБ 79-2004);
- Сводная таблица участников рынка Беларуси в сегменте газового тушения. Условия – первые поставщики, легализация оборудования на рынке Беларуси (сертификация ЕАС).

№2, март-апрель, 2014. Главные темы номера: «БАНКОВСКАЯ БЕЗОПАСНОСТЬ – ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ».

1. Экспертный обзор. Состояние и проблематика сегмента банковской безопасности, информационная и инженерно-техническая безопасность (ИТС). (УБЗИ, ЕРИП, ДО);
2. Информационная безопасность. Новые СТБ 34.101.41 (42, 62, 60, 61):

- Обзор требований принятых СТБ (ЕРИП);
- Организационно-техническое обеспечение принятых СТБ. Средства и системы, обзор производителей и поставщиков.

3. Инженерно-техническая безопасность.

- Обзор, состояние, ход разработки новых нормативных актов, регулирующих применение ИТС на банковских объектах (Инструкции по организации охраны на банковских объектах, Инструкция о требованиях к технической оснащенности и охране банкоматов и пр.);
- Изменение условий работы и взаимодействия служб безопасности банков с Департаментом охраны МВД (типовые договора на оказание охранных услуг);
- Внесение изменений в Указ Президента от 25.10.2007 г. №534, предусматривающих исключение из Указа п.5, распространение действия п.4 на все банки;
- Инновационные подходы к организации охраны банковских объектов – создание банковских центров мониторинга.

Приглашаем к участию профильные компании и специалистов.

С уважением, Драгун Сергей Адамович,
главный редактор журнала.

20-я международная выставка и конференция

ОХРАНА, БЕЗОПАСНОСТЬ И ПРОТИВОПОЖАРНАЯ ЗАЩИТА

ufi Approved Event

MIPS MOSCOW

Нам 20 лет!

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

Охранное телевидение и наблюдение

Технические средства обеспечения безопасности

Системы защиты периметра. Ограждения

Пожарная безопасность. Аварийно-спасательная техника. Охрана труда

Смарт карты

Организатор:

ITE

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

При поддержке:

МВД России

www.mips.ru

Планы по переработке технических нормативных правовых актов системы противопожарного нормирования и стандартизации (в рамках реализации плана государственной стандартизации на 2014 год)

Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций (НИИ ПБ и ЧС МЧС Республики Беларусь)

Лешкевич Максим Станиславович, майор внутренней службы, заместитель начальника отдела нормирования и стандартизации учреждения «Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций» МЧС Республики Беларусь

Лупандин Александр Евгеньевич, старший лейтенант внутренней службы, старший научный сотрудник отдела нормирования и стандартизации учреждения «Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций» МЧС Республики Беларусь.

Основным направлением совершенствования системы противопожарного нормирования и стандартизации является комплекс работ по обеспечению необходимого уровня пожарной безопасности и формированию доказательной базы подтверждения соответствия требованиям технических регламентов путем гармонизации национальных и международных нормативных документов в области пожарной безопасности. Решение указанной задачи осуществляется путем:

- введения в действие и применение в установленном порядке на территории Республики Беларусь международных и региональных стандартов;
- использования методической и испытательной материально-технической базы, сопоставимой с европейскими и международными аналогами;
- соответствия требований национальных нормативных документов по пожарной безопасности мировому уровню развития науки и техники;
- прогрессивности и оптимальности требований пожарной безопасности, гибкости нормирования в целях обеспечения конкурентоспособности отечественной продукции.

Гармонизация всего спектра национальных технических нормативных правовых актов в области пожарной безопасности создаст условия для повышения пожарной безопасности в Республике Беларусь, интеграции в мировую экономику, создания благоприятного инвестиционного климата, обеспечения соответствия отечественной продукции международным требованиям и повышения ее конкурентоспособности, устранения технических барьеров в торговле.

За период 2012-2013 годы основная работа Министерства по чрезвычайным ситуациям Республики Беларусь в области технического нормирования и стандартизации была направлена на инвентаризацию и систематизацию технических нормативных правовых актов в области обеспечения пожарной безопасности.

За указанный период признаны утратившими силу 23 Нормы пожарной безопасности. В их состав вошли нормы, взамен которых введены европейские стандарты, либо требования отмененных норм включены в соответствующие технические нормативные правовые акты Министерства архитектуры и строительства, государственные стандарты Республики Беларусь.

Переработано постановление МЧС Республики Беларусь от 25 ноября 2002 г. №27 «Об утверждении Инструкции по функционированию системы противопожарного нормирования и стандартизации», взамен которого введено постановление МЧС Республики Беларусь от 6 февраля 2012 г. №12 «О некоторых вопросах функционирования системы противопожарного нормирования и стандартизации».

Учитывая требования статьи 1 Закона Республики Беларусь от 10 января 2000 г. №361-З «О нормативных правовых актах Республики Беларусь», нормы и правила пожарной безопасности являются техническими нормативными правовыми актами, утвержденными (введенными в действие) в порядке, установленном законодательством Республики Беларусь. Министерством подготовлены и направлены предложения в «План государственной стандартизации Республики Беларусь на 2014 год» (далее – План).

В результате реализации Плана окончательно завершится переработка всех норм пожарной безопасности в соответствующие технические кодексы установившейся практики (7 технических кодексов установившейся практики) и стандарты Республики Беларусь (29 стандартов, а также 6 изменений).

Изменения коснутся и технических нормативных правовых актов Республики Беларусь, устанавливающих общие технические требования к оборудованию пожарной автоматики и методам их испытаний. Так планируется переработка с последующей отменой норм пожарной безопасности, приведенных в таблице 1.

В настоящее время по всем позициям Плана подготовлены технические задания, которые согласованы Госстандартом и утверждены Главным государственным инспектором Республики Беларусь по пожарному надзору.

Таблица 1 – Нормы пожарной безопасности, подлежащие переработке в государственные стандарты Республики Беларусь в соответствии с Планом

№ п/п	Нормы пожарной безопасности, подлежащие переработке в государственный стандарт Республики Беларусь	Наименование разрабатываемого государственного стандарта Республики Беларусь
1	2	3
1.	НПБ 40-2001 «Нормы пожарной безопасности Республики Беларусь. Установки пенного пожаротушения автоматические. Дозаторы. Общие технические требования. Методы испытаний»	СТБ ГОСТ Р 51114-97 «Установки пенного пожаротушения автоматические. Дозаторы. Общие технические требования. Методы испытаний»
2.	НПБ 41-2001 «Нормы пожарной безопасности Республики Беларусь. Установки водяного и пенного пожаротушения автоматические. Узлы управления. Общие технические требования. Методы испытаний»	СТБ ГОСТ Р 51052-2002 «Установки водяного и пенного пожаротушения автоматические. Узлы управления. Общие технические требования. Методы испытаний»
3.	НПБ 60-2002 «Нормы пожарной безопасности Республики Беларусь. Составы газовые огнетушащие. Общие технические требования. Методы испытаний»	СТБ ГОСТ Р 53280.3-2009 «Установки пожаротушения автоматические. Огнетушащие вещества. Часть 3. Газовые огнетушащие вещества. Методы испытаний»
4.	НПБ 79-2004 «Нормы пожарной безопасности Республики Беларусь. Установки газового пожаротушения автоматические. Резервуары изотермические. Общие технические требования. Методы испытаний»	СТБ ГОСТ Р 53282-2009 «Установки газового пожаротушения автоматические. Резервуары изотермические пожарные. Общие технические требования. Методы испытаний»
5.	НПБ 83-2004 «Нормы пожарной безопасности Республики Беларусь. Установки газового пожаротушения автоматические. Устройства распределительные. Общие технические требования. Методы испытаний»	СТБ ГОСТ Р 53283-2009 «Установки газового пожаротушения автоматические. Устройства распределительные. Общие технические требования. Методы испытаний»
6.	НПБ 104-2005 «Нормы пожарной безопасности Республики Беларусь. Извещатели пожарные газовые. Общие технические требования. Методы испытаний»	СТБ «Извещатели пожарные газовые. Общие технические требования. Методы испытаний»
7.	НПБ 113-2005 «Нормы пожарной безопасности Республики Беларусь. Системы передачи извещений о пожаре. Общие технические требования. Методы испытаний»	СТБ «Системы передачи извещений о пожаре. Общие технические требования. Методы испытаний»

Изменения технических нормативных правовых актов, устанавливающих общие технические требования к оборудованию пожарной автоматики, коснутся следующих стандартов:

- изменение № 1 СТБ 2243-2011 «Система стандартов пожарной безопасности. Оповещатели пожарные. Общие технические условия» (совершенствование требований к оповещателям, включение дополнительных методов испытаний);
- изменение № 1 СТБ 11.13.19-2010 «Система стандартов пожарной безопасности. Установки порошкового пожаротушения автоматические. Модули. Общие технические требования. Методы испытаний» (установление дополнительных требований к модулям порошкового пожаротушения, изменение порядка их условного обозначения);
- изменение № 1 СТБ 11.13.20-2010 «Система стандартов пожарной безопасности. Установки газового пожаротушения автоматические. Модули и батареи. Общие технические требования. Методы испытаний» (установление дополнительных требований к проведению испытаний);
- изменение № 1 СТБ 11.16.03-2009 «Система стандартов пожарной безопасности. Системы пожарной сигнализации. Извещатели пожарные дымовые точечные. Общие технические условия» (совершенствование требований, предъявляемых к чувствительности дымовых пожарных извещателей и объему сертификационных испытаний);
- изменение № 1 СТБ 11.16.05-2011 «Система стандартов пожарной безопасности. Установки аэрозольного пожаротушения автоматические. Генераторы огнетушащего аэрозоля. Общие технические требования. Методы контроля» (изменение условного обозначения генераторов огнетушащего аэрозоля, критериев признания результатов испытаний).

Решением Совета Евразийской экономической комиссии от 23 ноября 2012 г. № 103 утвержден План разработки технических регламентов Таможенного союза.

Продолжение на стр. 7 →

Некоторые вопросы работы органов и подразделений по чрезвычайным ситуациям Республики Беларусь

Приоритетные задачи и направления деятельности МЧС Республики Беларусь в 2013 году в части работы по предупреждению пожаров в зданиях повышенной высотности. Разработка нормативных документов.

Развитие архитектурного облика современного города, столицы государства, невозможно представить без уникальных объектов: крупных спортивно-культурных, многофункциональных и жилых комплексов, высотных зданий. Не всегда задуманные архитекторами «уникальные» идеи, учитывающие мировые тенденции в архитектуре, отвечают требованиям технических нормативных правовых актов. Это было учтено и, благодаря деятельности Министерства архитектуры и строительства, Министерства по чрезвычайным ситуациям и других заинтересованных, на протяжении 10 лет проводится целенаправленная работа по совершенствованию нормативной базы, которая помимо оптимизации и систематизации противопожарных требований действующих технических нормативных правовых актов, предусматривает и разработку новых.

Так, для осуществления беспрепятственного строительства высотных зданий в кратчайшие сроки был разработан технический кодекс установившейся практики ТКП 45-3.02-108-2008 «Высотные здания. Строительные нормы проектирования». Над кодексом работал авторский коллектив, в состав которого вошли ведущие специалисты различных направлений в области строительства и обеспечения безопасности зданий, в том числе и работники учреждений Министерства по чрезвычайным ситуациям. Этот документ разрабатывался с учетом мирового опыта проектирования и практики строительства таких объектов. Особенно стоит отметить, что, несмотря на относительно небольшой период действия, с учетом его требований, на настоящий момент выданы более 10 заключений государственного пожарного надзора на проектирование высотных зданий, которые уже реализуются (планируются к реализации) в республике, например: Бизнес-центр и многоквартирный жилой дом со встроено-пристроенными помещениями административно, общественно-бытового назначения и подземным гаражом-стоянкой по ул. М. Танка в г. Минске, «Административно-деловой, торгово-развлекательный центр с многоуровневой стоянкой в районе пр. Независимости-МКАД», «Современный многофункциональный торгово-развлекательный комплекс с гостиницей и паркингом в г. Минске» по пр. Победителей, 9».

Так как каждое высотное здание по своему уникально, ТКП 45-3.02-108 регламентирует необходимость разработки для проектирования здания специальных технических условий, с целью конкретизации требований к архитектурно-планировочным и конструктивным решениям проектируемого здания, противопожарных требований, требований к инженерным системам здания, системам мониторинга состояния здания при эксплуатации. Стоит отметить, что раздел «Противопожарные требования» специальных технических условий разрабатывает, что предусмотрено ТКП 45-1.01-234-2011 «Специальные технические условия в области архитектуры и строительства. Порядок разработки, построения, изложения, согласования и утверждения», а специальные технические условия в целом согласовываются с МЧС.

Повышенная пожарная опасность таких объектов потребовала и более детализированных требований, обеспечивающих действия пожарных аварийно-спасательных подразделений по тушению возможных пожаров и эвакуации людей из здания, одними из которых являются: сокращение максимально-допустимого расстояния от пожарных депо до высотных зданий, комплектование депо соответствующей пожарной техникой.

Мероприятия, проводимые МЧС по обеспечению эффективной противопожарной защиты при подготовке и проведению чемпионата мира по хоккею в 2014 г.

Министерством по чрезвычайным ситуациям, совместно с заинтересованными, осуществляется комплекс мероприятий по обеспечению безопасности при подготовке и проведении чемпионата мира по хоккею в 2014 г.

Отработаны приемы ведения аварийно-спасательных работ на объектах расселения официальных участников, гостей и болельщиков чемпионата (гостиницы, общежития и т.п.), а также на спортивных аренах.

Осуществлен обмен опытом с коллегами из России и Украины по вопросам обеспечения безопасности спортивных мероприятий.

Изучены принимаемые меры по предупреждению пожаров и других чрезвычайных ситуаций во время спортивно-массовых мероприятий и в других странах, в том числе в рамках визита делегации Французской Республики.

В ноябре 2013 г. совместно с НАТО организованы и проведены командно-штабные учения на тему «Реагирование на чрезвычайные ситуации при проведении международных спортивных мероприятий», приуроченные к чемпионату мира по хоккею 2014 г. в г. Минске.

Введен в действие закрепленный законодательством за МЧС номер «112», обеспечена возможность вызова спасателей по единому европейскому телефонному номеру в сетях операторов сотовой и фиксированной связи, в том числе на иностранных языках.

Реализуются мероприятия по контролю за обеспечением пожарной безопасности. Проведены проверки и мониторинги объектов, задействованных при проведении чемпионата.

На сегодняшний день работа по подготовке безопасного проведения спортивного мероприятия продолжается.

Подразделения Минского гарнизона оснащаются современной пожарной аварийно-спасательной техникой.

Органы и подразделения по чрезвычайным ситуациям готовы к выполнению задач по оперативному реагированию на пожары и иные чрезвычайные ситуации. Проводимая и планируемая работа и в дальнейшем будет направлена на обеспечение безопасности участников и гостей Чемпионата мира по хоккею в 2014 г. в г. Минске.

Подготовил, Колтович Андрей Васильевич,
подполковник внутренней службы, главный
специалист управления надзора
и профилактики МЧС

← *Начало на стр. 5*

Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций (НИИ ПБ и ЧС МЧС Беларуси)

Технические регламенты, работа по которым была начата вне графика в соответствии с поручением Совета Министров Республики Беларусь, определены ответственные республиканские органы государственного управления, отвечающие за выработку консолидированной позиции и участие в международных переговорах.

Так, одним из закрепленных за МЧС Республики Беларусь является технический регламент Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» *(изначально разрабатывался как «О требованиях пожарной безопасности к продукции»)*.

Проект технического регламента Таможенного союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» находится в высокой степени готовности, при этом, чтобы три страны перешли на единые правила и принципы технического регулирования, по мере введения в действие технических регламентов Таможенного союза будут отменяться национальные технические регламенты, объекты регулирования которых совпадают с объектами технических регламентов Таможенного союза, а также прекращена разработка национальных регламентов сторон, по которым идет параллельная работа на межгосударственном уровне.

Участники Таможенного союза обеспечивают обращение продукции, соответствующей требованиям технических регламентов Таможенного союза, на своей территории без предъявления дополнительных по отношению к содержащимся в техническом регламенте Таможенного союза требований к такой продукции, и без проведения дополнительных процедур оценки (подтверждения) соответствия.

Одновременно с проектом технического регламента Таможенного союза разрабатываются перечни стандартов, обеспечивающих соблюдение его требований. В настоящее время проекты перечней стандартов разработаны на основании предложений российской стороны. Поступившие предложения от Белорусской и Казахстанской стороны по формированию перечней рассматриваются Российской стороной и изучаются стандарты, предлагаемые для включения в перечень. Предполагается, что по результатам данной работы будет сформирован проект перечней стандартов, обеспечивающих соблюдение требований технического регламента Таможенного союза, согласованный всеми сторонами.

В связи с этим, перечень норм пожарной безопасности, подлежащий переработке в национальные стандарты Республики Беларусь, а также сроки выполнения работ корректируются в зависимости от вносимых изменений и дополнений в проект технического регламента Таможенного союза.

Предложения и замечания по проектам технических нормативных правовых актов и проектам изменений просим направлять в адрес учреждения «Научно-исследовательский институт пожарной безопасности и проблем чрезвычайных ситуаций» МЧС Республики Беларусь (220046, г. Минск, ул. Солтыса, 183а, e-mail: nii-onis@ya.ru). Будем рады сотрудничеству! ■

Планы и тенденции развития ДО МВД РБ нормативной базы, технических средств и методологии охраны на 2014 год

Шаблыко Олег Николаевич, заместитель начальника Департамента охраны – начальник управления средств и систем охраны, полковник милиции

Справка ТБ

Шаблыко Олег Николаевич, образование высшее, БГПА факультет приборостроения в 1995 г., Академия управления при Президенте Республики Беларусь – 2005 год. Заместитель начальника Департамента охраны, начальник управления средств и систем охраны Департамента МВД Республики Беларусь.

Статистика за 2013 год

По состоянию на 1 января 2014 года подразделениями Департамента охраны с использованием средств и систем охраны (ТСиСО) охраняется более 36 тыс. объектов, более 167 тыс. жилых домов (помещений) физических лиц. Прирост охраняемых объектов, жилых домов (помещений) в сравнении с началом 2013 года составил +150 и +5075 соответственно. Общее количество объектов и жилых домов (помещений) физических лиц, находящихся под охраной ДО, на конец 2013 года составило более 200 тыс.

Каналы связи. Количество объектов, которые контролируются:

- с помощью радиоканальных пультов – 7462;
- по каналам GSM-связи – 15971;
- по каналу Ethernet – 1160.

Произвольное срабатывание. Важнейшим показателем качества работы служб средств и систем охраны подразделений является количество произвольных срабатываний технических средств и систем охраны. За 2013 год поступило всего срабатываний средств сигнализации:

- из охраняемых объектов – 227 790;
- из жилых домов (помещений) физических лиц – 161 439.

Произвольных срабатываний:

- из охраняемых объектов поступило **144 094**, это на 133 больше, чем в аналогичный период 2012 года, однако в пересчете на одну условную установку количество срабатываний за 2013 года составляет **0,510**, что на 0,016 меньше, чем за аналогичный период прошлого года;
- из жилых домов (помещений) физических лиц поступило **151 209** произвольных срабатывания, что на 422 меньше чем в прошлом году, в пересчете на одну условную установку – **0,491**, что на 0,028 меньше, чем за аналогичный период прошлого года.

Таким образом, снижение количества произвольных срабатываний технических средств охраны в пересчете на одну условную установку произошло как на объектах, так и в жилых домах (помещениях).

Причины произвольных срабатываний.

Наибольший удельный вес в общем количестве произвольных срабатываний занимают срабатывания по причинам:

- несоблюдения условий эксплуатации (30% – объекты, 20% – помещения физических лиц);
- из-за отказа или сбоя в работе извещателей (26% – объекты, 22% – помещения физических лиц);
- из-за несвоевременного (неправильного) снятия из-под охраны (17% – объекты, 28% – помещения физических лиц).

Предотвращено с использованием ТСиСО:

- попыток проникновения на охраняемые объекты – 319;
- попыток проникновения в жилые дома – 50;
- Выявлено и локализовано (совместно с РО ЧС): возгораний на объектах – 28; в жилых домах – 16.

Что показывает, что при должной эксплуатации используемые ТСиСО работают качественно.

Разработка, модернизация ТСиСО

Сотрудники управления средств и систем охраны совместно с заинтересованными предприятиями в 2013 году участвовали в разработке, модернизации, проведении стендовых испытаний и опытной эксплуатации **17** новых извещателей, приборов и систем охранной сигнализации, предназначенных для охраны объектов и жилых помещений физических лиц, в том числе:

- извещателей охранных – 5 шт.;
- приемно-контрольного прибора «ПКП-128»;
- индикатора электромонтера технологического (ИЭТ-4);
- приемно-контрольного прибора «Аларм-3» со встроенным модулем связи;
- программного обеспечения для сопряжения систем видеонаблюдения с ПО ПЦН «Алеся-01» из состава СПИ «АСОС Алеся»;
- блока сопряжения «Аларм-ПКП-Ethenet» производства НТ ЗАО «Аларм»;
- системы мониторинга и охраны объектов СПИ «Неман»;
- приемно-контрольного прибора «Аларм-10» совместно с абонентским оптическим терминалом GPON ONT (MT-PON-AT с поддержкой Wi-Fi);
- систем видеонаблюдения, установленных в постовых помещениях банков с выводом сигнала на пункты централизованного наблюдения;

- модуля «Аларм – Ethenet – GPRS» для организации резервирования канала связи (в сетях VPN) между УТОИ-01 и ПЦН в СПИ АСОС «Алеся» по GSM/GPRS каналу;

- программного обеспечения СПИ «Неман» для автоматизированной постановке под охрану и снятию из-под охраны ручных средств тревожной сигнализации, находящихся не в круглосуточном режиме работы.

Технические средства и системы охраны

Насколько уровень технических средств и систем охраны (ТСиСО) используемых в работе Департамента охраны (ДО) соответствует современным потребностям обеспечения безопасности объектов?

Тактика блокировки с помощью ТСиСО, используемая ДО, обеспечивает надежную защиту объектов всех форм собственности. Серьезных нареканий к качеству используемого оборудования на объектах нет. На сегодняшний день у ДО достаточно сил, знаний и опыта для грамотной и качественной эксплуатации технических средств и систем охраны, которые были разработаны и установлены ранее. При этом следует учитывать, что сроки эксплуатации оборудования на объектах достигают 8-10 лет. Но Департамент охраны тоже развивается, соответственно требования к качеству оборудования растут.

Если говорить о проблематике в этом сегменте, то у ДО есть ряд претензий к качеству эксплуатации ТСиСО, к электромонтерам, осуществляющим техническое обслуживание на объектах. Зачастую качество выполняемых работ оставляет желать лучшего. Сотрудники ДО выявляют такого рода недостатки при проведении обязательного технического контроля и приемки, в ходе которых доводят качество монтажа до требуемого уровня. Для нас это важный вопрос, т.к. качество монтажа влияет на количество ложных сработок, что напрямую влияет на использование ресурсов.

Какие вопросы решаются для повышения уровня технического оснащения сотрудников ДО?

Сейчас Департаментом охраны ведется работа над уменьшением времени передачи информации о срабатывании охранной сигнализации на объекте. Зачастую мы теряем до 1 минуты при передаче сообщений от дежурного пульта управления непосредственно в группу задержания. Поэтому планируется организация передачи сигнала с охраняемого объекта напрямую в группу задержания, что позволит сократить время реакции на срабатывание. В новом техническом решении дежурный сможет осуществлять мониторинг и координировать действия групп задержания. Техническое оснащение – комплекс с мобильным устройством (планшетом), на который будет выводиться необходимая информация о срабатывании на объекте, характеристики объекта, подъездных путях, ответственных лицах и др. Информация, в зависимости от категории объектов и оперативной обстановки.

Сейчас изучаем возможности отечественных производителей, опыт зарубежных представителей. Ищем сочетание стоимости и технических возможностей интересующих нас систем.

Нормирование, лицензирование, сертификация

Планируется ли расширение, изменение нормативной базы, регулирующей условия и применение технических средств безопасности в ближайшее время?

Среди приоритетных задач ДО стоит задача – в 2015 году завершить работы по переводу используемых руководящих документов (РД) в технические кодексы установившейся практики (ТКП). Идет переработка внутренних регламентирующих документов (на техническое обслуживание), дорабатывается инструкция по охране квартир. Порядка 6 нормативных документов находятся на согласовании либо в юридическом отделе, либо в Национальном банке. В частности ведутся работы по следующим документам:

- ТКП «Технический надзор по оборудованию объектов системами охраны»;

- ТКП «Технический надзор в монтаже систем охранной сигнализации»;

- Постановление МВД Республики Беларусь №290 «Об утверждении инструкции о порядке передачи под охрану ДО объектов и имущества граждан, их обследования и организации делопроизводства по договорам оказания охранных услуг. Инструкция по организации личной и имущественной безопасности граждан с использованием ТСО»;

- Постановление МВД Республики Беларусь №209 «Об утверждении инструкции по эксплуатации систем охраны, обслуживаемых подразделениями ДО МВД РБ»;

- Разработан проект изменения в приказ ДО №194 «Об утверждении инструкции по эксплуатации ТСиСО, обслуживаемых подразделениями ДО»;

- Переработан Приказ №124 «Организация оборудования СО и домов граждан».

Планируются изменения в документах, регламентирующих тактику охраны под современные тенденции. Одна из современных тенденций – ДО принимает под охрану все больше удаленных объектов (коттеджей), что требует изменений во времени реагирования и тактику блокировки объектов.

В части организации охраны банковских учреждений ДО ведется работа по согласованию совместного приказа МВД и Национального банка № 25/10, который утвердит документ – «Инструкция по оборудованию банков техническими средствами охраны». Инструкция будет предусматривать все нюансы охраны банковских учреждений. На сегодня практически все вопросы согласованы, документ готов к принятию.

Какова политика ДО в части расширения полномочий служб безопасности банков? Возможно ли в ближайшее время создание института ЧОПов или расширение полномочий служб безопасности предприятий в Республике Беларусь?

На сегодняшний день ДО не участвует в разработке документов, которые будут давать возможность организации в нашей стране ЧОПов.

Формально, создание таких структур подтолкнуло бы к принятию новых методик и более быстрому развитию технологий для ТСиСО. Мы спокойно относимся к вопросу демонополизации рынка охраны. Сегодня количество объектов, находящихся под охраной департамента, велико, мы прекрасно понимаем трудоемкость работ по мониторингу и техническому обслуживанию.

Планирует ли ДО взять функции регулятора в части установки, применения, эксплуатации СВН на объекте?

К сожалению, по ряду причин ДО не осуществляет сертификацию данных технических средств, осуществлять такое регулирование пока не планируем. Хотя тема актуальная, т.к. заказчик, устанавливающий СВН, не обладает знаниями и информацией по качеству и необходимым требованиям к оборудованию. Поэтому сегодня основным показателем при установке СВН на объектах является цена, что сказывается на качестве видео.

Какой документ может регулировать требования к техническим характеристикам СВН на объектах?

Может быть ТКП. Возможно провести реализацию такого документа постановлением Совета министров, который утверждает требования к лицензированию по видам деятельности. Требования к СВН могут быть прописаны при получении лицензии на вид деятельности (например, на торговлю).

Каналы связи

Какие работы ведутся ДО по переходу на новые каналы связи?

При проведении ЧМ по хоккею в 2014 году на ДО будет возложена задача по охране значимых объектов, объектов жизнеобеспечения и гос. управления. В рамках подготовки к данному мероприятию происходит внедрение цифровых средств связи в работу всех подразделений ДО. К концу апреля 2014 года планируется переход ДО на цифровую радиосвязь.

Для подразделений ДО, выполняющих охрану объектов, актуально получение качественной радиосвязи, это касается в первую очередь постов, находящихся внутри помещений (особенно в монолитных зданиях). В таких помещениях аналоговую связь использовать проблематично.

Преимущества цифровой связи очевидны, кроме качества и стабильности она позволяет передавать как речевые сообщения, так и любую значимую текстовую информацию (например, от дежурного ПЦО). Кроме того, данный вид связи позволяет организовать GPS-навигацию, функция встроена в носимые радиостанции. Что позволит организовать более качественное взаимодействие всех служб единой дислокации и организовать более качественное управление нарядами и их мониторинг. Повысится оперативное реагирование.

Существуют ли планы по созданию единого центра мониторинга?

Такие планы есть. Сейчас вопрос прорабатывается на базе Витебского областного ДО. Планируется на базе трех районных подразделений ДО создание единого центра управления нарядами под названием «Цунами». Идут работы по разработке программного обеспечения. Центр позволит осуществлять качественное руководство нарядами в городе и ближайших населенных пунктах.

Планируется ли строительство собственного ЦОД для ДО?

Мы прекрасно понимаем важность построения собственного ЦОД. На сегодняшний день этот вопрос рассматривается.

Каковы результаты работ по переходу систем охранной сигнализации на оптоволоконные линии связи?

Развитие ВОЛС продолжается, идет плановый переход на новые каналы связи систем охранной сигнализации. В частности, по технологии GPON уже активно подключаются под охрану квартиры и объекты, всего по стране подключено около 500 объектов.

Нареканий по работе каналов связи пока нет, в дальнейшем при подключении большего числа объектов можно будет говорить о статистике и результатах перехода.

Поменялась ли тарифная политика ДО при переходе на ВОЛС?

Для заказчика тарифы не изменились. На сегодняшний день охрана квартиры для физического лица осталась прежней – 50 тысяч. При этом ДО оплачивает линии связи РУП «Белтелеком».

Возникают ли вопросы при организации, построении сети и использовании охранного оборудования на ВОЛС? Как решился вопрос по обеспечению питания абонентских терминалов для соответствия их нормативным требованиям ДО?

В мае 2013 года на техническом совете было принято решение предусмотреть увеличение мощности блоков питания ПКП, что позволит реализовать подключение абонентских терминалов. Все три белорусские компании-производители, реализовали это решение в выпускаемых ПКП.

Проблем с переходом на ВОЛС нет, в основном такие подключения идут в новостройках, где нет установленного ранее охранного оборудования. Сложнее приходится, когда установка идет в домах, где была старая телефонная линия, которую изолируют и подводят ВОЛС. В таком случае возникают дополнительные затраты, приобретается адаптор, либо меняется ПКП.

Как отразится перенос мониторинга объектов с «меди» на оптоволоконные каналы связи на объектовом оборудовании и тактике охраны объекта, а также на оптимизации затрат на охранный мониторинг?

Благодаря применению ВОЛС охранные возможности расширяются. В планах ДО получение дополнительной информации с объекта: видео или фото. Это позволит принимать решения о направлении групп задержания и позволит экономить ресурсы. Применение новых методик потребует изменений в нормативных и правовых документах, в 2014 году мы планируем согласовать этот вопрос.

Кроме экономической части не менее важный вопрос – качество охраны, работа с ВОЛС, благодаря повышению технологичности, способна вывести охрану на более высокий уровень.

Ранее заявлялось о необходимости разработки единого протокола для ТСиСО? Ведутся ли такие работы с производителями оборудования?

Сейчас ДО совместно с белорусскими производителями ведется работа по созданию единого протокола для ТСиСО. Единый протокол даст возможность сопряжения более широкой линейки оборудования с пультами различных производителей. Это позволит ДО диктовать производителям свою политику и требования в разработке новых средств и систем охраны. Если отечественные производители не смогут соответствовать нашим требованиям, мы будем обращать внимание на ведущих мировых производителей.

Какие работы планируются по обучению, повышению квалификации специалистов ДО и лицензиатов?

Запущены процессы по повышению квалификации и обучению нескольким профессиям. Посредством специализированных курсов будем повышать квалификацию электромонтеров и дежурных пульта управления. На базе УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь планируется создание современной технической базы (с включением максимально полной линейки современного оборудования) для повышения квалификации электромонтеров, на её основе будут изучаться современные технологии и каналы связи.

Будут ли изменения в правилах и условиях при проведении тендеров ДО на закупку оборудования в 2014 году?

Нормативные документы, регламентирующие правила проведения тендеров не изменились, таких изменений не предвидится. Единственное, что хотел бы отметить – это то, что при проведении тендеров мы более внимательно будем учитывать статистику отказов оборудования, т.к. на сегодняшний день для Департамента охраны важно качество и надежность установленных охранных средств и систем.

Беседовал Драгун Сергей

ЭКСПЕРТНЫЙ ОБЗОР
Комментарии экспертов, участников рынка

Руководители, специалисты-эксперты ведущих компаний нашей страны подводят итоги, комментируют тенденции, состояние и предлагают прогнозы развития сегментов безопасности Республики Беларусь.

Вопросы, темы:

Экономика:

1. Продажи, объемы: рост/снижение, в % к прошлому (2012 году);
2. Тенденция развития, планы на 2014 год;
3. Факторы роста/снижения;
4. Достижения сегмента в 2013 году.

Технология (Технологические тренды):

1. Популярные продукты (системы), их особенности;
2. За счет каких технологий продукт популярен в РБ).

Проблематика сегмента (факторы влияющие на развитие/ сдерживание сегмента):

1. Нормативное регулирование;
2. Экономика/политика (административные, кадровые и пр.);
3. Прочее.

Достижения компании в 2013 году:

1. Знаковые проекты и решения с участием продуктов компании (выполненных в 2013 году).

Аларм, НТ ЗАО

Шелюто Дмитрий Эдуардович, заместитель главного конструктора

Сегмент: Технические средства и системы охраны.

Оборудование: Разработчик и производитель систем передачи извещений о проникновении и пожаре «АСОС Алеся», приборы приемно-контрольные охранные, пожарные и охранно-пожарные.

Экономика:

- Падение объемов продаж на 30%.
- Факторы снижения: уменьшение объемов закупок со стороны Департамента охраны (ДО); переход охранных сигнализаций на новые каналы связи (ВОЛС).
- Планы и перспективы на 2014 год: увеличение объемов за счет перехода на ВОЛС.

Технологические тренды сегмента охранной сигнализации в Беларуси в 2013-2014 гг.:

- Переход на новые каналы связи: ВОЛС (в частности – GPON), GPRS, 3G, 4G.
- Первые примеры использования информации с СВН при централизованной охране и мониторинге объектов (т.е., с выводом информации на ПЦН Департамента охраны). Данные технические решения имеются у всех производителей СПИ в Беларуси («Ровалэнт», «Новатех», «Аларм»). Однако применение СВН при централизованной охране объектов продвигается не быстро. Основные факторы, влияющие на повсеместное использование СВН в охранном мониторинге, в первую очередь, – отсутствие у заказчиков желания на использование такой услуги, неопределенность/отсутствие нормативной базы, отсутствие высокоскоростных каналов связи на удаленных объектах (3G), стоимость аренды каналов.
- Разработка/принятие единого протокола для ТСиСО, который позволит выполнять подключение широкой линейки оборудования, с пультами различных производителей. В 2013 году создана рабочая группа из представителей белорусских компаний-производителей пультового оборудования: ЗАО «Аларм», НПО «Агат», ЗАО «Новатех», «Ровалэнт» и регулятора ДО. Рассматривался вопрос необходимости доработки протокола под всех производителей, либо принятия единого универсального протокола. На сегодняшний день рассматривается принятие протокола DC-09 как базового.

Справка ТБ:

ANSI/SIA DC-09 – открытый протокол транспортного уровня. На нем работают порядка 17 производителей в Северной Америке и Канаде.

Логический уровень обмена должен быть реализован каждым производителем ПЦН под всю существующую в Беларуси линейку приборов (производители должны обменяться протоколами). В результате, любой прибор производства «Ровалэнт», «Новатех», «Аларм» будет работать с оборудованием СПИ «АСОС Алеся», СПИ «Неман», СПИ «Новатех-РДО» по Ethernet каналам, а в будущем и по GPRS (3G, 4G). К концу 2014 г. началу 2015 г. должны начаться работы по внедрению нового протокола. Собственником протокола будет регулятор – ДО.

Ход работ по переходу систем охранной сигнализации на оптоволоконные линии связи, проблематика:

– В настоящий момент уже имеется ряд объектов с ППКОП, работающих по Ethernet (xDSL, GPON) на ПЦН как СПИ «АСОС Алеся», так и СПИ «Неман», СПИ «Новатех-РДО» в Беларуси (Гомель, Витебск, Минск, Могилев). На сегодня (февраль 2014 г.) можно говорить о первых полноценных подключениях ОС на квартирах и объектах, оборудованных модемами GPON. Департаментом охраны МВД РБ совместно с РУП «Белтелеком» разработаны и согласованы карты сети для каждого отдела ДО по всей Республике, закуплено требуемое

оборудование (сервера управления и DHCP сервера), согласована тарифная политика. В Минске уже проведена установка и настройка серверного оборудования на площадях РУП «Белтелеком», перестроены карты сети на ПЦН, подключен ряд квартир (Фрунзенский отдел ДО). В ближайшее время будет начать процесс подключения квартир и объектов в Центральном, Заводском отделах ДО (в этих районах наибольшее количество домов с ВОЛС). На конец февраля 2014 г. запланированы курсы повышения квалификации специалистов областных подразделений ДО МВД РБ в части настройки и администрирования сетей. После проведения своего рода «обкатки» в Минске, установки ППКО, работающих по Ethernet каналам, начнутся в областях.

Для объектов, где уже были установлены охранные приборы, работающие по стандартным ТЛФ линиям, и планируется переход под оптоволокно (или уже данное переключение произведено), подключение будет производиться через приставку – блок сопряжения БС-«Аларм»-Ethernet.

Оценка и вопросы защиты информации (целостность, доступность, конфиденциальность) при прохождении сигнала в сетях ВОЛС по технологии xPON (GPON):

– Возникает ряд вопросов, связанных с политикой безопасности при эксплуатации ППКО Ethernet по сетям GPON. Терминал MT-PON-AT, установленный у абонента, организует выход как в открытую сеть Internet, так и в закрытую Intranet сеть, организованную для нужд Департамента охраны МВД РБ. Естественно, весть тракт обмена между ПЦН и объектовыми приборами защищается с помощью современных алгоритмов кодирования, однако необходимо рассмотреть ряд организационных мер, для исключения вмешательства со стороны пользователя. Например, возможен запрет на применение абонентского модема с MT-PON-AT с функцией Wi-Fi.

Вопросы обеспечения бесперебойного питания:

– В данный момент РУП «Белтелеком» поставляет абонентские терминалы MT-PON-AT с сетевыми адаптерами без встроенных резервных источников питания (возможно, при следующих закупках оборудования ситуация изменится). Вследствие этого, при установке охранного прибора на объект, резервное питание абонентского терминала осуществляется непосредственно от ППКО. В апреле 2013 г. в ДО МВД РБ принято решение, обязывающее всех производителей объектовых приборов в РБ повысить мощность блоков питания изделий (в частности, предусмотреть 2 выхода по питанию (для подключения GPON MT-PON-AT и для датчиков), отдельную защиту по выходам и т.д. В настоящий момент все производители прошли необходимые испытания и начали выпуск приборов в соответствии с требованиями ДО.

Эффективность эволюционного перехода СПИ АСОС «Алеся-01» на ВОЛС без существенной замены верхнего уровня СПИ (ОС «Windows XP» («Windows-7»), изменение конфигурации ПЭВМ для АРМ ДО/ДИ/ДПЦО, серверов):

– С точки зрения существующей конфигурации ПЦН практически ничего не изменилось. Программное обеспечение «Алеся-01» построено очень гибко. Были дополнительно разработаны новые программы транспортного уровня для парка Ethernet приборов, и сейчас ПЦН «Алеся-01» поддерживает как весь существующий парк оборудования (приборы, ретрансляторы), работающие по проводным и GSM (GPRS) каналам связи, так и новые приборы, работающие по каналам Ethernet. Интерфейсную часть программ мы стараемся поддерживать, т.к. она достаточно оптимизирована и за 15 лет операторы уже привыкли к определенным действиям. Однако надо учитывать, что раньше большая часть транспортного потока обрабатывалась ретрансляторами, установленными на АТС (либо модулями сопряжения «Alarm-GSM», установленными на объектах). Сейчас весь поток информации, поступающий от ППКО-Ethernet, обрабатывается непосредственно на ПЦН. Вероятнее всего, при увеличении количества абонентов с ППКО-Ethernet, необходимо будет дополнительно устанавливать на ПЦН IP-сервер транспортного уровня, который будет выполнять роль, аналогичную существующим ретрансляторам. То же, кстати, касается и развития СВН при передаче видео на ПЦН – необходимо будет устанавливать дополнительный сервер для обработки видеоданных.

Влияние принятия технических регламентов Таможенного союза на рынок охранных систем:

– Ситуация до конца не ясна. Пока признаются белорусские сертификаты на рынке РБ, однако через полгода для всех производителей сертификация ТС будет обязательна. Сейчас 4 регламента подходят под ОС. До конца нет согласованности ТР между странами. Откроется ли рынок соседних стран? Мы планируем проведение сертификации с учетом новых ТР в конце 2014 года. ■

Атлас Радио (ЧУП «Технический центр «Атлас радио»)

Кудрявцев Сергей Васильевич, главный инженер

Сегмент: Комплексное выполнение услуг по созданию радиосистем связи.

Оборудование: 1-й поставщик в Беларуси радиомодемов и антенно-фидерных устройств.

Экономика:

- Продажи в сегменте за 2013 год: рост объемов продаж в 3 раза.
- Факторы роста/снижения: активное использование оборудования в системах видеонаблюдения.
- Категория объектов: обеспечение канала связи (в т.ч. для систем безопасности и СВН) на строительных площадках, для мониторинга протяженных участков: теплицы, сельские хозяйства, склады и пр.

Планы и перспективы на 2014 год:

- Получение сертификатов Таможенного союза.
- Освоение новой линейки оборудования (для силовых структур) с большей производительностью и стабильностью канала.

Популярные продукты в 2013 году:

- Радиомодемы UniFi с использованием внутренних точек доступа при организации канала связи, организации Wi-Fi сети в учебных, офисных и пр. помещениях.

Знаковые проекты:

- Передвижные командные пункты МВД.
- Организация сети Wi-Fi в БПУ, БНТУ.
- Организация сети Wi-Fi в логистических центрах ООО «Мегатоп», ОДО «Тут и Там Логистик».
- Комплекс радиосвязи на заводе «Гранит», порядка 12 точек (Инсталлятор «СпецТоргЛаб»). ■

ELKO.BY

Владислав Гранатов, менеджер по работе с продуктовой линейкой Schneider Electric

Сегмент: СВН

Оборудование: ТМ Pelco (СВН)

Экономика:

- В 2013 году компания ELKO.BY стала дистрибьютором Schneider Electric по ТМ Pelco (СВН), и мы имеем также прямой европейский контракт с Pelco;
- Давая объективный прогноз на 2014 год, думаю, что динамика продаж продуктов Pelco сохранится на уровне 2013 года, планируется рост продаж, но он не будет скачкообразным.

Факторы роста:

- использование бренда в крупных проектных решениях;
- наличие системы управления Pelco Endura;
- появление новых моделей IP-камер, кожухов и аксессуаров;
- спрос на IP СВН;
- нормативное регулирование СВН – линейка Pelco полностью сертифицирована в РБ.

По заявлению директора представительства Schneider Electric в Беларуси Антона Королева, «Pelco – это продуктовый бренд, под которым мы предлагаем как камеры видеонаблюдения, так и другие средства сбора, хранения и представления визуальной информации, но далеко не единственный, с точки зрения сегмента бизнеса. Мы рассматриваем это направление как бизнес интегрированных систем безопасности и автоматизации зданий».

Тенденции развития:

- Основная тенденция – массовый спрос на IP СВН;
- У Pelco идет обновление линейки IP-камер СВН, новые камеры разделены на три условные группы:

1. Начальный бюджетный уровень (камеры серии Sarix IL);
2. Серия Professional (новые камеры серий IXP/IBP/IMP), являющаяся наиболее оптимальной для использования в проектных решениях;
3. Серия Enhanced (камеры IXE/IME с поддержкой набора технологий SureVision) для решений, где требуется использование дополнительного функционала и расширенных функций видеоаналитики.

- Состоялся альянс Pelco™ by Schneider Electric™ и Oncam Grandeye, благодаря которому появились камеры кругового обзора Evolution 360°.
- Появились новые модели кожухов (EH16) и появилась возможность заказа собираемых и испытываемых на заводе готовых комплектов ImagePak на базе новых камер и новых усиленных кожухов. Кроме того, обновились линейки инжекторов питания и медиаконвертеров.

Знаковые проекты в 2013

- Стадион ФК БАТЭ, гостиница Виктория. ■

EverFocus

EverFocus Electronics Corporation (Тайвань)

Евдокимов Сергей, региональный менеджер

Сегмент: СВН
Оборудование: EverFocus (СВН)
Экономика:

- Увеличение продаж по белорусскому рынку на 20% (к 2012 году).
- Факторы роста: увеличение продаж EverFocus произошло в сегменте IP (камеры, сетевые регистраторы); один из факторов роста – интеграция оборудования EverFocus практически во все ведущие программы по видеонаблюдению; конкурентное преимущество реализуется за счет предложения комплексных решений, за счет более плотной работы с партнерами, дистрибьюторами, непосредственно с вертикалями (ритейл, банковский сегмент и пр.).

Планы на 2014 год:

- Продвижение IP решений для средних и крупных объектов.

Технологические тренды, новинки EverFocus:

- Выпуск 5 Мп купольной IP-камеры (февраль 2014 г.), в 1 квартале 2014 г. будут 5 Мп уличные камеры с ИК-подсветкой.
- Разработка профессиональной линейки сетевых регистраторов (NVR) для IP-камер на 32 канала и выше.

Тенденции развития сегмента СВН:

Тенденции схожи для всего постсоветского пространства. Можно отметить общие:

- Рост IP.
- Рост ценовой конкуренция. Как результат, востребованы бюджетные решения (в массовом сегменте), либо высокотехнологичные решения (где цена не является первостепенной). Конечно, влияют и внутренние процессы, либо нормативные акты. Например, в Молдове периодически возникают вопросы по «белым поставкам», это влияет на рынок.
- На рынке Беларуси наиболее популярны 2 Мп камеры. Они заложены в большинстве реализованных проектов. Данного разрешения достаточно для решения большинства задач.

Знаковые проекты в 2013 году:

Был реализован ряд крупных проектов на оборудовании EverFocus:

- В сегменте ритейла: гипермаркет «Корона» (Минск, Уручье), ТЦ «Замок» (пр. Победителей).
- Логистические объекты. ■

АВАНТ-ТЕХНО
системы безопасности

«Авант-Техно», ОДО

Красногоров Александр Михайлович, начальник отдела систем видеонаблюдения

Сегмент: СВН
Оборудование: ТМ Hikvision (HV)
Экономика:

- Рост продаж в 2013 составил 30 % к 2012 году, планируем, что в 2014 году рост составит не менее 30% к 2013г. В этом году мы снизили объемы на гос. закупках но очень серьезно продвинулись на коммерческих заказчиках, когда можно «доказать, показать, сравнить и объяснить» по преимуществам оборудования.

Факторы роста:

- Рост продаж в 2014 году будет стимулироваться в т.ч. выполнением дилерских обязательств перед Hikvision. Следует отметить, что планы по росту в компании Hikvision основываются на серьезных статистических исследованиях национальных рынков.
- Высокая технологичность оборудования HV. Этому способствует максимально быстрое внедрение HV при производстве в свое оборудование самых последних технологических разработок, научных решений. По скорости внедрений HV опережают таких мировых «мэтров» как Honeywell, Bosh и пр. Это позволяет улучшать качество изображения, оптимизировать затраты на производство и пр.
- Надежность оборудования, конкурентно-способная цена на рынке. Факторы: внедрены серьезные программы по выявлению некачественной сборки/брака, проводятся серьёзные испытания продукции HV, например – 100 % термо-тренировки оборудования. Перед запуском продукта идет многоступенчатая программа испытаний на локальных рынках Китая. Проведены оптимизации производства и схемотехники (прямое сотрудничество с ведущими мировыми производителями микрочипов, напр. Texas Instruments, США).
- Приближение IP технологий к неспециализированным пользователям. Рост реализации аппаратных IP регистраторов произошел благодаря простоте устройства и легкости работы с ним. Сейчас Hikvision сделал IP регистратор, ничем не отличающийся от аналогового (по простоте интерфейса, по уровню обслуживания, по надежности работы и пр.).

Тенденция развития, планы на 2014 год:

- Наибольший рост продаж наблюдается в реализации IP продукции: ка-

меры, регистраторы.

- Самая популярная линейка IP камер Hikvision – 3 Мп камера. Сейчас Hikvision готовит новую модель с разрешением 6 Мп. В будущей разработке – 10 Мп (под специальные проекты) но полного комплексного решения по таким камерам еще нет (малогабаритная оптика, мониторы и пр.).

- Внимание разработчиков HV сейчас сосредоточено на выпуске 5 Мп камеры, со скоростью записи 25 К/сек. Камера предназначена для работы в городских условиях. Данное решение будет впервые реализовано в мировой практике как массовое решение. Камера планируется с качественной оцифровкой, без искажений, анонс запланирован на 2014 год.

- Популярные продукты в Беларуси: вандалостойкая IP камера Hikvision DS-2CD7153F, офисная IP камера Hikvision DS 2CD8153F.

Технологические тренды:

- Развитие облачных сервисов. HV активно разрабатывают облачные сервисы. В 2013 году стали партнером многих мировых лидеров по облачным сервисам. Широкая линейка камер уже интегрирована в сервис.

- Интеграцию камер в софт. Производители софта сами инициируют и предлагают HV интеграцию оборудования в свои платформы. Как признанные гранды Exacq, Milestone, Seetec и пр. так и небольшие компании. Сегодня около 100 производителей ПО уже интегрировали камеры HV (на уровне протокола) (в свой софт), в т.ч. HV естественно поддерживает Onviif.

Проблематика сегмента (факторы влияющие на развитие сегмента СВН):

- На рынке много ТМ и оборудования с характеристиками не соответствующими заявленным. Сейчас идут подделки другого уровня. Раньше шла имитация бренда Pelco – Pelko, Sony – Sonu и пр. Теперь идет технологические имитации – в паспортах и технических характеристиках указываются аналогичные или завышенные характеристики известных торговых марок: чувствительность, качество, количество ТВЛ и пр. Проверить очень сложно. Но мой взгляд в сегменте СВН среди малоизвестных ТМ такого оборудования не менее 50%.

Зачастую заказчик при обращении к нам серьёзно сравнивает наше оборудование по цене, тех. характеристикам и пр. с ТМ о которой мы никогда не слышали. При получении информации о данном производителе на сайте madeinchina.com выясняется, что компания имеет штат в 20 человек, оборот 30 млн. долларов в год. Противопоставляется компания HV имеющая около 2000 человек только научного персонала и более 7000 рабочих, около 200 патентов, оборот 1,5 млрд. долларов (2014г) и пр. Это говорит только о том, что не может соответствовать заявленные тех характеристики реальным возможностям малоизвестной марки. Причем такой производитель не несёт никакой ответственности за информацию в тех паспорте.

- Несовершенная система проведение тендеров по СВН в Беларуси. Тендера проводятся «вслепую», нереально таким образом выбрать оборудование для СВН учитывая специфику. Как правило, мы предлагаем проводить дополнительно к торгам стендовые испытания на объекте. Только на примерах можно демонстрировать качество СВН. В этой связи у нас родилась шутка, 3 категории СВН в Беларуси: «Чтобы было», «чтобы работало» и «для себя».

Знаковые проекты и решения с участием продуктов компании (выполненных в 2013 году):

- Бизнес-центр класса А, на пр. Держинского (порядка 150 IP камер, внутреннего и наружного исполнения).

- Все магазины «5 элемент» (1500 камер: заказчик выбрал для торговых залов – 2 Мп камеру).

- Сеть (около 30 магазинов) «МегаТоп», передача по каналам 3G (оператор Life) с возможностью для руководителей вести мониторинг на мобильных устройствах. ■

ITV axxon Experience The Next

АкссонСофт, Унитарное предприятие

Лисовский Дмитрий, коммерческий директор

Сегмент: Системы управления видеонаблюдением (VMS – video management systems), видеоаналитика, интегрированные системы безопасности.

Оборудование: интегрированная система безопасности «Интеллект» и система интеллектуального видеонаблюдения Axxon Next.

Экономика:

- Увеличение основных продаж на 75% (к уровню 2012 года).

- Планы на 2014 год – удержать заявленный уровень продаж.

- Факторы роста: динамичное развитие самого рынка СВН; уникальная технология интеллектуального поиска архивной информации, интеграция с различными системами безопасности.

Популярность продукта обеспечивается за счет:

- Увеличения запросов заказчиков на создание систем видеонаблюдения с аналитическими функциями: интеллектуальный быстрый поиск в архиве по заданным постфактум событиям, деление объектов на категории (люди, машины и т.д.), поиск по цвету и пр.

- Возможности объединения в единой системе любого количества аналоговых и IP-каналов.

- Возможность интеграции с различными системами СКУД и ОПС.

- Применения технологии оптимизации нагрузки на сеть передачи данных и места мониторинга.

Технологические тренды:

- Развитие аналитического модуля распознавания лиц. В частности, в последнюю версию Интеллект 4.9. интегрирован модуль распознавания лиц компании Cognitec v.8.8, что значительно улучшило захват и распознавание лиц в реальных условиях. Первый проект с использованием

нового модуля реализован в метро Санкт-Петербурга, станция «Ладожская». Результат распознавания лиц составляет около 95%, при естественном поведении людей.

Знаковые проекты компании в 2013 году:

- Центр мониторинга ГАИ Мингорисполкома, продукт – «Интеллект», партнер – ЗАО НПП «Белсофт».
- Городская СВН города Жлобин («Дожинки 2013»), продукт – Axxon Next, партнер – ОДО «Мультисофт».
- Социальные проекты: более 100 школ города Минска, продукт – Axxon Next, партнеры – СООО «Саммит Технолоджиз», ЗАО НПП «Белсофт».
- Филиалы Нацбанка, продукт – «Интеллект», партнер – НПООО «Акова».
- СВН и контроля кассовых операций магазинов Duty Free, продукт – «Интеллект», партнер – ЧТУП «Систематикс».
- СВН предприятия «Санта Бремор», предприятия «Кварцмелпром», продукт – «Интеллект», партнер – ООО «Научно-производственная фирма ТриС». ■

Дивитек, ООО

Корда Андрей Николаевич, директор

Сегмент: Системы видеонаблюдения. Системы контроля и управления доступом. Комплексные системы безопасности.

Оборудование: Системы видеонаблюдения: ТМ Beward, Acumen, Tantos. Оборудование для передачи сигналов SC&, OSNOVO, TFORTIS. Видеосерверы SOVA, видеоаналитика распознавания автономеров «НомерОк».

Экономика:

- Продажи в сегменте за 2013 год: компания открыта в апреле 2013 года, год закрыт с прибылью.

Достижения в 2013 году, планы на 2014:

- Создание и развитие дилерской сети на территории Республики Беларусь, внедрение оборудования СВН под ТМ «Дивитек» на объектах. Дальнейшее продвижение ТМ на рынок Беларуси, в т.ч. посредством участия в выставке-форуме «Центр безопасности. Инженерно-техническая безопасность 2014».

Популярные продукты (системы) в 2013 году:

- Гибридный видеорегистратор «Дивитек» с возможностью работы в облаке и каналом видеоаналитики, видеокамеры 700, 800, 1000 ТВЛ «Дивитек», IP-камеры «Дивитек». Популярность продуктов обеспечивается использованием технологий: гибридные технологии видеонаблюдения, комплексные решения Sova (с использованием видеоаналитики распознавания номеров, подсчет очереди, мгновенный поиск в архиве, работа с Pos-терминалами и др.).

Проблематика сегмента (факторы, влияющие на развитие/сдерживание сегмента):

- Нормативное регулирование не оказывает заметного влияния на развитие сегмента (все наши продукты удовлетворяют требованиям нормативных документов по тех. параметрам).
- Административные, кадровые факторы: отсутствие профессионалов на различных уровнях принятия решения (при проведении тендеров, закладке оборудования, формировании технического задания и пр.). Как следствие – проектирование систем видеонаблюдения на устаревших моделях оборудования и технологиях.

Знаковые проекты и решения с участием продуктов компании (на 2013 год):

- Создание системы видеонаблюдения на логистическом центре компании «ТУТ и ТАМ Логистикс» (Прилесье) на базе серверов Sova.
- Внедрение системы «НомерОк» на предприятии ЖКХ. ■

Унибелус, СП ООО

Манойленко Иосиф Анатольевич, директор

Сегменты: Оказание комплексных услуг в сегменте безопасности.

Экономика:

- Состояние отрасли безопасности напрямую зависит от состояния экономики страны, в частности, от количества строящихся объектов.

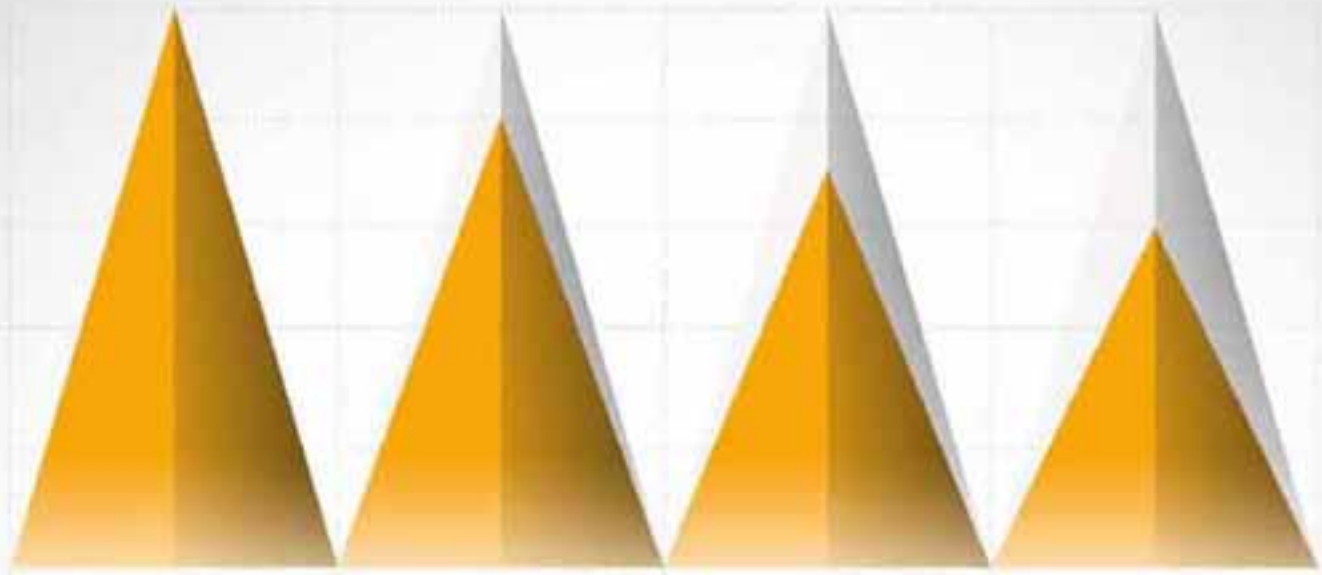
Тенденция развития, планы на 2014 год:

- На ближайший год лидером в финансовых объемах будет сегмент пожарной сигнализации и автоматики. Причины – сегмент стабилен, присутствуют импортные игроки, есть конкуренция.
- Можно прогнозировать падение объемов продаж в сегменте СВН (по крайней мере, в среднем ценовом сегменте). Причины: насыщение рынка, уменьшение количества вновь возводимых объектов, соответственно начнется борьба за рынок бюджетных решений. На росте сегмента СВН скажется введение норм по СВН, но возникнут угрозы формального подхода к установкам СВН (как обязательного). Заказчикам станут не интересны качественные установки, есть риск создания проектов по «видимости видео».
- Меняется структура рынка СВН Беларуси, появился ряд небольших компаний, представителей крупных российских импортеров, имеющих техническую поддержку, которые работают в сегменте бюджетного СВН, они начали занимать долю рынка.
- Благодаря нормативной базе, национальные производители пока защищены. Но принятие общих нормативных документов (разрешительной нормативной базы) с Россией (и странами Таможенного союза) в сегменте ОПС вопрос ближайших лет.
- Успешно конкурировать на рынке России (Таможенного союза) имеют шанс белорусские инсталляторы при оказании комплексной услуги (проект, монтаж, инсталляция), т.к., например, рынок России требует комплексного подхода. Нашей компании интересны сложные инженерные решения, мы видим свою перспективу в реализации знаний, освоении новых технологий, серьезных поставок, проектов и пр.

NOVUS®

Профессиональные решения для систем безопасности

4 НОВЫЕ СЕРИИ КАМЕР
инновационные разработки



800 SERIES

разрешение 960H

600 SERIES

разрешение 960H

400 SERIES

разрешение 960H

200 SERIES

Дистрибьюторы оборудования NOVUS® в Беларуси:

СМАРТ ПРОЕКТ

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

новатех

Новатех Системы Безопасности ЗАО
ул. Городецкая, 38А, 3й этаж
г. Минск 220125, Беларусь
+375 17 206-39-51, +375 17 206-39-52
sales@novatekh.by, www.novatekh.by

RVi

www.rvi-cctv.by

НАДЕЖНОСТЬ И ФУНКЦИОНАЛЬНОСТЬ

СЕТЕВЫЕ КОММУТАТОРЫ RVi

RVi-NS1602

Power 240 Вт | PoE | PoE 16 port | 19" [1U] Rack mount | 2 port SFP combo

RVi-NS2402

Power 360 Вт | PoE | PoE 24 port | 19" [1U] Rack mount | 2 port SFP combo

RVi-NS0800

Power 120 Вт | PoE | PoE 8 port

RVi-NS0401

Power 60 Вт | PoE | PoE 4 port

НОВОЕ ТОВАРНОЕ НАПРАВЛЕНИЕ - НОВЫЕ ВОЗМОЖНОСТИ!

ГАРАНТИЯ 3 ГОДА

RVi Group

+7 (495) 735 3847, 735 3857

Технологические тренды:

- Стал очевидным массовый переход на IP СВН, СКУД и пр. Думаю в ближайшие 2-3 года большинство систем безопасности «уйдет» в IP. Соответственно безопасность «уйдет» от простых решений, как результат небольшие бюджетные объекты будут централизоваться, объединяться в большие сети. При таком темпе развития оптических каналов связи, лет через 5, например, будет возможно собрать на единый пульт всю сигнализацию в Минске.

- Сегмент охранных систем достаточно консервативный, прорывных решений не ожидается. В перспективе будут востребованы сложные комплексные решения с быстрой, удобной инсталляцией и расширенным функционалом. Как пример можно привести развитие технических решений у компании «Болид», кроме того их системы находятся в отличном сочетании цена/качество. ■

СервисСбытАвтоматика, УП

Чичиков Александр, коммерческий директор

Сегмент: Пожарная сигнализация и автоматика.

Оборудование: Дистрибьютор СЗАО «Аргус-Спецавтоматика», радиоканальная система (РС) «СТРЕЛЕЦ», ОАО «Завод Спецавтоматика».

Экономика:

Продажи в сегменте за 2013 год:

- Снижение продаж по основным позициям ОПС и пожарной автоматики, около 35% (к 2012 году).

- Увеличение продаж РС «СТРЕЛЕЦ» на 70% (к 2012 году).

- Факторы роста: РС «СТРЕЛЕЦ» становится более известной на белорусском рынке; пришло понимание заказчиков преимуществ радиоканала перед проводными системами; клиенты, опробовавшие систему, стремятся применить ее на новых.

- Достижения в 2013 году: наша команда смогла обратить внимание корпоративных клиентов на РС «СТРЕЛЕЦ»; в частности, ряд банков строящиеся филиалы проектируют на РС «СТРЕЛЕЦ».

Тенденция развития, планы на 2014 год:

- Повышение спроса на РС «СТРЕЛЕЦ», увеличение объемов продаж системы.

Проблематика сегмента (факторы, влияющие на развитие):

– Нежелание проектных учреждений к изучению и внедрению новых решений. Как аргумент звучит – отсутствие времени на изучение новых продуктов.

Знаковые проекты и решения с участием продуктов компании (на 2013 год):

- В Беларуси: Новый Червенский рынок в Лошице (Минск); Архикафедральный костел (Минск), филиалы ОАО «Приорбанк».

- В России и Европе: ЦУП в г. Внуково (РФ); Саммит G20 в Санкт-Петербурге (сентябрь 2013 года) обеспечение пожарной безопасности; Корабли Королевского ВМФ Великобритании. ■

Новатех Системы Безопасности, ЗАО

Рунов Юрий Адольфович, директор

Сегменты: Технические средства и системы охраны. Пожарная сигнализация и автоматика. Системы видеонаблюдения.

Оборудование: Системы пожарно-охранной сигнализации и радиоохраны, комплексные системы охранного видеонаблюдения ТМ Novus, «2x2».

Экономика:

- Снижение продаж в сегменте СВН примерно на 20%.

- Рост продаж в сегменте охранных систем (ОС).

- Факторы роста/снижения: отсутствие финансирования на крупных объектах; рост в сегменте ОС за счет ранее «раскрученного» оборудования (извещателей). Благодаря переходу ОС на ВОЛС наблюдается рост спроса на ПКП с Ethernet-каналом.

Тенденция развития, планы на 2014 год:

- Считаю сегмент СВН самым быстрорастущим. Ожидаем рост продаж по СВН (завершение прошлых проектов). При участии в проектах используем имеющуюся линейку СВН: «средний» уровень используем Novus, «нижний» сегмент собственной линейкой «2x2».

- Планируем продвижение на рынке собственной линейки СВН под брендом «2x2». Позиционируем её как недорогую линейку (аналоговые камеры стоят примерно по 30 долл.), с возможным применением на социальных объектах: школы, д/сады и пр. Сейчас ведем испытания IP-камер, перспективность вывода на рынок которых рассматриваем. Причина та же – ценовая конкуренция и необходимость наличия бюджетной линейки.

- Развиваем собственный сегмент пожарной безопасности, в течение 2-х месяцев планируем вывести ранее

нами продаваемые пожарные извещатели ИП 212 (дымовые).

- В сегменте охраны планируется обновление ассортимента, в частности ведется доработка нашего пультового оборудования, что даст возможность для работы наших пультов с оборудованием СПИ «Алеся». Таким образом, ДО сможет устанавливать пульты любых производителей.

Технологические тренды:

- В Беларуси активно развиваются беспроводные и проводные цифровые (Ethernet) технологии передачи информации. В них заложен большой потенциал для развития систем безопасности.

- Думаю, что благодаря развитию каналов связи существующие в стране системы охранного мониторинга получат новый виток развития, т.к. на сегодняшний день они дошли до предела своих технологических возможностей.

Достижения компании в 2013 году:

- Компанией заложен фундамент по переводу производства приборов и оборудования на новый, более качественный уровень (в сегментах СВН, охранного оборудования и пр.). Проведен ряд мероприятий, позволяющий компании больше сконцентрироваться на качественной разработке и инжиниринге.

- Самым знаковым была победа на тендере НИИ ПБ и ЧС МЧС РБ по закупке работ для выпуска СПИ «Молния». ■

ROVALANT

РовалэнтСпецСервис, ООО

Полев Михаил Викторович, директор

Сегмент: Разработка, производство комплексных средств и систем безопасности.

Оборудование: ИСБ "777", АСПС «Бирюза», СУОЭ «Гонг», СПИ "Нёман".

Экономика:

- Снижение объемов реализации в 2013 году, ожидаем незначительное снижение в 2014 году.

- Факторы снижения – уменьшение объемов строительства в стране.

Тенденция развития рынка:

- Рынок сужается, платежеспособность ухудшается, идет ценовая конкуренция. На рынке востребованы и инсталлируются дешевые продукты, в т.ч. на ответственных критически важных объектах (КВО). Возникают сложности при внедрении инновационных решений, т.к. такие решения находятся в высокой ценовой категории, хотя в эксплуатации более эффективны и выгодны.

- Продолжит развитие сегмент IP СВН в связи с принятием соответствующих законодательных актов. С одной стороны сформированные требования подтолкнут к более широкой установке СВН, с другой – из-за недостаточно проработанных технических требований, лежащих в основе принятых законов, стимулируется установка самой дешевой продукции, в том числе на КВО, в ущерб качеству обеспечения безопасности. Можно прогнозировать лавину подключений, основанных на дешевых некачественных китайских камерах, а через некоторое время пойдет массовый отказ оборудования и недовольство качеством камер и получаемого изображения со стороны потребителей.

(Примечание: Подробнее обсуждение норм СВН см. ТБ №1, 2014 год)

Новые разработки и решения, реализованные компанией «РовалэнтСпецСервис» в 2013 году:

- В сегменте средств и системы охраны реализована интеграция беспроводных извещателей «РИЭЛТА» (С-Петербург, Россия) в охранный прибор А16-512.

- Готов к выпуску новый 4-х портовый репитер для линий связи с интерфейсом RS485, совместимый со всеми системами производства «РОВАЛЭНТ»: ИСБ «777», приборами серии «А», АСПС «Бирюза», СУОЭ «Гонг» и оборудованием других производителей. Его возможности: организация любой топологии сети по интерфейсу RS485. Это изделие всегда было в составе ИСБ «777». Новый репитер выполнен на новой элементной базе с учетом всех потребностей рынка по части обеспечения надежности и резервирования линий связи. В нём заложены качественно новые возможности: 4 порта (2 из которых изолированные) с поддержкой более высоких скоростей (от 300 бит/сек до 115 Кбит/сек), поддержка большего адресного пространства (до 256 адресных устройств), работа от 12 В и 24 В. Имеет минимальную задержку, благодаря чему можно обеспечить длину линии связи до 7,5 км, применив до 4-х репитеров в линию. Аналогов на рынке нет, репитер можно использовать с любыми системами, где есть интерфейс RS485.

- Завершили разработку малогабаритного высокоэффективного квазирезонансного источника питания (ИП) со стабилизированным выходным током 2 А и напряжением 12 В. Планируются к выпуску два его исполнения: стабилизированный источник на 2А/30 Вт для встраивания в любые приемно-контрольные приборы и бесперебойный источник питания на 2 А с контролем состояния и управлением зарядом аккумуляторной батареи емкостью 7 А/ч. При их разработке учитывались требования Беларуси, России, Евросоюза и США. Таким образом, мы рассчитываем его продавать не только на внутреннем рынке, но и на экспорт, в другие страны мира. Блоки питания выделяются рядом качественных характеристик: имеют все необходимые защиты (защита от перегрузок по входу/выходу, защита от перегрева, от перегрузки по мощности), стабилизированный выход, КПД порядка 90%, минимальный уровень шумов, встроенную защиту от поражения электрическим током по классу II. В настоящее время

завершается разработка более мощных источников питания 12 В с использованием новых технологий на 5А/80Вт.

- Компания ООО «РовалэнтСпецСервис» в 2013 году стала официальным представителем фирмы Crow Electronics Engineering Ltd. в Республике Беларусь. До нас в Беларуси у этого известного и авторитетного в мире производителя официальных представителей не было. Мы побывали на производстве в Израиле, убедились в высоком уровне технологий и культуре производства. Имидж этих извещателей в стране высок, они исключительно надежны, имеют современный дизайн, все характеристики подтверждаются на испытаниях, при этом извещатели имеют разумную цену;

- Продолжение сотрудничества с Samsung Techwin в области видеонаблюдения. Нас устраивает уровень этого мирового производителя и те инновационные продукты, которые они разрабатывают. Сейчас Samsung Techwin сделал упор на выпуск камер с т.н. интеллектуальным видео. Выпущена серия IP-камер со встроенной аналитикой, есть линейка оборудования с высокой скоростью записи до 60 к/сек, при этом с низкой скоростью цифрового потока – до 3 Мбит/с.

- В сегменте СВН компания «Ровалент» планирует вывод новой недорогой линейки оборудования СВН.

- Продолжаем сотрудничество с корейской компанией Paradise Industry Co., Ltd – производителем спринклерных оросителей и узлов управления. Работаем с данной компанией несколько лет. Спринклеры отличаются соотношением цена/качество и хорошо себя зарекомендовали.

Проблематика сегмента:

- Принимая участие в крупных проектах в 2013 году и консультируя специалистов других организаций, мы столкнулись с проблемой – нежеланием многих инсталляторов изучать документацию на применяемое оборудование. В связи с этим у них возникают трудности в работе, а следом необоснованные претензии к оборудованию и ПО. На тех объектах, на которых работали мы или обученные нами специалисты других компаний, проблем нет. Мы всегда стараемся обеспечивать необходимую техническую поддержку. Для этого мы проводим семинары, в том числе обучающие с выдачей сертификата, обновляем документацию на сайте, даем консультации по телефону.

Знаковые проекты и решения с участием продуктов компании (выполненные в 2013 году):

– Дворец Независимости (ул. Орловская – пр. Победителей) – один из самых знаковых и ответственных объектов 2013 года. Высокие требования к надежности оборудования и ПО успешно удовлетворены применением АСПС «Бирюза» и ПО «АРМ-Сеть».

– РУП «Белтелеком», построение СКУД для разветвленной филиальной сети. Создана распределенная по всей территории Гомельской области система контроля и управления доступом, охватывающая все подразделения РУП «Белтелеком» с полной синхронизацией баз данных пропусков. ■

Национальная выставка-форум
«Информационная безопасность. Телекоммуникации»
2-3 декабря, 2013
Центр безопасности

Выставка-форум «Информационная безопасность. Телекоммуникации: 2013»

Symantec. Fima

Компания «АэркомБел» продолжает работу по созданию эффективных способов предоставления информации специалистам отрасли безопасности. Под брендом «Центр безопасности» уже проводится выставка «Инженерно-техническая безопасность». Проведя выставку «Информационная безопасность. Телекоммуникации: 2013» мы, как специальные медиа, создали цикл комплексного информационного обеспечения отечественных специалистов.

Важность тематики информационной безопасности (ИБ) растет. ИБ сегодня – это совершенно новые вызовы, ИБ из узкопрофильного занятия превратилась в политический фактор, который касается практически всех в обществе. К специалистам этого сегмента сегодня предъявляются очень высокие требования. Продукты в сегменте сложные, инновационные, наукоемкие. Обновление продуктов частое, требующее постоянного повышения компетенций для всех участников рынка.

Задача выставки-форума «Информационная безопасность. Телекоммуникации» – создать информационную среду. Стать мостом между заказчиками, пользователями и производителями, поставщиками продуктов и решений. В рамках деловой программы мы стремились предоставить первичную информацию от мировых лидеров, от лучших экспертов, от регуляторов отрасли, тем самым придать импульс, динамику развития сегмента информационной безопасности в нашей стране.

Мы планируем и далее развивать тематику и выставочные сервисы, ищем понимание потребностей белорусских потребителей. Мы хотим предоставлять более глубокую экспертизу, делать выставку более удобной для посетителей. В 2014 году учтем организационные недочеты, скорее всего мероприятие поменяет место проведения, поработаем над форматом. Поэтому нам важна обратная связь. Предлагайте идеи, темы. Мы готовы к общению.

Большое спасибо специалистам и компаниям, которые помогли создать это мероприятие. В первую очередь спасибо всем участникам: стендистам, докладчикам. Отдельная благодарность генеральным партнерам компаниям Symantec и Fima.

При организации мероприятия, взаимодействуя с регуляторами сегмента (ОАЦ, НИИ ТЗИ), мы впервые увидели инициативу и получили глубокую поддержку со стороны руководителей и специалистов государственных ведомств. Сейчас, занимаясь подготовкой следующих мероприятий, можно говорить о такой поддержке и участии, как об общем тренде.

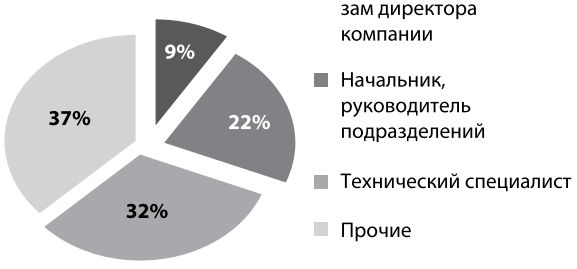
По итогам мероприятия сформирована база знаний, состоящая из видеороликов по материалам докладов, выступлений экспертов, круглых столов и презентаций.

Сайт: http://is.aercom.by

Статистика посетителей:

Профессиональная деятельность

Должностной состав



Беларусь в международном исследовании компании EY по информационной безопасности за 2013 год

В статье представлены результаты 16-го ежегодного международного исследования по информационной безопасности, которое проводилось также на территории Республики Беларусь. Проведено сравнение ответов респондентов из Беларуси с общемировыми тенденциями. В статье также приведены краткие рекомендации руководству по совершенствованию подходов к управлению информационной безопасностью.

Ворошилов Анатолий Леонидович,
консультант в области информационных технологий и ИТ-рисков EY, ИООО «Эрнст энд Янг»

Домнич Кирилл Викентьевич,
старший консультант в области информационных технологий и ИТ-рисков EY, ИООО «Эрнст энд Янг»

Об исследовании

Компания EY (до переименования в текущем году – Ernst & Young) уже 16 лет проводит международное исследование по информационной безопасности (ИБ), из них 4 года исследование проводится также на территории Беларуси.

В 2013 году в исследовании приняли участие 1909 респондентов из 64 стран и 25 секторов экономики. В Беларуси из 18 участников исследования – 11 банков, что позволяет говорить о том, что выводы исследования по Беларуси в большей мере характеризуют состояние дел именно в банковском секторе.

Исследование представляло собой самостоятельное анкетирование организаций по 32 вопросам, касающимся финансирования и инвестиций в информационную безопасность, управления безопасностью, эффективности мер по обеспечению безопасности, а также новейших технологий и тенденций в данной области.

Полные результаты исследования и аналитические материалы доступны на сайте www.ey.com/giss.

Наблюдение: увеличение внешних угроз и рост количества инцидентов безопасности в 2013 году

Компании приняли значительные меры для устранения угроз в области информационной безопасности. Однако количество и сложность угроз, а вместе с этим и количество инцидентов непрерывно возрастает, что ставит перед сотрудниками, ответственными за информационную безопасность, задачу не отставать от времени. В результате, разрыв между тем, что делают системы информационной безопасности, и тем, что они должны делать, увеличивается. Результаты исследования 2013 года свидетельствуют о том, что организации движутся в правильном направлении, но им предстоит еще многое сделать, причем незамедлительно.

Беларусь в международном исследовании EY по информационной безопасности 2013

В целом, по большинству вопросов исследования мнение участников из Беларуси и организаций со всего мира отличается незначительно, и Беларусь по многим вопросам находится в общемировом тренде. Однако есть и исключения с заметными различиями. Именно на их обзоре мы бы хотели сконцентрироваться в данной статье.

Четверть респондентов в Беларуси отметили увеличение числа инцидентов безопасности в 2013 году, при этом оценка роста инцидентов более консервативная по сравнению с мировыми показателями (Рисунок 1).

У 39% респондентов в Беларуси увеличились затраты на ИБ в текущем году, и более 56% организаций планируют увеличить затраты на ИБ в 2014 году (Рисунок 2).

Учитывая бурное развитие информационных технологий (ИТ), в организациях ежегодно значительно возрастают объемы данных в электронной форме, количество информационных систем и их пользователей, количество ИТ-зависимых бизнес-процессов. Если проводить аналогии со сферой обеспечения физической безопасности (физическая охрана объектов), то следует себе представить периметр и территорию организации, которая каждый год в несколько раз увеличивается, при этом увеличивается количество сотрудников и посетителей, а ценность охраняемых объектов и материального имущества возрастает. Гораздо

Рис. 1. Количество инцидентов безопасности за 2013 год

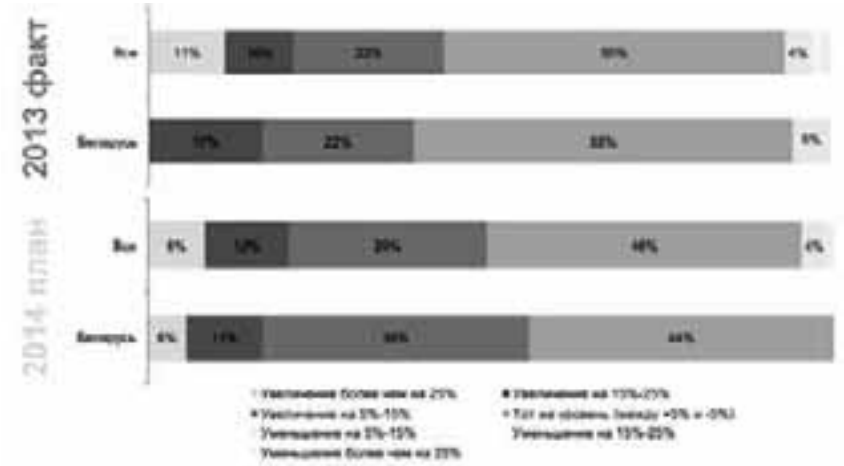


Рис. 2. Динамика бюджета на информационную безопасность

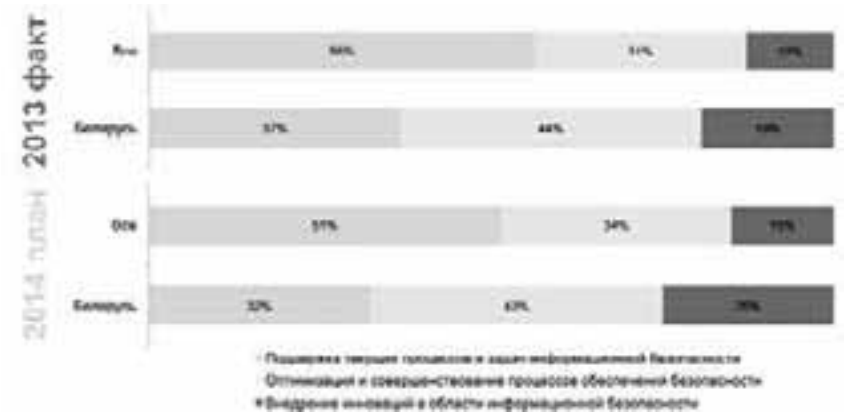


Рис. 3. Структура затрат на информационную безопасность

Рис. 4. Основные приоритеты деятельности в области ИБ (сокращено до 12 из 21 направлений)

проще осознать, что обеспечение физической безопасности при таких обстоятельствах ежегодно будет обходиться все дороже и дороже. Но, поскольку сфера информационной безопасности связана с нематериальными сущностями (электронные данные, программное обеспечение, время и возможность выполнения операций), зачастую сложно понять необходимость ежегодного увеличения затрат на обеспечение информационной безопасности. Рост бюджетов на обеспечение ИБ – общемировая тенденция, которая обусловлена современными реалиями.

В то время, как во всем мире большая часть затрат на ИБ связана с поддержкой существующих процессов, организации в Беларуси находятся на этапе внедрения и совершенствования этих процессов, поэтому вынуждены расходовать большую часть бюджета именно на это (Рисунок 3). Следует отметить, что организации в Беларуси в 2014 году планируют еще больше сконцентрироваться на инновациях.

Основные приоритеты деятельности в области информационной безопасности, по мнению респондентов из РБ (Рисунок 4), – это обеспечение непрерывности деятельности, обнаружение утечек данных, управление доступом к информационным системам и реагирование на инциденты безопасности. Один из важных приоритетов деятельности организаций в Беларуси связан с наймом специалистов по ИБ, хотя во всем мире данному направлению деятельности уделено гораздо меньше внимания. Очевидно, это вызвано недостатком ИТ- и ИБ-специалистов на рынке труда в последние годы. Также мы хотели бы отметить, что организации в Беларуси не осознают необходимость в глубокой реструктуризации функции ИБ: ни один из респондентов не указал в приоритетах деятельности данное направление, хотя подходы к обеспечению ИБ значительно изменились за последние годы и для реализации эффективных мер по данному направлению требуются существенные изменения.

В Беларуси подразделения ИБ подчиняются почти в половине случаев напрямую первому лицу организации (Рисунок 5), в отличие от общемировой практики, где подразделения ИБ либо входят в Службу ИТ, либо напрямую подчиняются Директору по ИТ. При этом, в каждой пятой

организации служба ИБ подчинена операционному или финансовому директору.

Две из трех организаций в Беларуси считают, что их стратегия ИБ не отражает актуальные риски, при этом очень редко стратегия ИБ учитывает риск-аппетит и допустимые уровни риска для организации (Рисунок 6).

Самыми популярными в Беларуси являются такие стандарты и методологии как ISO/IEC 27001 и 27002, ITIL и COBIT (Рисунок 7). Однако на практике заявления об использовании перечисленных документов являются скорее декларативными: зрелость процессов управления информационной безопасностью в большинстве организаций является недостаточной, а сертификации по данным стандартам белорусскими организациями выполняются очень редко, в единичных случаях.

Только 6% респондентов в Беларуси считают, что службы ИБ полностью удовлетворяют потребностям организации, а улучшения все еще на подходе (Рисунок 8).

Основными препятствиями респонденты из Беларуси считают недостаточное финансирование ИБ и нехватку квалифицированных кадров (Рисунок 9). При этом отсутствие поддержки со стороны высшего руководства не является столь значимой проблемой, в отличие от участников исследования со всего мира.

Только у 22% процентов организаций в Беларуси есть формализованная программа выявления уязвимостей, которая включает в себя моделирование сложных атак и системную работу над корректирующими мероприятиями (Рисунок 10).

44% организаций в Беларуси либо не тестируют безопасность собственных информационных систем вообще, либо тестируют очень небольшой процент таких систем, несмотря на то, что эти системы взаимодействуют с сетью Интернет (Рисунок 11). Проактивный подход к выявлению уязвимостей в используемых информационных системах позволяет организациям обнаруживать проблемы и устранять их раньше, чем эти проблемы приведут к инцидентам ИБ. Однако когда процесс не формализован (т.е. руководство не требует и не контролирует исполнение необходимых процедур и подходов от служб ИБ), этот процесс может выполняться от случая к случаю, или не выполнятся вообще.

Рис. 5. Подчинение подразделений, ответственных за ИБ

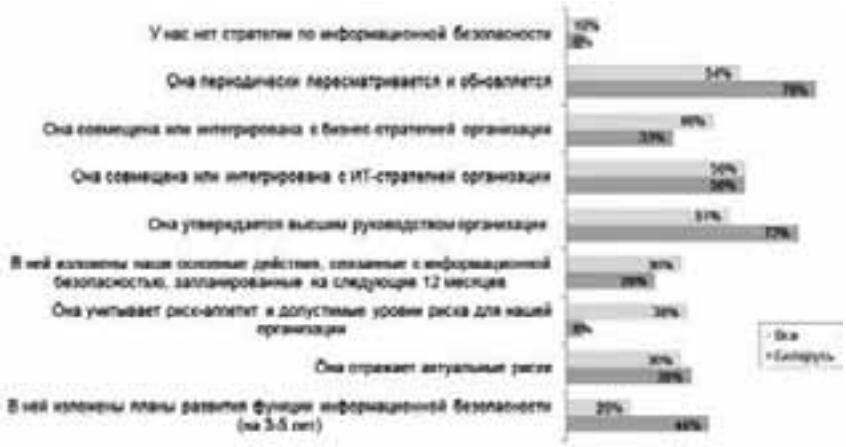


Рис. 6. Характеристики стратегии ИБ

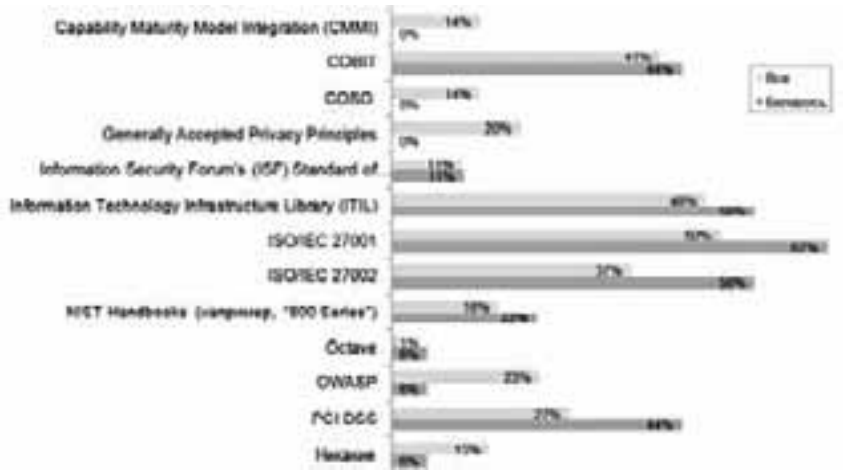


Рис. 7. Использование ведущих практик

Рис. 8. Соответствие службы ИБ потребностям организаций

Рис. 9. Основные препятствия эффективной работе службы ИБ

Рис. 10. Характеристики программы выявления уязвимостей

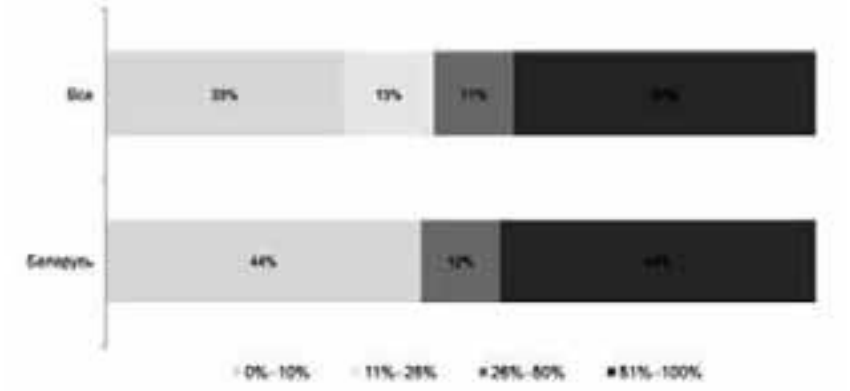


Рис. 11. Сколько систем, взаимодействующих с Интернетом, тестируется ежегодно

Рис. 12. Баланс между усилиями на обеспечение ИБ и их эффектом

Наши рекомендации: поиск баланса между усилиями на обеспечение ИБ и их эффектом

Только сбалансированный подход по приоритезации инвестиций в безопасность, основанный на понимании целей и задач бизнеса, будет способствовать успеху организации, и в то же время обеспечит необходимые действия по защите организации (Рисунок 12).

Высшему руководству организаций следует задать своим службам информационной безопасности следующие вопросы:

1. Насколько хорошо вы понимаете бизнес-стратегию организации?
2. Как инициативы в области обеспечения информационной безопасности поддерживают реализацию бизнес-стратегии?
3. Какие пробелы в данный момент существуют в вопросах обеспечения ИБ?
4. Как развиваются подходы к обеспечению ИБ, чтобы соответствовать динамично изменяющимся рискам?

Ключевые задачи для специалистов ИБ

- Поднимите вопросы информационной безопасности на уровень высшего руководства, сделав их более заметными в компании с помощью четкой стратегии обеспечения безопасности, которая не просто защитит бизнес, но и обеспечит необходимое соответствие функции информационной безопасности потребностям бизнеса.
- Выявите актуальные и реальные риски информационной безопасности для вашей организации, защитите, в первую очередь, наиболее ценное, непрерывно обеспечивайте эффективность процессов ИБ и их результативность.
- Выработайте структурированный и прагматичный подход к управлению рисками. Мы считаем, что интегрированный подход к управлению предприятием, рисками и соответствием нормативным требованиям (Governance, Risk management, and Compliance – GRC) может стать ключевой инвестицией для многих организаций.
- Сделайте информационную безопасность неотъемлемой частью работы организации и образом повседневного мышления каждого сотрудника.

www.ey.com/belarus

Опубликовано в издании «Банковский вестник» № 1/606 январь 2014. ■

Нормативно-правовое регулирование обеспечения национальной безопасности в информационной сфере – изменения и направления развития

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

Справка ТБ

Барановский Олег Константинович, образование высшее, радиофизик, в 1998 году 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.

Согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. №575, в информационной сфере устанавливаются два ключевых объекта защиты информации:

- критически важные объекты информатизации (далее – КВОИ);
- информационные системы (далее – ИС) обеспечения государственного управления в различных областях.

Результаты работ по совершенствованию нормативной правовой базы обеспечения информационной безопасности в 2013-2014 гг. реализованы в двух документах:

- Указ Президента Республики Беларусь от 16 апреля 2013 г. №196 «О некоторых мерах по совершенствованию защиты информации»;
- постановление Совета Министров Республики Беларусь от 15.05.2013 г. №375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)».

Указ №196 определяет порядок осуществления технической и криптографической защиты информации с учетом типа объекта защиты.

Во исполнение требований Указа №196 введен в действие ряд положений приказами Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) от 26 августа 2013 г. №60 и от 30 августа 2013 г. №62:

- Положение о порядке проведения государственной экспертизы средств технической и криптографической защиты информации;
- Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;
- Положение о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации;
- Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Таким образом, с 19 октября 2013 года введены новые требования защиты информации для:

- КВОИ;
- объектов информатизации, предназначенных для обработки государственных секретов;
- государственных ИС;
- ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (за исключением государственных секретов).

Приказом ОАЦ от 17 июля 2013 г. №47 «Об утверждении технического кодекса установившейся практики» введен в действие ТКП 483-2013 (01019) «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования». ТКП устанавливает обязательный перечень мероприятий по созданию системы безопасности КВОИ. В настоящее время проходит апробацию пакет предварительных стандартов Республики Беларусь, содержащих профили защиты для типовых объектов и методические рекомендации по разработке задания по безопасности.

1 января 2014 года вступает в действие технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (далее – ТР). ТР устанавливает обязательные требования информационной безопасности и процедуры подтверждения их соответствия для средств защиты информации. Подтверждению соответствия в форме сертификации подлежат средства защиты информации, которые будут использоваться для:

- технической защиты государственных секретов;
- создания систем защиты информации ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;
- создания систем безопасности КВОИ;
- обеспечения целостности и подлинности электронных документов в государственных ИС.

Соответствие средств защиты ин-

Продолжение на стр. 27 →

Центры реагирования на компьютерные инциденты в системе практической защиты национального сегмента сети интернет

Матвеев А.А., и.о. начальника Национального центра реагирования на компьютерные инциденты CERT.BY

Информационно-коммуникационные системы стали одним из существенных и основных факторов экономического и социального развития. Компьютеры и компьютерные сети используются в настоящее время столь же повсеместно, как электричество или водоснабжение.

Безопасность коммуникационных сетей и информационных систем, особенно их работоспособность и отказоустойчивость, стала крайне актуальной темой для нынешнего общества. Эта тревога объясняется риском появления проблем в ключевых информационных системах, которые могут возникнуть из-за их сложности, склонности к авариям и ошибкам, а также из-за атак на инфраструктуры, предоставляющие критические сервисы для большинства граждан.

Первая крупная вспышка компьютерного червя в глобальной IT-инфраструктуре произошла в конце 80-х годов. Компьютерного червя прозвали «Моррисом» и распространялся он молниеносно, эффективно заражая огромное количество информационных систем по всему миру.

Этот инцидент подействовал на общество как сигнал тревоги, после которого люди внезапно осознали сильную потребность в кооперации и координации совместных действий между системными администраторами и IT-менеджерами для дальнейшей борьбы с подобными инцидентами. Учитывая тот факт, что время простоя является основным критическим фактором в данной ситуации, необходимо иметь более организованный и структурированный подход к процессу обработки инцидентов компьютерной безопасности. Несколько дней спустя «инцидента Морриса» Агентство передовых оборонных исследовательских проектов (DARPA) создало первую CSIRT – CERT/CC [1], располагавшуюся в университете Carnegie Mellon в Питтсбурге (Пенсильвания).

Эта модель вскоре была адаптирована в Европе, и в 1992 году датский академический провайдер SURFnet создал первую CSIRT в Европе под названием SURFnet – CSIRT [2].

Со временем группы CERT расширили свой потенциал от всего лишь простых откликов на инциденты до предоставления полного списка сервисов безопасности, включая предупредительные сервисы, такие как предупреждения, рекомендации по безопасности, тренинги и управление системами безопасности. Термин «CERT» вскоре стал считаться недостаточным.

В результате, в конце 90-х годов был принят новый термин «CSIRT». В настоящее время оба термина (CERT и CSIRT) используются как синонимы, однако CSIRT является более точным термином.

Термином CISRT называется группа экспертов в области IT-безопасности, чья основная обязанность реагировать на инциденты компьютерной безопасности. Эти группы также предоставляют необходимые сервисы для обработки инцидентов и поддержки своих клиентов в процессе восстановления после обнаружения уязвимостей в системах безопасности.

Основными задачами указанных центров являются:

- координация действий подразделений компьютерной безопасности государственных органов, операторов связи, а также других субъектов национальной информационной инфраструктуры по вопросам предотвращения правонарушений в области использования компьютерных и информационных технологий;
- сбор, анализ и накопление в соответствующих базах данных информации о современных угрозах компьютерной безопасности, получаемой от пользователей, производителей компьютерной техники и программного обеспечения, аналогичных зарубежных структур, а также материалов по конкретным компьютерным инцидентам, эффективности применяемых программно-технических средств защиты компьютерных систем;
- технический мониторинг и выявление механизмов и ресурсов сети Интернет, функционирующих в нарушение нормативных правовых актов, регулирующих деятельность участников национального сегмента сети Интернет;
- выработка рекомендаций национальным пользователям сети Интернет по обеспечению защиты интересов личности, общества и государства в информационной сфере, применению наиболее эффективных программно-аппаратных средств, направленных на предотвращение актов незаконного проникновения в информационные системы на основе изучения и обобщения международного опыта обеспечения компьютерной безопасности, оказание консультативных услуг и технической поддержки национальным пользователям;
- оперативный приём сообщений и оказание экстренной помощи по пресечению хакерских атак компьютерных систем, своевременное оповещение национальных пользователей сети Интернет и других информационных систем, в том числе локальных и корпоративных, о возникающих угрозах компьютерной безопасности.

Вопросы кибербезопасности в Республике Беларусь обрели стратегическое значение и заняли прочное место в системе предотвращения угроз национальной безопасности. С этой целью в государстве реализуется взаимоувязанная система правовых, технических и организационных мер, направленных на противодействие угрозам информационной безопасности.

Одним из практических шагов по защите информационных систем явилось решение о создании Национального центра реагирования на компьютерные инциденты CERT.BY.

27 сентября CERT.BY вступил в международное сообщество команд реагирования на инциденты безопасности FIRST. В настоящий момент FIRST насчитывает более 200 стран-участников из Европейского Союза, Азиатско-Тихоокеанского региона, США, Канады, Австралии и СНГ. Процедура присвоения подобного статуса достаточно сложна и требует от выдвигаемого CERT в члены FIRST исполнения ряда требований по оперативности реагирования, безопасности учета поступающих заявок и информации об инцидентах, методам ее хранения и обработки, наличия квалифицированного и профессионального штата для расследования инцидента, а также поручительства со стороны других членов [3].

Основная задача Национального центра реагирования на компьютерные инциденты Республики Беларусь – снижение уровня угроз информационной безопасности национального сегмента сети Интернет. CERT.BY осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Беларуси, а также реагирование на сами инциденты, как в информационных системах государственных органов и организаций, так и у самостоятельно обратившихся субъектов национального сегмента сети Интернет. Учитывая то, что CERT.BY входит в международное сообщество команд реагирования на инциденты безопасности FIRST, он осуществляет взаимодействие с большинством таких же команд реагирования CERT/CSIRT, антивирусными компаниями и может напрямую координировать с ними действия, связанные с инцидентами информационной безопасности.

Примером такой работы может служить результаты взаимодействия с «Лабораторией Касперского» по расследованию функционирования международной кибершпионской сети «Красный октябрь», атаки из которой были направлены на информационные системы, содержащие информацию о научно-технических разработках, анализе экономической деятельности, сферах государственного управления и банковского сектора [4].

Результаты анализа подобного рода инцидентов указывают на то, что сегодня на смену идее массового заражения приходит концепция точечного удара. При этом уровень технологий целевых атак значительно повысился, от них не защищена, по сути, ни одна компания, ни одно государственное учреждение.

Несмотря на это, CERT.BY осуществляет технические мероприятия по противодействию различного рода угрозам, разрабатывает собственные системы анализа и защиты в государственных органах и организациях, а также у иных защищаемых субъектов. Данные системы осуществляют анализ всего жизненного цикла исследуемых угроз, в том числе, способы заражения, методы обновления, признаки угрозы и её выявления. Данная информация передается защищаемым субъектам для противодействия выявленным угрозам.

Таким образом, система обеспечения безопасности информационных систем и ресурсов предполагает участие всех субъектов в данной работе. ■

Список источников

1. http://www.cert.org.
2. http://www.cert.surfnet.nl.
3. http://www.first.org.
4. http://it.tut.by/330356.

← *Начало на стр. 25*

Нормативно-правовое регулирование обеспечения национальной безопасности в информационной сфере – изменения и направления развития

формации ТР обеспечивается выполнением требований информационной безопасности ТР непосредственно, либо выполнением требований, взаимосвязанных государственных стандартов, определенных приказом ОАЦ от 17 декабря 2013 г. №94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY».

Одновременно, в 2014-2015 гг. планируется ввести ряд отечественных и гармонизированных международных стандартов, определяющих требования и рекомендации по обеспечению информационной безопасности и устанавливающих требования защиты информации. ■

Безопасность банковско-финансовой сферы. Актуальность выработки методик и ознакомления с технологиями расследования инцидентов в системах электронных платежей

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

Говоря о значимых событиях, мероприятиях, решениях на уровне государственных регуляторов в 2013 году следует обозначить следующие:

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

- 11 апреля 2013 г. принято решение о создании Комитета по безналичным расчетам, в рамках деятельности которого рассматриваются вопросы развития системы безналичных расчетов, в том числе обеспечение безопасности безналичных расчетов. Указанный комитет принял решение о создании документа, который введет в Республике Беларусь принцип нулевой ответственности для владельцев банковских карт, который предполагает безусловный возврат банком клиенту украденных с карточки средств;

Банки с введением такой ответственности будут нести прямые финансовые потери, в то время как на сегодняшний день несут потери держатели карт. Банки будут стимулированы проводить расследование таких инцидентов. В свою очередь, принятие такого рода нормативного акта создаст условия для фактов мошенничества со стороны держателей карт, что потребует разработки методик работы с такого рода правонарушениями. Для стабильной работы банковской системы и доверия населения к ней необходимо обеспечивать защиту денежных средств и информации клиентов (держателей карт);

- 27 марта 2012 г. ООО «АэркомБел» организовало семинар «Расследование инцидентов информационной безопасности в системах электронных платежей», ставший знаковым в данном направлении для Республики Беларусь, так как на этом мероприятии эксперты из Российской Федерации и Республики Беларусь впервые подняли пласт такой проблематики для белорусских банков и иных организаций;

- 2–3 декабря 2013 г. состоялась 1-ая Национальная выставка-форум «Центр безопасности: Информационная безопасность. Телекоммуникации», создав национальную площадку для обсуждения актуальных вопросов обеспечения информационной безопасности, презентаций инновационных решений, повышения профессиональной квалификации специалистов. Перед слушателями выступили более 40 докладчиков, приняли участие более 30 участников со стендами в экспозиции. География участников была представлена Республикой Беларусь, Россией, Украиной, Литвой и США.

В 2014 году продолжится работа по совершенствованию безопасности безналичных расчетов, систем электронных платежей.

Необходимо совершенствовать эффективность взаимодействия с правоохранительными органами, применение в практике Свода рекомендаций рабочей группы по противодействию мошенничеству в области электронных платежей, повышать компетенцию в расследовании инцидентов, прорабатывать аспекты внедрения принципа нулевой ответственности.

В свете увеличения показателей доли безналичного денежного оборота международные платежные системы со значительным ростом количества операций в стране могут более жестко отнестись к соответствию белорусских участников платежных систем стандарту PCI DSS.

Требования стандарта PCI DSS распространяются на банки, организации торговли и сервиса (ОТС), поставщиков технологических услуг и другие организации, деятельность которых связана с обработкой, передачей и хранением данных о держателях платежных карт.

В 2014 году ООО «АэркомБел» совместно с Национальным банком планирует проведение специализированных мероприятий на тематику расследования инцидентов информационной безопасности в системах электронных платежей с привлечением представителей государственных регуляторов, экспертов из банковской сферы, правоохранительных органов, аудиторских организаций, представителей международных платежных систем, а также экспертов зарубежных компаний, имеющих опыт деятельности по указанной тематике.

Продолжится деятельность информационной площадки Национальной выставки-форума «Центр безопасности: Информационная безопасность. Телекоммуникации».

Принимаемые решения и проводимые мероприятия, безусловно, способствуют повышению безопасности систем электронных платежей и безналичных расчетов в Республике Беларусь, повышению доверия населения к банковской системе.

www.nbrb.by

Роль судебной экспертизы в возврате клиенту похищенных денежных средств

Суханов Максим Андреевич, специалист отдела расследований инцидентов информационной безопасности компании Group-IB (ООО «Группа информационной безопасности»)

Справка ТБ

Суханов Максим, обладает обширным опытом в области реагирования на инциденты в системах ДБО и проведения соответствующих криминалистических исследований компьютерной информации. Участник российских и международных проектов, посвященных судебным компьютерным экспертизам («Компьютерно-техническая экспертиза», «ForensicsWiki» и др.).

Принцип нулевой «ответственности»[1], реализованный вступившими в силу 1 января 2014 года нормами статьи 9 ФЗ «О национальной платежной системе», закрепляет обязанность оператора по переводу денежных средств (которым может выступать банк или небанковская кредитная организация) возмещать клиенту сумму похищенных с использованием электронного средства платежа денежных средств, при наступлении определенных условий. Анализ норм статьи 9 указанного федерального закона (ФЗ РФ) позволяет составить следующую схему условий возмещения клиенту похищенных у него денежных средств со стороны оператора по переводу денежных средств (в первом приближении):

1. Если оператор по переводу денежных средств исполняет обязанность по информированию клиента о совершенных операциях:

- безусловное возмещение клиенту денежных средств, переведенных без его согласия **после** *получения* оператором по переводу денежных средств уведомления клиента об утрате или о несанкционированном использовании электронного средства платежа (часть 12 статьи 9 обсуждаемого федерального закона);
- возмещение клиенту (физическому лицу) денежных средств, переведенных без его согласия **до** *направления* оператору по переводу денежных средств уведомления клиента об утрате или о несанкционированном использовании электронного средства платежа, при условии, что оператор по переводу денежных средств не докажет, что клиент нарушил правила использования электронного средства платежа (часть 15 статьи 9).

2. Если оператор по переводу денежных средств не исполняет обязанность по информированию клиента о совершенных операциях:

- безусловное возмещение денежных средств, о переводе которых клиент не был проинформирован, и которые были переведены без его согласия (часть 13 статьи 9).

Дальнейший анализ правовых норм ФЗ РФ «О национальной платежной системе» обременяет вышеописанную схему дополнительными условиями:

1. информирование клиента о совершенных операциях осуществляется способом, предусмотренным договором между оператором по переводу денежных средств и клиентом (часть 4 статьи 9);
2. уведомление клиента об утере или о несанкционированном использовании электронного средства платежа передается оператору по переводу денежных средств в форме, предусмотренной названным договором (часть 11 статьи 9);
3. этим же договором определяется порядок использования клиентом электронного средства платежа (части 1 и 3 статьи 9), который может содержать требования информационной безопасности;
4. уведомление клиента об утере или о несанкционированном использовании электронного средства платежа передается оператору по переводу денежных средств незамедлительно после наступления соответствующего события, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции. В случае несвоевременной реакции клиента, выходящей за указанные временные рамки, оператор по переводу денежных средств освобождается от обязанности возместить похищенные за пределами указанных временных рамок денежные средства (часть 14 статьи 9);
5. оператор по переводу денежных средств не возмещает клиенту (физическому лицу) электронные денежные средства, похищенные **до** *направления* соответствующего уведомления клиента, если электронное средство платежа является «не персонифицированным» (т.е., в случае, если клиент не был идентифицирован – в терминах законодательства о противодействии отмыванию доходов и финансированию терроризма; см. часть 16 статьи 9).

Одновременно необходимо учитывать следующие обстоятельства:

1. вышеописанный порядок возмещения клиенту похищенных денежных средств распространятся не только на случаи использования банковских карт, но и на случаи использования систем интернет-банкинга (поскольку система интернет-

1 Строго говоря, юридическую ответственность за хищение денежных средств несет правонарушитель, а не кредитная организация или ее клиент, поэтому истинный принцип нулевой ответственности клиента (без кавычек) существует в праве уже очень давно.

банкинга является электронным средством платежа в терминах ФЗ «О национальной платежной системе» – пункт 19 статьи 3);

2. вышеописанный порядок возмещения клиенту похищенных денежных средств распространяется и на случаи хищений электронных денежных средств (за уже названным исключением для «неперсонифицированных»[2] (анонимных) электронных средств платежа; связь норм, определяющих порядок использования электронного средства платежа для перевода электронных денежных средств – статья 10, и норм, определяющих порядок использования электронного средства платежа в целом – статья 9, как частного и общего подтверждается частью 15 статьи 9);

3. оператор по переводу денежных средств вправе приостановить или прекратить использование клиентом электронного средства платежа по собственной инициативе при нарушении клиентом порядка использования электронного средства платежа (часть 9 статьи 9);

4. искусственное усложнение или затягивание процедур взаимодействия клиента с оператором по переводу денежных средств, если это влечет возникновение формального основания для отказа от возмещения оператором по переводу денежных средств похищенных у клиента денежных средств, не может считаться законным, даже если соответствующий усложненный или затянутый порядок прямо предусмотрен заключенным договором присоединения (пункт 2 статьи 428 ГК РФ; см. также Постановление Конституционного Суда РФ от 23 февраля 1999 г. №4-П, вынесенное в отношении схожего способа умаления прав граждан при заключении договора срочного банковского вклада).

Все вышеописанное в определенной степени закрепляет дополнительные меры защиты клиента банка или небанковской кредитной организации в условиях массовых хищений денежных средств злоумышленниками. Но, в то же время, обязанность банка или небанковской кредитной организации возмещать похищенные у клиента денежные средства создает существенный риск мошенничества со стороны клиента – когда последний делает заведомо ложное заявление о совершении несанкционированной операции и получает соответствующее возмещение. Поскольку информирование клиентов о совершенных операциях является обязанностью оператора по переводу денежных средств, которая может исполняться с минимальными затратами (путем направления СМС-уведомлений или даже путем размещения соответствующей информации об операциях на страницах сайта в сети Интернет, доступных клиенту после авторизации), то наибольший риск для кредитных организаций представляют потенциальные мошеннические действия клиентов (физических лиц), направленные на получение компенсации по операциям, совершенным **до** *направления* клиентом уведомления об утрате или о несанкционированном использовании электронного средства платежа. Компенсации по операциям, совершенным **после** *получения* от клиента указанного уведомления, не представляют существенного риска, если кредитная организация своевременно обрабатывает поступающие уведомления клиентов и без промедлений блокирует использование скомпрометированных электронных средств платежа.

Как можно противодействовать мошенническим действиям клиентов, направленным на незаконное получение компенсаций по заведомо ложным сообщениям о фактах хищений денежных средств? Если рассуждать не о банковских картах, а о системах интернет-банкинга, то следы хищения (если оно действительно имело место) следует искать в трех местах:

- на компьютере клиента;
- у интернет-провайдера клиента;
- на серверах банка (более подробная информация об этом была представлена в моей предыдущей статье для журнала «Технологии безопасности» – см. №2 (29) за 2013 год).

С криминалистической точки зрения, наиболее ценные и наиболее однозначные сведения представлены на компьютере клиента, а сведения, хранимые на стороне интернет-провайдера клиента или банка, носят, за редким исключением, ориентирующий характер.

Следовательно, единственным способом, которым кредитная организация может достоверно подтвердить факт хищения денежных средств у клиента, а равно доказать факт нарушения клиентом правил использования электронного средства платежа (что автоматически освобождает кредитную организацию от обязанности возмещения похищенных денежных средств), является исследование содержимого носителей информации компьютера клиента. Но на каком основании можно проводить такое исследование? Если конфликт между кредитной организацией и клиентом был доведен до суда, то таким основанием будут процессуальные нормы, регулирующие назначение и производство судебной экспертизы. А в рамках досудебного разрешения конфликтов таким основанием может служить договор между кредитной организацией, действующей в качестве оператора по переводу денежных средств, и клиентом. При этом результаты внесудебного исследования, проведенного на основании гражданско-правового договора, не могут быть использованы в рамках судопроизводства в качестве заключения судебного эксперта. Т.е., даже при наличии документа, содержащего результаты исследования компьютера клиента на предмет выявления обстоятельств хищения денежных средств, суд будет вынужден назначить аналогичное по своему техническому содержанию процессуальное исследование – судебную экспертизу. До недавнего времени аналогичная ситуация имела место в рамках уголовного судопроизводства – когда назначение и производство судебной экспертизы были возможны только после возбуждения уголовного дела, а результаты исследований, проведенных в рамках проверки сообщения о преступлении – до возбуждения уголовного дела. Необходимо было впоследствии, после возбуждения уголовного дела, воспроизвести судебную экспертизу. Указанное обстоятельство является недостатком действующего процессуального законодательства в области судебной экспертизы, который, в некоторой степени, усложнит и затянет судебное разбирательство по потенциальным фактам мошенничества клиентов, связанным с возмещением якобы похищенных у них денежных средств, а также приведет к увеличению процессуальных издержек, связанных с производством судебных экспертиз.

Некоторые ученые предлагают устранить названный недостаток путем законодательного признания результатов непроцессуального

2 Важно помнить, что слово «персонификация» в русском языке обозначает олицетворение (но никак не идентификацию или персонализацию).

исследования равносильными заключению судебного эксперта, если специалист, проводивший такое непроцессуальное исследование, подтвердит достоверность своего заключения в суде. Суд, в свою очередь, предупредит специалиста об ответственности за представление заведомо ложного заключения (по аналогии с ответственностью за дачу заведомо ложного заключения).

Важно заметить, что модернизировать целесообразно не только законодательство, но и средства судебной экспертизы. Наибольшую опасность представляют, как было сказано ранее, заведомо ложные сообщения о несанкционированных операциях от клиентов (физических лиц), а компьютеры физических лиц обычно содержат большое количество информации, относящейся к личной и семейной тайне, охраняемой Конституцией РФ. Трудно представить, что весь объем личной информации физического лица может быть передан постороннему специалисту для проведения исследования под страхом невозмещения похищенных денежных средств. Поэтому для поддержания баланса законных интересов кредитной организации и прав физического лица необходимо разработать и внедрить такие методы и средства исследования компьютерных носителей информации, которые позволят сделать юридически значимые выводы о факте хищения денежных средств. В т.ч. включая выводы об использованных вредоносных компьютерных программах и средствах для удаленного (сетевого) управления компьютером, без создания риска несоразмерного вторжения в частную жизнь.

Такими средствами могут быть экспертные программы, производящие исследование компьютерной информации в автоматическом режиме, с минимальным участием специалиста. Без этих программ кредитные организации вряд ли смогут преодолеть риск мошенничества со стороны клиентов, делающих заведомо ложные заявления о хищении денежных средств с использованием электронных средств платежа. Причины – при традиционном, преимущественно ручном подходе к исследованию компьютерной информации соответствующие условия договора присоединения, обязывающие клиента (физическое лицо) предоставлять личный компьютер на исследование посторонним лицам, вполне могут быть признаны обременительными и отменены на основании статьи 428 ГК РФ.

Заключение

1 января 2014 года уже в прошлом, но пока еще рано делать какие-либо принципиальные правоприменительные выводы по вступившим в силу нормам статьи 9 ФЗ РФ «О национальной платежной системе». Автор считает, что постепенно роль судебной экспертизы в возврате клиенту похищенных денежных средств будет возрастать, равно как будет возрастать и роль непроцессуальных (внесудебных) исследований, проводимых банками (или по их заказу) с целью уменьшения риска мошенничества со стороны клиентов. И к этому нужно быть готовым.

www.group-ib.ru
www.letagroup.ru

Банковский сектор лидирует по числу утечек информации в Беларуси

Сфера информационной безопасности в Беларуси в настоящее время находится на стадии активного развития. По мере возрастания количества новостных сообщений об утечках конфиденциальных данных из частных и государственных организаций появляется интерес к технологиям обеспечения защиты корпоративной информации. Настоящий материал был подготовлен аналитическим отделом компании Falcongaze на основе сведений из белорусских средств массовой информации, а также данных, полученных в ходе использования DLP-системы SecureTower в белорусских организациях из различных отраслей и сфер деятельности.

Утечки информации из белорусских организаций в 2013 году:
- персональные данные (53%);
- сведения, представляющие коммерческую тайну (25%);
- конфиденциальные данные, банковская тайна, адвокатская тайна, тайна страхования и врачебная тайна (22%).

По форме собственности:
- частные предприятия (52%);
- государственные предприятия (48%).

Хотя большинство организаций в Беларуси, как и в других странах СНГ, предпочитает, по возможности, не разглашать сведения о произошедшей утечке информации, число таких случаев, которые освещаются в средствах массовой информации, неуклонно возрастает.

Так, в 2013 году сотрудник «Белвнешэкономбанка», как сообщает портал Onliner.By1, по долгу службы имея доступ к компьютерной системе обслуживания банковских карточек, содержащей сведения о клиентах «Белвнешэкономбанка» и банков-партнеров, отобрал счета с крупными суммами и произвел многократное перечисление средств (на общую сумму Br 270 млн.) с них на счета, зарегистрированные в другом банке на подставных лиц.

Широкий общественный резонанс в 2013 году также вызвал случай, связанный с утечкой персональных данных россиян через белорусские Интернет-ресурсы. По сообщениям БелТА1, Оперативно-аналитический центр при Президенте Республики Беларусь оказал помощь Роскомнадзору в остановке утечки личных данных российских граждан через четыре белорусских сайта, которые незаконно распространяли конфиденциальную информацию.

Утечки информации в Беларуси (по данным аналитического отдела компании Falcongaze)

В 2013 году при помощи разработки компании Falcongaze, DLP-системы SecureTower, были выявлены инциденты, связанные с утечкой конфиденциальной корпоративной информации, и, благодаря своевременному реагированию, предотвращено наступление серьезных негативных последствий для целого ряда компаний.

Среди лидирующих по количеству утечек областей – банковский сектор (34%). В пример можно привести случай, когда в короткий срок после внедрения DLP-системы SecureTower в один из белорусских банков сотрудники отдела информационной безопасности зафиксировали утечку персональных данных клиентов финансового учреждения, которые попали в открытый доступ в сети Интернет, что поставило под угрозу репутацию банка и могло повлечь за собой существенные финансовые потери.

В ходе служебного расследования было выявлено, что один из сотрудников учреждения регулярно пересылал персональные данные клиентов на внешний электронный адрес, откуда, как выяснилось, и происходила утечка информации путем распространения данных третьими лицами.

Утечки были зафиксированы и в сфере, где информация фактически имеет основополагающую значимость, – в логистике (27%). Одна из сотрудниц белорусской логистической компании предприняла попытку передачи клиентской базы данных, заархивированной и предварительно сохраненной в несвойственном такому типу информации формате, на электронный адрес сотрудника конкурирующей компании. При помощи SecureTower инцидент был своевременно выявлен, отправка данных пресечена, а специалистам службы информационной безопасности удалось провести оперативное расследование инцидента.

Значительное количество утечек корпоративных данных в 2013 году было выявлено также в сфере розничной торговли (16%). Отличительной особенностью розничных торговых сетей является необходимость ведения активной внутриотраслевой борьбы за поставщиков: так, после внедрения DLP-системы SecureTower в корпоративную сеть крупной компании, специализирующейся на розничной торговле, был выявлен сговор нескольких топ-менеджеров с представителями другой ритейл-корпорации, которым передавалась конфиденциальная информация о сотрудничестве с официальными поставщиками.

Кроме того, инциденты, связанные с утечкой и разглашением конфиденциальных данных, имели место в промышленных, туристических и ИТ-компаниях.

Заключение

Общая картина информационной безопасности в Беларуси в 2013 году в значительной степени отражает мировые тренды: лидирующим типом утечек стали персональные данные, за которыми следует коммерческая информация организаций. В разрезе отраслей по количеству утечек информации по-прежнему лидирует банковский сектор.

Продолжение на стр. 34 →

Троян – как серьезная угроза для электронных банковских систем

Рынок финансовых мошенничеств становится все более организованным, а трояны, нацеленные на электронные банковские системы, все более изощренными. За первые три квартала 2013 г. число финансовых троянов возросло в три раза, и на сегодняшний день они являются одним из самых распространенных типов угроз. Для того чтобы лучше понять масштабы и механизмы работы финансовых троянов, эксперты Symantec проанализировали более 1000 конфигурационных файлов восьми троянских программ, направленных против банковских систем.

Электронные банковские системы – это то место, где сейчас осуществляются все денежные операции, и именно поэтому они привлекают внимание злоумышленников. Не является неожиданностью так же и то, что трояны, нацеленные против электронных банковских систем, становятся все более изощренными. Одним из таких примеров является недавно упомянутый специалистами Symantec троян Neverquest, преемник Trojan.Snifula, который впервые появился еще в 2006 г., однако применяется до сих пор.

В 2007 г. появился продвинутый финансовый троян под названием Zbot (Zeus). Он был создан Российским вирусописателем под ником Slavik/Monstr и продавался на черном рынке за тысячи долларов. Два года спустя у этого трояна появился конкурент под названием Spyeye, автором которого был некий Gribodemon. Цена нового продукта была более доступной и составляла $700. Подпольный рынок финансовых троянов процветал.

С тех пор рынок претерпел значительные изменения: в 2011 г. исходный код Zeus был украден и выложен в открытый доступ, что привело к резкому обвалу его цены. С этого момента начало появляться множество версий Zeus, включая доработанные Ice IX и Citadel, которые стали бороться за рынок. Банды киберпреступников также создали альтернативные варианты Zeus, предназначенные для частного использования, как, например, знаменитый Gameover, который появился в июле 2011 г. Через месяц после публикации исходного кода Zeus некто Xylibox путем взлома получил доступ к исходному коду Spyeye, что привело к аналогичному обвалу цены. На данный момент какая-либо информация о дальнейшей разработке двух этих троянов их создателями отсутствует. Многие нынешние финансовые трояны позаимствовали приемы и архитектуру Spyeye и Zeus.

К маю 2003 г. существовало около 20 различных банковских троянов. И по мере того, как финансовые учреждения укрепляли защиту и системы выявления мошенничеств, злоумышленники приспосабливались. С тех пор появилось множество банковских троянов. К сожалению, внедрение новых, надежных технологий защиты происходит довольно медленно, и злоумышленники успешно пользуются уязвимостями нынешних, пока еще несовершенных механизмов. За последние несколько лет трояны стали значительно более изощренными, и именно финансовые трояны на сегодняшний день являются одним из самых распространенных типов угроз.

За первые девять месяцев 2013 г. число случаев заражения финансовых учреждений увеличилось на 337%. Это почти полмиллиона заражений в месяц. Для того, чтобы лучше понять масштабы и механизмы работы финансовых троянов, эксперты Symantec проанализировали более 1000 конфигурационных файлов восьми троянских программ, направленных против банковских систем. В этих файлах хранится информация об атакуемых URL-адресах, а также о стратегии атаки. Стратегии варьируются от простого перенаправления пользователей до сложных вебинжектов (Web-injects), способных автоматически осуществлять транзакции в фоновом режиме. Проанализированные конфигурационные файлы содержали более 2000 адресов, принадлежащих 1486 организациям-жертвам, из которых почти 95% – финансовые учреждения. Оставшиеся 5% – это компании, предлагающие онлайн-услуги, например СМИ, сайты поиска работы, аукционы и сервисы электронной почты. Это указывает на широкий охват таких троянов: злоумышленники атакуют любые цели, способные принести прибыль. Объектами атак являются финансовые учреждения практически всех типов – от коммерческих банков до кредитных кооперативов. Основной целью злоумышленников являются сайты классических банков, однако, помимо этого, в качестве потенциальных объектов атак рассматриваются и учреждения нового типа. В попытках максимизировать прибыль злоумышленники начинают атаковать популярные и, соответственно, прибыльные сети финансовых транзакций, такие как американская Automated Clearing House, а также европейская Single Euro Payments Area (SEPA), подвергшаяся атаке совсем недавно.

Злоумышленники выходят и на новые рынки, расширяют сферу своей деятельности и ищут новые цели, против которых бы работали существующие приемы. В таких регионах, как Ближний Восток, Африка и Азия, число объектов атак продолжает расти. При этом густонаселенные и богатые районы представляют для них больший интерес, и именно поэтому такие районы, как Саудовская Аравия, Объединенные Арабские Эмираты, Гонконг и Япония, недавно подверглись многочисленным атакам.

Современные финансовые трояны отличаются невероятной гибкостью и поддерживают широкий спектр приемов, помогающих упростить осуществление мошеннических транзакций в различных банковских системах. Такие трояны во многом схожи между собой. Так, например, техника MITB (Man in the Browser, «Человек-в-браузере») характерна для всех рассмотренных экземпляров. Степень же изощренности атаки зависит от уровня защищенности конкретного учреждения – в конечном итоге, выбор трояна зависит от финансовых ресурсов злоумышленника и того, насколько продвинута система защиты атакуемого учреждения.

По данным исследования, наиболее часто атакуемый банк расположен на территории США, и его данные присутствовали в 71,5% всех проанализированных конфигурационных файлов. Другие банки из Топ-15 самых атакуемых были обнаружены более чем в 50% всех конфигурационных файлов. Это значит, что каждый второй троян был нацелен хотя бы на один из этих банков. Вероятно, такой высокий показатель связан с тем, что эти URL выступают в качестве приме-

ров при конфигурировании троянов. Другая причина может состоять в том, что эти трояны все еще работают против этих организаций, т. к. не все фирмы успели обновить свои системы защиты. Конечно, большинство организаций осведомлены об этих угрозах и внедряют новые механизмы защиты, способные блокировать подобные атаки. К сожалению, на внедрение новых технологий требуются время и средства, так что здесь злоумышленники всегда будут обладать преимуществом. В конечном итоге, слабым звеном любой финансовой операции остается пользователь, и даже лучшие технологии не гарантируют защиты от атак, использующих методы социальной инженерии. Можно ожидать, что в ближайшие годы троянские атаки на финансовые учреждения продолжатся.

www.symantec.ru

← *Начало на стр. 32*

Банковский сектор лидирует по числу утечек информации в Беларуси

Ожидается, что в 2014 году тенденции в сфере информационной безопасности на белорусском рынке не претерпят существенных изменений. Число разглашаемых утечек данных из государственных и частных организаций несколько возрастет. Однако можно отметить тот факт, что наблюдаемый в последнее время рост внимания к проблеме защиты данных не только среди профессионалов, но и на уровне управления частными компаниями и государственными организациями, а также в законодательной сфере, с большой вероятностью сохранится и в будущем. Более того, актуальность проблемы заметно возрастет для сферы гостеприимства: в связи с намечающимся в начале 2014 года Чемпионатом мира по хоккею, который будет проходить в Беларуси, повышенное внимание к защите персональных данных ожидается в белорусской туристической отрасли.

Использованные источники:

1. Беларусь остановила утечку в Интернет личных данных россиян. – [Электронный ресурс]. – Режим доступа: http://www.belta.by/ru/all_news/society/Belarus-ostanovila-utechku-v-Internet-lichnyx-dannyx-rossijan_i_635216.html

2. Данные белорусов, обратившихся в МТБанк за услугами, попали в интернет. Банк ведет расследование. – [Электронный ресурс]. – Режим доступа: http://news.tut.by/economics/245339.html

3. Сотрудник «Белвнешэкономбанка» украл со счетов клиентов 270 млн. – [Электронный ресурс]. – Режим доступа: http://people.onliner.by/2013/06/28/ban-2 ■

Три направления стратегии информационной безопасности современного предприятия

Алексей Лукацкий – бизнес-консультант по безопасности Cisco

Справка ТБ

Алексей Лукацкий, окончил Московский институт радиотехники, электроники и автоматики (МИРЭА), специальность «Прикладная математика» (специализация – «Защита информации»). В области ИБ с 1992 года. Работал специалистом по ЗИ в различных государственных и коммерческих организациях. Прошел путь, от программиста средств шифрования и администратора и заканчивая аналитиком и менеджером по развитию бизнеса в области ИБ. Имеет ряд сертификаций в области ИБ. Опубликовал свыше 600 печатных работ в различных изданиях, ведет блог в Интернете «Бизнес без опасности». В 2005 году удостоен награды Ассоциации документальной электросвязи «За развитие инфокоммуникаций в России», а в 2006 – награды Инфофорума в номинации «Публикация года». В январе 2007 года включен в рейтинг 100 персон российского ИТ-рынка. За время работы в Cisco удостоен ряда внутренних наград, в т.ч. и как один из 4 людей года, сделавших многое для внутренней безопасности компании (Security Champion). Является автором множества курсов по ИБ. Участвовал в создании ряда проектов по ИБ, самый известный из которых freescan.ru, позволяющий проверить защищенность своих Интернет-ресурсов.

Так часто складывается, что Cisco в области ИБ выступает одновременно в двух ипостасях – разработчика и поставщика средств защиты информации и информационных систем и корпоративного заказчика решений по информационной безопасности. Причем заказчика очень крупного – 70000 сотрудников, десятки тысяч устройств по всему миру, множество законодательных требований, различные платформы доступа… Наверное именно поэтому мы не просто предлагаем рынку то, что просят потребители, – мы предлагаем то, что нужно и нам самим. И мы, как никто другой, прекрасно осознаем все сложности разработки стратегии ИБ современного предприятия.

Давайте вспомним, с чего начиналась информационная безопасность в мире; когда еще и сетей-то почти не было? С безопасности автономных компьютеров, обменивающихся информацией с помощью дискет. Именно в ту пору возникла концепция защиты ПК, которую активно развивали антивирусные производители, а затем подхватили и другие нишевые игроки. Сегодня, в условиях всепроникающей мобильности, концепция (или направление) защиты оконечных устройств трансформировалась в MDM-рынок (mobile device management). В компании Cisco эту концепцию реализуют сразу несколько решений – антивирус и система защиты ПК и мобильных устройств Sourcefire FireAMP, многофункциональный защитный клиент Cisco AnyConnect и интеграция Cisco ISE с ведущими мировыми решениями MDM (IBM, AirWatch, Good, MobileIron, SAP и т.п.). Но является ли это направление единственно верным? Представьте, что у вас защищаемый информационный актив находится на принтере, камере видеонаблюдения, контроллере АСУ ТП, кардиостимуляторе или ином устройстве, составляющем Интернет вещей? Стратегия защиты оконечных устройств в данном случае будет неэффективной, т.к. на такие устройства нельзя поставить систему защиты. Тут потребуется активное вовлечение в решение задачи сетевой инфраструктуры, которая может не только передавать защищаемые данные или команды, но и контролировать доступ к защищаемой инфраструктуре и устройствам. У Cisco, как лидера рынка сетевых технологий и Интернета вещей, многие защитные механизмы встроены в само сетевое оборудование, что позволяет переложить часть функций ИБ на сеть и снять нагрузку с устройств, исторически трудно защитимых.

Направления защиты

Уже в 90-е годы, в начало расцвета локальных и глобальных сетей, стало понятно, что необходим другой подход к защите, который бы позволял защищать данные в местах их аккумуляции. Так появилось два направления защиты – серверное, переросшая в безопасность центров обработки данных, и периметровое, заключающееся в установке защитных шлюзов, через которые и проходили все данные, требующие защиты и контроля. Оба подхода нашли и до сих пор находят свое отражение в решении Cisco Secure Data Center и Secure Unified Access, включающего традиционные и виртуализированные межсетевые экраны (Cisco ASA 5500-X, Cisco ASA 1000V, Cisco Virtual Security Gateway, Cisco ASA SM, Cisco IOS Firewall и т.п.), системы предотвращения вторжений (Cisco IPS 4300, Cisco IPS 4500, Cisco IPS for ASA, Sourcefire NGIPS и т.д.), системы контентной фильтрации (Cisco Email Security Appliance, Cisco Web Security Appliance) и многие другие решения, ориентированные на защиту ЦОДов и периметра.

Указанные 2 направления (защита оконечных устройств и мест аккумулирования защищаемых данных) долгое время главенствовали в мире. Но с течением времени стали появляться вопросы, на которые эти две стратегии не давали ответов. Как защищать данные в процессе передачи по сети – внутренней или глобальной? Что делать, если данные все-таки утекли из компании? Как защитить миниатюрные устрой-

Продолжение на стр. 37 →

Частное IT Облака за 2 часа – Cisco UCS Director

Виктор Подкорытов, инженер-консультант Cisco Systems

Справка ТБ

Виктор Подкорытов, работает в области информационных технологий с 1995 года, с 2005 года работает в Cisco Systems Ukraine. Области экспертизы: решения для промышленности и энергетики, технологии ЦОД, виртуализации, облачные вычисления.

Облачные вычисления – безальтернативный путь эволюции ИТ. И неважно, развивает компания собственный корпоративный ЦОД или решает задачу перевода своих задач на внешнего провайдер – все это, в конечном итоге, имеет отношение к собирательному термину «облако». Другое дело, что в реальности большинство компаний находятся лишь где-то в начале этого пути. И операторы, и их потенциальные клиенты испытывают сложности, связанные, в первую очередь, с необходимостью меняться организационно, чтобы иметь возможность трансформировать модель ИТ, а с ней и весь бизнес.

На практике мы сталкиваемся с несколькими причинами по которым заказчики хотели бы внедрить облачные сервисы для использования внутри организации:

- Минимизация времени на обработку запросов и максимально быстрое предоставление ресурсов;

- Возможность получения информации под какие задачи используется оборудование, а также его стоимость под каждую из них;

- Сокращение рутинных операций, выполняемых вручную администраторами.

Стоимость и длительность построения облачных систем во многом зависит от подхода – проект (интеграция множества разрозненных продуктов, компонентов облака) или готовый продукт (интегрирующий предопределенное аппаратные и программные компоненты удобные для разворачивания облака). Чем более целостнее решение, тем меньше работ по интеграции между всевозможными модулями необходимо будет выполнить, чтобы все компоненты инфраструктуры были задействованы в сценариях автоматизации.

Cisco UCS Director (UCSD) – самый простой, недорогой, и в то же время многофункциональный продукт на рынке облачных решений. Изначально был разработан как средство автоматизации для инфраструктуры FlexPod, а на сегодняшний день к Cisco и Netapp добавилась поддержка оборудования EMC, Brocade, HP, HDS. Обеспечена интеграция со всеми распространенными гипервизорами: VMWare, Microsoft, Linux KVM и XenDesktop. Также доступна интеграция с облаком Amazon, чтобы в случае нехватки локальных ресурсов можно было задействовать внешние.

Для инсталляции и запуска в эксплуатацию UCS Director не требуется высокая квалификация со стороны администратора. Настройка состоит из нескольких простых шагов, которые необходимо выполнить через интуитивно-понятный графический интерфейс.

В первую очередь системе необходимо предоставить логины и пароли доступа на физическое оборудование и виртуальные среды, которыми Вы хотели бы управлять. Затем вручную или через интеграцию с корпоративным AD определяются группы пользователей, каждой из которых будет доступен свой веб-портал и каталог сервисов. Опционально, но желательно также создать политики стоимости ресурсов, т е задать системе значения сколько стоит CPU, память, дисковое пространство, сетевой трафик. Последним шагом является настройка каталога сервисов. Интересно, что в системе уже предопределено множество сценариев, релевантных для любой организации. Например, создание виртуальной машины

из шаблона или инсталляция нового физического сервера с подключением к инфраструктуре. Кроме того есть возможность описывать свои процессы или менять существующие через удобный графический редактор.

После выполнения этих несложных операций, пользователям предоставляется веб-портал с каталогом сервисов, доступных к заказу и автоматическому исполнению. А для администраторов – полная статистика об использовании ресурсов в организации.

www.cisco.ru

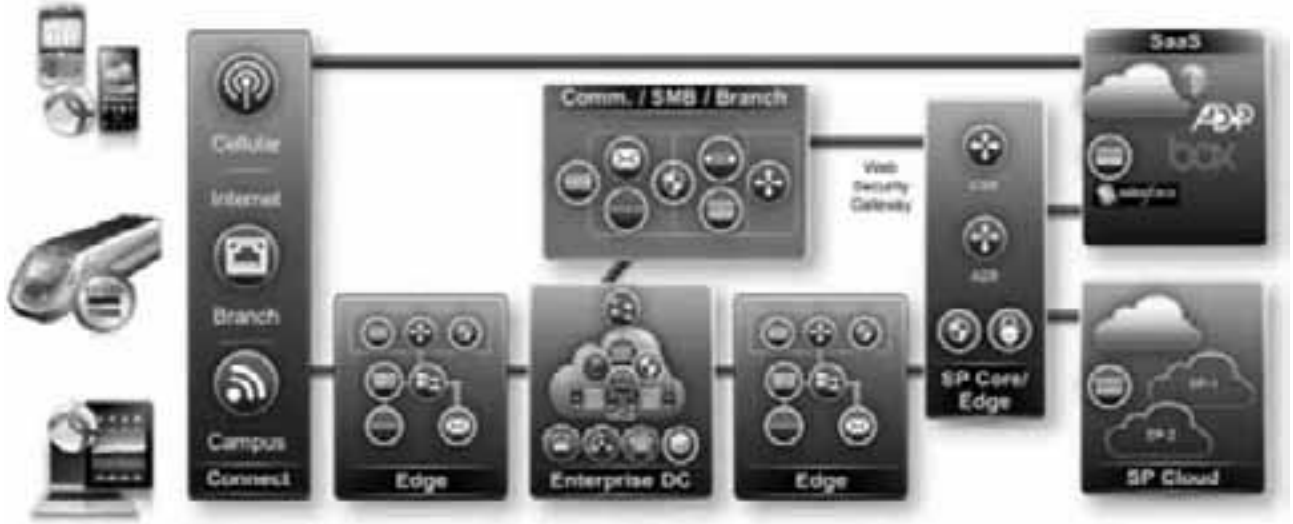
← *Начало на стр. 37*

Три направления стратегии информационной безопасности современного предприятия

ства, составляющие Интернет вещей? Стало формироваться третье направление, которое сейчас, не без помощи Cisco, становится одной из движущих сил современной ИБ. Ведь именно оно позволяет обнаруживать то, что проходит в обход периметра и попадает во внутреннюю сеть. С помощью именно этого направления можно эффективно задействовать потенциал уже построенных, но мало участвующих в защите корпоративных и глобальных сетей. Ярким представителем такого подхода является решение Cisco Cyber Threat Defense (CTD). Именно эта стратегия может дать ответ на вопрос, который возникнет в самое ближайшее время – как защитить SDN (Software Defined Network)? Cisco и тут может предложить ряд решений, как интегрированных в сетевую инфраструктуру (коммутаторы, маршрутизаторы, точки беспроводного доступа и т.п.), так и позволяющих ею эффективно управлять в контексте информационной безопасности (например, с помощью Cisco ISE).

Описанные три направления и составляют костяк стратегии информационной безопасности современного предприятия. Очевидно, что для того, чтобы обеспечить эффективную защиту от современных угроз, которые могут атаковать корпоративные или ведомственные информационные активы, нужно применять комбинацию этих подходов. Только в этом случае можно хоть как-то обезопасить себя от постоянно развивающихся угроз и постоянно меняющих свою тактику нарушителей. И компания Cisco готова помогать в решении этой задачи.

www.cisco.ru



Защищенные микроконтроллеры и модули Inside Secure

Крутиков Александр Олегович, ведущий специалист ООО «Инсайд РУС»

Компания ООО «Инсайд РУС» предлагает своим клиентам на рынках России, Беларуси и Казахстана защищенные микроконтроллеры и модули, созданные на их основе. Отличительной особенностью защищенных микроконтроллеров Inside Secure является комплексное обеспечение хранящихся данных и исполняемых процедур.

Высокий уровень защиты (согласно стандарту EAL level4) в микроконтроллерах Inside Secure достигается благодаря использованию ряда технологических решений:

- проактивный экран, закрывающий микросхему, позволяющий обнаружить нарушение целостности корпуса чипа;
- наличие в микроконтроллере датчиков мониторинга внешней среды (температуры, давления и т.д.).

Данные, получаемые от перечисленных компонентов системы, позволяют своевременно обнаружить несанкционированное воздействие на микроконтроллеры и уничтожить конфиденциальную информацию, тем самым предотвратив ее попадание к злоумышленникам. Также в микроконтроллерах Inside Secure поддерживаются изменяемый случайным образом уровень потребления электроэнергии и запуск «пустых циклов», что делает невозможным несанкционированное получение какой-либо конфиденциальной информации в ходе внешнего мониторинга микроконтроллера.

В микроконтроллерах Inside Secure на аппаратном уровне поддерживаются алгоритмы шифрования DES/TDES, ECC, RSA, AES. Для обеспечения быстрой работы данных алгоритмов в микроконтроллерах Inside Secure присутствует криптоакселератор. Важной особенностью криптоакселератора является обеспечение поддержки математических функций, используемых в перечисленных алгоритмах криптографии, а не самих алгоритмов как единого целого. Благодаря этому, у разработчиков имеется возможность использовать криптоакселератор при создании собственных алгоритмов (например, реализации национальных ГОСТов криптографии).

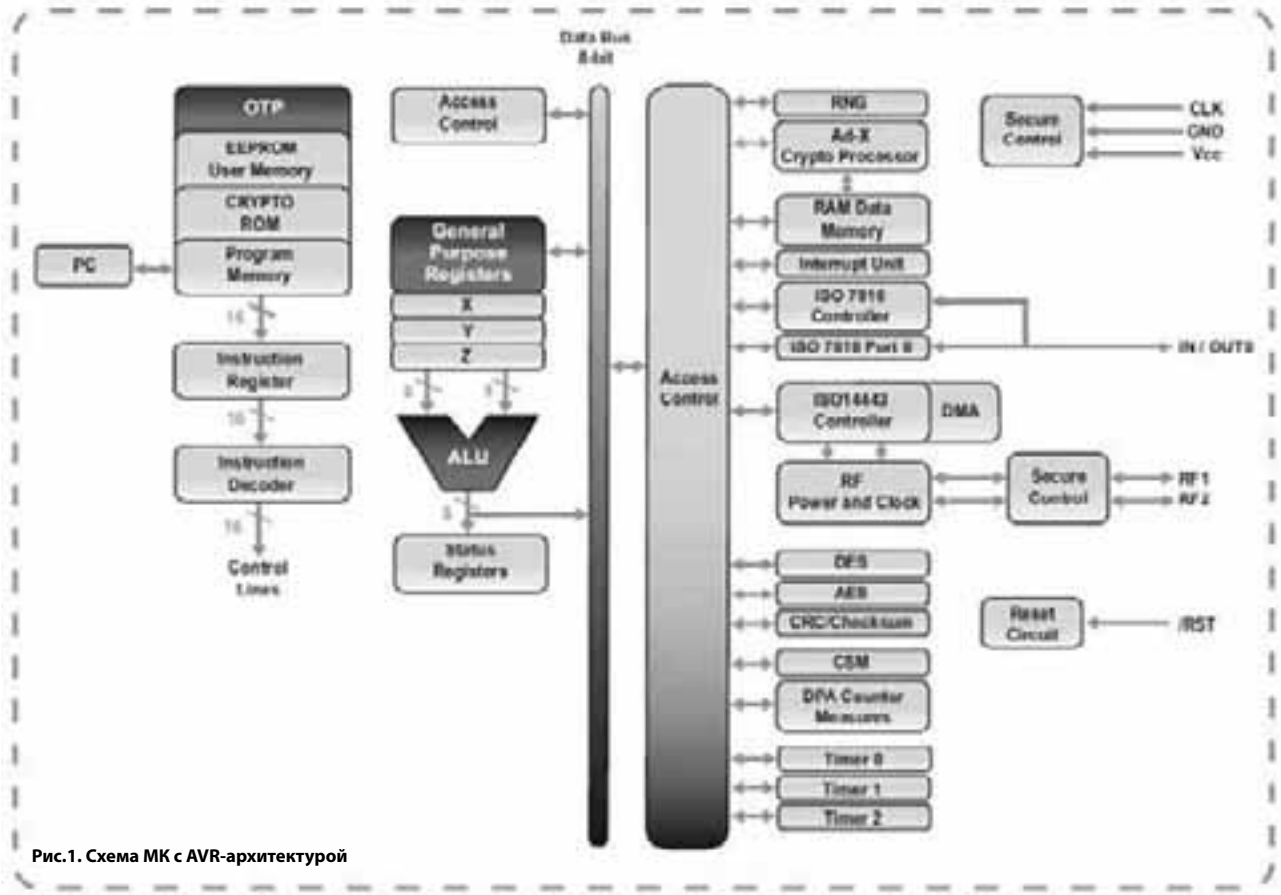


Рис.1. Схема МК с AVR-архитектурой

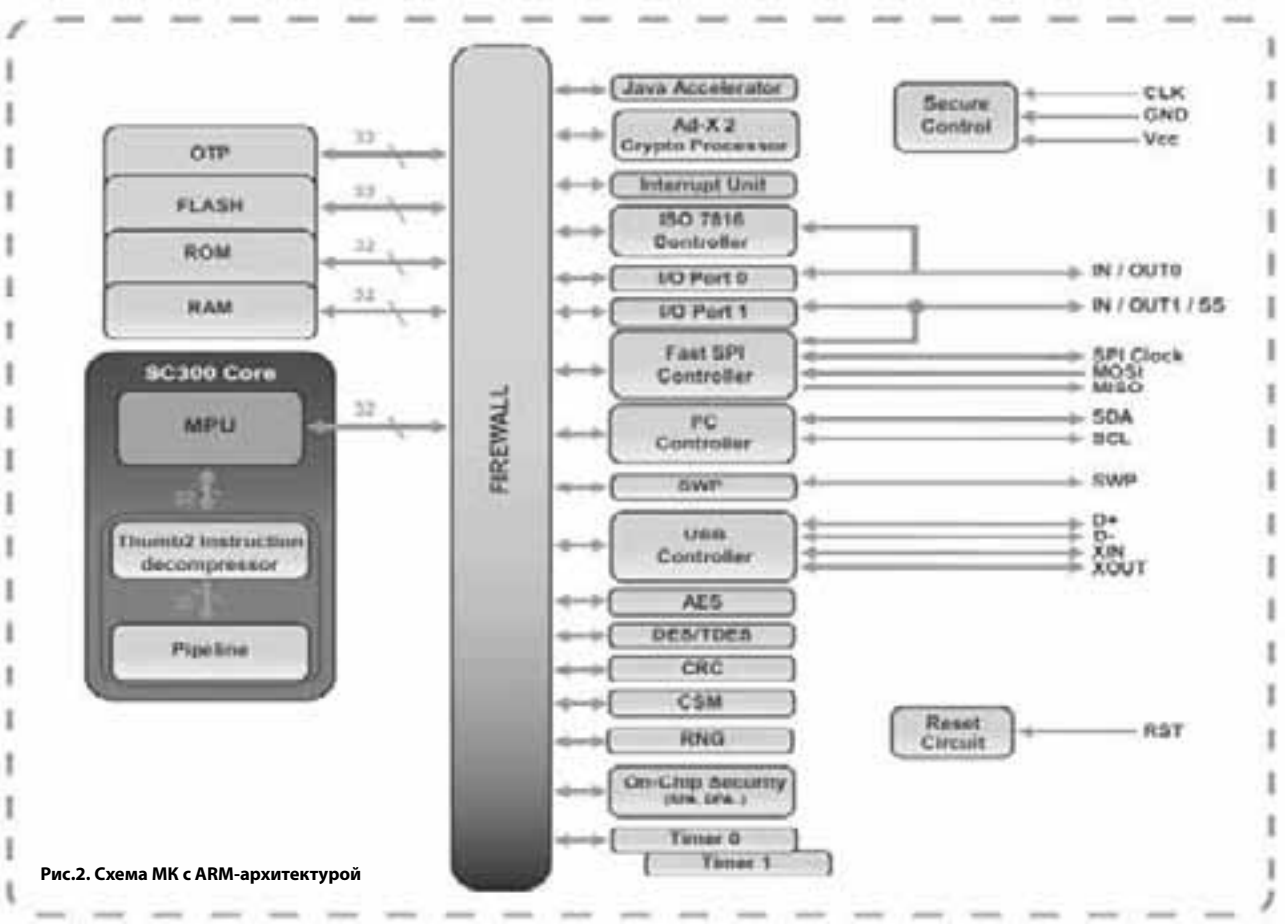


Рис.2. Схема МК с ARM-архитектурой

Также следует отметить, что изделия Inside Secure обладают широким набором интерфейсов: I2C, USB, NFC, ISO7816, SWP, ISO14443, SPI.

Для создания микроконтроллеров используются AVR или ARM архитектуры.

На базе микроконтроллеров, выполненных на базе AVR-архитектуры, компания Inside Secure производит следующие модули:

- **Модули семейства VaultIC.** Защищенные криптомодули для широкого применения. Поставляются с предустановленной операционной системой и файловой системой;

- **Модули семейства MicroPass.** Пре-персонализированные модули для производства банковских карт. Данные модули и апплеты, установленные на них, сертифицированы по стандартам Visa и MasterCard и полностью соответствуют технологическим требованиям производственного оборудования DATACARD.

Микроконтроллеры Inside Secure, сразу после их представления рынку России и Беларуси, вызвали живой интерес разработчиков. Однако есть ряд недостатков, ограничивающих применение данных устройств. А именно, отсутствие реализации национальных криптографических стандартов (согласно ГОСТам России и Беларуси) и отсутствие поддержки JAVA. Данные недостатки будут устранены в 2014 году. В настоящее время ведутся работы по разработке и сертификации микроконтроллеров, поддерживающих национальные криптографические стандарты. Поддержка JAVA планируется к реализации в микроконтроллере MS6001 (ARM-ядро) к лету 2014 года.

www.inside-rus.ru

Новые решения компании «Инсайд РУС»

Использование модулей VaultIP в автономных системах или замена архитектуры ARM TrustZone в мобильных устройствах.

INSIDE Secure, представила новую платформу безопасности для мобильных устройств, которая позволяет надежно защитить их от атак, обеспечивая сохранность и целостность системы. Это инновационное решение VaultIP с оптимизированным энергопотреблением, набором аппаратных IP (встраиваемых)- модулей, соответствующих международным сертификатам по безопасности. Благодаря вышеперечисленным свойствам производители могут использовать VaultIP для быстрого и экономически эффективного внедрения в аппаратную защиту своих устройств, либо использовать его автономно в архитектуре ARM TrustZone ® .

Мобильные устройства с безопасными модулями VaultIP могут защитить данные в банковских операциях, платежных системах проезда, строгой идентификации и безопасности на предприятии, сфере здравоохранения и системах электронного правительства, а также DRM-системах и др.

Реализация данного решения стала возможной благодаря приобретению INSIDE компании ESS (Eurest Support Services), в результате которого достигнуто сочетание экспертных знаний в микропроцессорных технологиях и технологиях обеспечения информационной безопасности. Это позволило INSIDE создать встроенную платформу безопасности, которая обеспечивает целостность программной и аппаратной систем. Модули прошли сертификацию, включая сертификаты EMVCo, GlobalPlatform, FIPS 140-2 и Common Criteria, что позволяет клиентам, использующим VaultIP, быстрее и без дополнительных затрат выйти на рынок и соответствовать всем критериям безопасности. ■

Средства доверенной загрузки

Обеспечение безопасности вычислительной инфраструктуры, обрабатывающей конфиденциальную и секретную информацию, на сегодняшний день приобрело особое значение. Кибертерроризм, появление «вирусов» нового поколения, внедряющихся на уровне BIOS (до старта операционной системы), атаки на системы управления критически важными объектами, разрушение цифровых баз данных из абстрактных угроз превратились в реальность.

Используемые в настоящее время программно-аппаратные средства защиты информации зачастую не могут в полной мере обеспечить безопасность вычислительной инфраструктуры, т.к. их инициализация происходит после запуска операционной системы, когда вредоносный код уже мог быть записан во флэш-память BIOS.

Кроме того, следует отметить, что подавляющее большинство используемых вычислительных систем построено на материнских платах импортного производства. Нельзя исключить возможность наличия в их BIOS незадекларированных возможностей, позволяющих обойти любые установленные на данном устройстве средства зашиты.

В сложившихся условиях в рамках общих критериев оценки безопасности информационных технологий (аналог международного ISO 15408) зафиксированы требования к средствам доверенной загрузки. Определяются следующие типы таких средств:

- программно-аппаратные средства доверенной загрузки;
- средства доверенной загрузки уровня базовой системы ввода-вывода;
- средства доверенной загрузки уровня загрузочной записи.

Программно-аппаратные средства доверенной загрузки обычно устанавливаются на шину расширения PCI, PCI-Express и т.д., и позволяют при подаче питания на устройство и получении управления выполнять контроль целостности конфигурации и логических объектов на накопителях данных.

Средства доверенной загрузки уровня базовой системы ввода-вывода обычно тесно интегрированы с прошивкой материнской платы, активируются прямым вызовом из базовой системы ввода-вывода, пользуются всеми защитными функциями контроллера доступа к внутренней памяти, не требуют дополнительных затрат на установку, эксплуатацию, при покупке обходятся дешевле по сравнению с программно-аппаратными устанавливаемыми решениями.

Средства доверенной загрузки уровня загрузочной записи являются нишевым решением, которое обеспечивает в большей степени недоступность пользовательских данных с помощью нестандартного форматирования/шифрования носителя этих данных. В отличие от перечисленных выше средств не обеспечивается защита от загрузки нештатных операционных систем и несанкционированного использования компьютерного оборудования.

Выбор средства доверенной загрузки должен определяться анализом угроз и выработкой необходимых мер защиты. Типовой состав угроз, которые должны нейтрализовываться средствами доверенной загрузки:

- загрузка нештатной операционной системы для обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;
- несанкционированная загрузка штатной операционной системы и получение несанкционированного доступа к информационным ресурсам;
- нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средства вычислительной техники.

Компании ЗАО «Аладдин Р.Д.» и ЗАО «Крафтвэй корпорейшн ПЛС» разработали защищённую вычислительную платформу на основе средства доверенной загрузки TSM от ЗАО «Аладдин Р.Д.» и защищённого

firmware разработки ЗАО «Крафтвэй корпорейшн ПЛС».

Решаемые задачи:

- Идентификация и аутентификация пользователей компьютера с применением идентифицирующих устройств (eToken PRO, eToken PRO Java, JaCarta);
- Поддержка интеграции с системами сбора, контроля, обработки, корреляции и реагирования на события информационной безопасности (требование PCI DSS, SOX, ISO 27001 и др.);
- Контроль целостности объектов, размещённых на жёстком диске компьютера для файловых систем FAT16/FAT32/NTFS/Ext2/Ext3/Ext4;
- Контроль неизменности CMOS;
- Контроль целостности объектов, таблиц, разделов жестких дисков:
  - главные загрузочные записи жестких дисков (MBR);
  - расширенные загрузочные записи жестких дисков (EBR);
  - загрузочные сектора разделов (Boot sector);
  - первые 62 сектора после MBR.
- Регистрация в журнале событий:
  - включение компьютера;
  - идентификация и аутентификация пользователя;
  - результаты проверки целостности контролируемой программной среды.
- Невозможность обхода загрузки СДЗ при любых режимах загрузки компьютера (в том числе при загрузке с отчуждаемых носителей);
- Невозможность извлечения СДЗ даже при непосредственном физическом доступе к защищённой платформе без нарушения физической целостности материнской платы вне заводских условий.

www.beltim.by

Основные направления развития и взаимодействия технологических решений в сферах аутентификации, электронной подписи и сервисов доверенной третьей стороны

Комисаренко Владимир Владимирович, директор по развитию ЗАО «БЕЛТИМ СБ»

Среди основных тенденций в сфере инфраструктуры открытых ключей в 2012–2013 годах можно выделить следующие:

- Выход на активные продажи услуг удостоверяющих центров (УЦ);
- Статус тренда «множественность алгоритмов ЭЦП» не изменился;
- Новые разработчики средств криптографической защиты информации, включая программно-технические средства, реализующие функции удостоверяющих и регистрационных центров не появляются.

Оценивая развитие сервисов инфраструктуры открытых ключей, следует отметить появление новых компонентов, реализующих:

- сервисы валидации по OCSP протоколу (validation);
- сервисы, связанные с восстановлением ключей шифрования (key recovery);
- сервисы управления работой с клиентами (CRM).

В зарубежной практике оценка безопасности программно-технических средств, реализующих функции удостоверяющих и регистрационных центров, как правило, проводится по общим критериям (Common Criteria) по уровню EAL 4.

В Российской Федерации, Республике Беларусь, Украине оценка защищенности осуществляется на соответствие специфическим национальным требованиям.

В Республике Беларусь в Положении о порядке криптографической защиты информации №62 от 30.08.2013 г. указано, что системы защиты информации информационных систем, системы безопасности КВОИ и системы электронных документов государственных информационных систем должны включать в себя не только средства криптографической защиты информации, но и комплекс средств обеспечения их безопасности. При этом программные СКЗИ и программное обеспечение аппаратных СКЗИ должны соответствовать требованиям, установленным СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации». А программно-аппаратные и технические СКЗИ – требованиям, установленным СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации».

Различие подходов приводит к невозможности сравнения уровней безопасности удостоверяющих центров различных государств при организации их взаимодействия по «мостовой» схеме.

Все более популярной становится применение электронной подписи в «облаках». Основной проблемой при этом является соответствие требованиям законодательства:

- при использовании усиленных электронных подписей участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности, не допускать использование принадлежащих им ключей электронных подписей без их согласия (в Российской Федерации);
- владелец личного ключа обязан хранить в тайне личный ключ (в Республике Беларусь).

Использование безопасных сертифицированных средств электронной цифровой подписи на «облачных» серверах и, в тоже время, применение легких решений на стороне пользователя составляют противоречие.

В связи с необходимостью поддержки различных методов аутентификации и уровней защищенности все более популярно становится применение единых серверов идентификации и аутентификации (Single sign-on). В этом случае прикладная система взаимодействует только с сервером идентификации-аутентификации.

Продолжаются работы по развитию сервисов доверенной третьей стороны (ДТС). Достигнуто понимание вопросов обеспечения безопасности на уровне ДТС-ДТС. Проводится тестирование реализаций форматов и протоколов на базе программно-технических платформ России, Казахстана и Беларуси.

С целью реализации требований статьи 10 «Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза», утвержденного Правительствами государств от 21 сентября 2010 года, в Республике Казахстан создана Доверенная третья сторона и принято постановление Правительства Республики Казахстан от 12 марта 2013 года №227 «Об утверждении Правил подтверждения подлинности иностранной электронной цифровой подписи доверенной третьей стороной Республики Казахстан».

ДТС Республики Казахстан на основе полученных запросов осуществляет их проверку, при этом перенаправляет запросы в соответствующий ДТС иностранного государства, в котором было выпущено проверяемое регистрационное свидетельство.

На основании полученного ответа от ДТС иностранного государства ДТС РК формирует ответ в виде квитанции DVC, являющейся необходимой и достаточной для подтверждения подлинности иностранной ЭЦП на территории Республики Казахстан.

Подтверждение подлинности иностранной ЭЦП ДТС Республики Казахстан осуществляется в круглосуточном онлайн-режиме на бесплатной основе через интернет-ресурс.

В Республике Беларусь программно-технические решения, необходимые для развития сервисов ДТС, создаются Государственным предприятием «НИИ ТЗИ» и ЗАО «БЕЛТИМ СБ» в рамках реализации мероприятия «Разработка программно-аппаратного комплекса доверенных центров обеспечения электронного документооборота» 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 20.04.2012 г. №6.

www.beltim.by

s•terra BEL

Белорусский VPN: перспективные продукты, технологии и решения

Сапрыкин Александр Михайлович, директор ИП «С-Терра Бел» (РБ)

Справка ТБ

Сапрыкин Александр Михайлович, родился в 1957 году, в 1979–1996 гг. – военнослужащий, в 1996–2004 гг. – начальник Управления информационных технологий Министерства иностранных дел Республики Беларусь, в 2004–2008 гг. – советник-начальник отдела ИТ Посольства Республики Беларусь в Российской Федерации, с 04.2008 г. по наше время – директор ИП «С-Терра Бел» (РБ), представитель международной конференции «Инфофорум» в Республике Беларусь. Имеет звание – полковник запаса, дипломатический ранг – советник, третий класс госслужащего. Опыт работы в области ИБ свыше 20 лет.

Компания «С-Терра Бел» занимается разработкой сертифицированных в национальной системе соответствия Республики Беларусь Bel VPN продуктов, предназначенных для защиты (шифрования) межсетевого трафика и удаленного доступа в распределенных ведомственных (корпоративных) IP-сетях с функцией межсетевого экрана. Как известно, VPN продукты со встроенной криптографией являются основой для создания защищенных распределенных информационных систем во всем мире, в первую очередь, в развитых странах.

Bel VPN продукты – это первые в Беларуси программные и программно-аппаратные VPN продукты с полномасштабной реализацией международных технических стандартов архитектуры IKE/IPsec, а также основных отечественных криптографических стандартов и ТНПА (в версии 3.0.1 – ГОСТ 28147, СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011, СТБ П 34.101.43-2009, РД РБ 07040.1202-2003).

Продукты применяются примерно в двадцати белорусских министерствах, ведомствах и организациях. За пять лет (с 2009 года) поставлено несколько сотен единиц Bel VPN продуктов. Объем рынка Беларуси оценивается на уровне многих тысяч единиц подобных продуктов. То есть, в настоящее время мы находимся в начальной фазе развития рынка ИБ, но потребители уже и сейчас хотели бы видеть более широкий спектр СЗИ, в том числе и VPN продуктов, с различным функционалом.

Компания анонсировала на выставке-форуме «Центр безопасности. Информационная безопасность 2013» следующие решения:

- Специализированное решение для банкоматов – Bel VPN Gate 100B;
- Программно-аппаратный комплекс «Клиент безопасности Bel VPN Client 3.0.1 на базе электронного планшета», предназначенный для применения в категорированных сетях уровня Б2.

В режиме изучения спроса также анонсировались:

- Продукт С-Терра КП (панель управления) для централизованного управления Bel VPN продуктами (Client/Server/Gate);
- Продукт «Среда построения доверенного сеанса связи (СПДС) – ПОСТ», обеспечивающий при удалённом доступе доверенную загрузку целостной информационной среды и изолированное сетевое соединение с сервером приложений.

За последние два-три года в Беларуси отмечается все более широкое применение национальных стандартов в сфере средств защиты информации. Причем динамику задает государственный регулятор – Оперативно-аналитический центр при Президенте Республики Беларусь. В частности, если Bel VPN продукты версии 3.0 соответствовали требованиям приказа ОАЦ №18 от 03.11.2011 г., то следующая версия 3.0.1 – приказу №46 от 25.05.2012 г., а новая продуктная линейка версии 4.1, разработка которой ведется в настоящее время (и которая была презентована на ЦБ-2013), соответствует уже требованиям приказа ОАЦ №62 от 30.08.2013 г., вступившего в силу с 19.10.2013 г. Этот приказ, как известно, лег в основу требований к СКЗИ в техническом регламенте ТР 2013/027/BY, вступившем в силу с января 2014 года.

Пользователям Bel VPN продуктов не стоит беспокоиться по поводу изменения требований к СКЗИ – в рамках гарантийного и дополнительного (платного) технического сопровождения они имеют право на бесплатную (или за незначительную доплату) модернизацию используемых Bel VPN продуктов на весь срок их эксплуатации. А каждая новая версия Bel VPN продуктов в обязательном порядке совместима с предыдущей, и обе линейки продуктов могут эксплуатироваться необходимое для полного перехода время одновременно.

Кратко об основных характеристиках и отличиях перспективной версии 4.1, которая, как планируется, поступит на рынок в конце 2014 года (учитывая время на сертификацию):

- Поддерживаемые ОС:
  - Debian 6 (32/64bit),
  - Windows XP/Vista/7/8 (32/64bit),
  - Windows Server 2003, 2008, 2008 R2, 2012,
  - Android 4.
- Более широкий перечень поддерживаемых аппаратных платформ;
- Усовершенствованный межсетевой экран;
- Соответствие требованиям приказа ОАЦ от 30.08.2013 №62:
  - шифрование по СТБ 34.101.31 (БелТ) по умолчанию,
  - ЭЦП на эллиптических кривых по СТБ 34.101.45,
  - генерация псевдослучайных чисел по СТБ 34.101.47,
  - протокол согласования ключей с реализацией на эллиптических кривых по СТБ 34.101.66,
  - криптобиблиотека AvC и USB-носители ключей и сертификатов AvPass/AvBign производства ЗАО «Авест».

Также сотрудники компании на выставке-форуме «Центр безопасности. Информационная безопасность 2013» демонстрировали всем работу стенда по перехвату открытого трафика в общественных IP-сетях – на примере «кафе с wi-fi сетью».

www.s-terra.by

Энергоэффективность: методы оптимизации инженерной инфраструктуры

Александр Николаевич Саванович – территориальный менеджер по Беларуси APC by Schneider Electric.

По оценкам ассоциации GreenGrid доля потребления ЦОД от общего уровня электричества в мире составляла около 1% 5 лет назад, сейчас эта цифра близка к 2%, прогноз роста на ближайшие 5 лет – 3%.

Сегодня типичный центр обработки данных расходует намного больше необходимого количества энергии. Известен ряд экономически обоснованных путей сокращения энергопотребления существующих ЦОД в краткосрочной перспективе, а также мер, применяемых при проектировании новых объектов. И если буквально несколько лет назад проблема повышения энергоэффективности не вызывала особенного интереса у ИТ-руководителей, то сейчас данная тематика стала очень актуальной. Это связано с одной стороны с тенденцией укрупнения ЦОД. При этом наблюдается рост стоимости электроэнергии и сложности с получением необходимых мощностей в точке строительства ЦОД. С другой стороны количество ЦОД в мире увеличивается, и этот сегмент стал самым быстрорастущим с точки зрения потребления энергии за последние 5 лет.

На настоящий момент энергоэффективность становится одним из ключевых показателей в бизнес-модели ЦОД, переходя из технологической плоскости в плоскость экономическую. Однако состояние нормативной базы в области энергоэффективности ЦОД несовершенно. При детальном рассмотрении обнаруживается большое количество «подводных камней» в области измерения, расчета и сравнения показателей энергоэффективности.

Существует соглашение отраслевых организаций и правительственных ведомств США, Европы и Японии, в соответствии с которым в качестве предпочтительной меры энергоэффективности утверждён показатель PUE (Power Usage Effectiveness). PUE определяется как соотношение общей мощности, подводимой к ЦОД, к мощности, потребляемой непосредственно ИТ-оборудованием ЦОД. Смысл PUE заключается в том, насколько велики/низки потери мощности на обеспечение работы активного оборудования ЦОД. Как видно из определения, идеальное значение PUE = 1 (0% потерь мощности на инженерную инфраструктуру). Реальные значения PUE для традиционных ЦОД лежат в диапазоне 1.5-3.0.

Несмотря на то, что PUE является одной из ключевых метрик эффективности ЦОД, не стоит идеализировать значимость данного параметра. Это лишь только коэффициент энергоэффективности ЦОД. Помимо этого, есть ряд других ключевых параметров, таких как отказоустойчивость, стоимость общего счета за электричество и т.д., которые также очень важны для понимания эффективности ЦОД в целом. Производя оценку энергоэффективности ЦОД, необходимо помнить, что PUE – это результат вычисления, и сравнивать эти коэффициенты для разных объектов очень сложно, нужно четко понимать соответствие методик измерения PUE и сопоставимость параметров сравниваемых объектов. На практике встречаются различные показатели PUE: моментальный, среднемесячный, годовой, и необходимо специфировать, о каком коэффициенте идет речь. Много дата-цетров строятся в офисных или промышленных зданиях. Для таких объектов при расчете коэффициента энергоэффективности обязательно нужно учитывать центральные инженерные системы зданий (делить пропорционально). Также на коэффициент энергоэффективности большое влияние оказывает уровень отказоустойчивости, поскольку при увеличении уровня резервирования

добавляются резервные устройства, имеющие собственное потребление и изменяется уровень загрузки инженерных систем.

Ставя перед собой задачу повышения энергоэффективности ЦОД, прежде всего, необходимо обеспечить контроль соответствующих параметров с целью отслеживания эффективности предпринимаемых мер. Сегодня на рынке представлены системы измерения, контроля, мониторинга расхода электроэнергии и PUE в ЦОД, позволяющие иметь полное представление об энергетических потерях подсистем, отслеживать текущее и «историческое» значение PUE, а так же позволяющие моделировать изменения инженерной инфраструктуры с прогнозированием результатов.

Опыт аудита площадок существующих ЦОД позволяет говорить о том, что основные резервы снижения PUE лежат в области систем охлаждения. **В качестве общих рекомендаций по оптимизации инженерной инфраструктуры ЦОД и повышения эффективности системы охлаждения можно выделить следующие:**

- **Оптимизация воздушных потоков, переход от периметрального к внутирядному охлаждению.** Рядные кондиционеры размещаются не по периметру помещения, а среди стоек с ИТ-аппаратурой. Благодаря укорочению маршрутов циркуляции горячие и воздушные потоки меньше смешиваются, их распределение становится более предсказуемым, что позволяет более точно автоматически подстраивать производительность кондиционеров под текущие потребности. Работа вентиляторов с переменной скоростью вращения ровно на той мощности, которая необходима для обслуживания нагрузки, обеспечивает дополнительную экономию энергии. Кроме того, рядная архитектура позволяет обрабатывать отработанный воздух максимально горячим, прямо из источника тепла, не позволяя ему смешиваться с более холодным окружающим воздухом. В совокупности все эти факторы значительно повышают эффективность системы кондиционирования;

- **Стратегия зонирования ЦОД по уровню отказоустойчивости и плотности мощности.** Для любого ЦОД характерно наличие высоконагруженных и малонагруженных стоек, также присутствует критичная и менее критичная нагрузка. Разделение нагрузок по разным зонам позволяет обеспечить соответствующий уровень резервирования и не переразмеривать системы кондиционирования и применять тот тип охлаждения, который наиболее подходит к данному уровню нагрузки;

- **Применение систем свободного охлаждения (free-cooling).** На сегодняшний день это, пожалуй, самый эффективный способ снижения PUE в ЦОД. Благодаря расширению ассоциацией ASHRAE рекомендованного температурного режима в машинном зале стало доступно применение свободного теплообмена между ЦОД и окружающей средой большую часть года. Сегодня известно более 15 различных способов естественного охлаждения, каждый из них имеет свои особенности применения. Для большинства систем свободного охлаждения характерна большая занимаемая площадь вне ЦОД, большая начальная стоимость по сравнению с традиционными системами охлаждения, однако, экономия места в машинном зале и снижение расходов на электроэнергию может дать экономическую выгоду в применении подобных систем. Для класса систем естественного охлаждения, подающих в машинный зал непосредственно холодный воздух, концептуально упростилось построение отказоустойчивых систем за счет уменьшения количества компонентов: достаточно зарезервировать сами устройства и воздуховоды в машинный зал, чтобы получить полностью резервированную систему охлаждения. Также следует отметить появление на рынке модульных систем естественного охлаждения, позволяющих постепенно наращивать систему охлаждения соразмерно растущей нагрузке ЦОД;

- **Соразмерная с нагрузкой инфраструктура.** В большинстве случаев инженерная инфраструктура ЦОД строится с запасом по мощности относительно основного ИТ-оборудования. К тому же, наличие резервных систем и поэтапный ввод нагрузки приводят к тому, что реальная нагрузка на инженерные системы ЦОДа находится в пределах 30-40%. Это приводит к лишним затратам за счет включенного «лишнего» оборудования и за счет падения эффективности систем: для большинства устройств лучший КПД достигается при загрузке 65-80%. Поэтому целесообразно отслеживать уровень загрузки систем и отключать лишнее оборудование. Исключение составляют некоторые системы естественного охлаждения: при уменьшении нагрузки на устройство увеличивается период, в течение которого можно обойтись без включения компрессорного цикла, и, следовательно, сэкономить электроэнергию.

Нужно также отметить, что каждый ЦОД является уникальным объектом, для которого необходим свой комплекс мероприятий, направленных на повышение эффективности инженерных систем. Поэтому работа по повышению эффективности работы инженерных систем в ЦОДе должна начинаться с аудита ВЦ для анализа текущей ситуации и формирования рекомендаций и мер, направленных на снижение PUE и повышение надёжности и эффективности инженерных систем.

Несмотря на то, что PUE является важным показателем эффективности ЦОД, для конечного результата не менее важны такие абсолютные показатели, как потребление электричества и его стоимость, а также стоимость самого инженерного оборудования, позволяющего добиться экономии электроэнергии. Самое главное, в погоне за энергоэффективностью не навредить ИТ-оборудованию и не снизить уровень надежности ЦОД. Поскольку стоимость, даже кратковременного простоя оборудования, может оказаться выше всей экономии энергии.

www.schneider-electric.com

DataHata
надежный датацентр

История запуска коммерческого ЦОД

Кожуховский Евгений Андреевич, технический директор ООО «Датахата»

1. Цели, задачи

- **Быстрый выход на рынок**. ДатаЦентр «Датахата» – первый провайдеронезависимый ЦОД в Республике Беларусь. Введен в эксплуатацию в 1 квартале 2011 года. Общая площадь дата-центра составляет 100 кв.м. На сегодняшний момент размещается 20 шкафов с 40 полезными U (19", глубиной до 1000 мм) и 2 tower шкафа по 16 мест в каждом. Средняя электрическая мощность одной стойки – 5 кВт.

- **Независимость от операторов.** На сегодняшний момент в ДатаЦентре «Датахата» присутствуют следующие операторы связи: СП ООО «Деловая сеть», TCM.BY – Оператор связи, Интернет-провайдер «Атлант Телеком», velcom – оператор мобильной связи, РУП «Белтелеком», ЗАО «Банковско-финансовая телесеть». Кабельное и кроссовое оборудование удовлетворяет требованиям международных стандартов.

- **Надежность.** При строительстве Дата-центр «Датахата» создана максимально защищенная инфраструктура, путем резервирования всех модулей по схеме N+1. Помещение Дата-центр «Датахата» расположено на цокольном уровне в охраняемом здании, что обеспечивает дополнительный уровень безопасности и защиты от несанкционированного проникновения. Дата-центр «Датахата» имеет необходимые технические ресурсы и подготовленных специалистов для оказания услуг по обслуживанию сетевого оборудования клиентов, организации и поддержке отказоустойчивых веб-систем, балансировке нагрузки, автоматической защиты от DDOS, динамической маршрутизации трафика.

- **Гибкость в подходе к клиенту.** Мы поставили перед собой цель построить дата-центр, который мог бы удовлетворить потребности как крупных и требовательных клиентов, так и тех, кому критична стоимость услуг. За два года работы коэффициент отказоустойчивости составил 99,981%.

2. Проблемы, с которыми мы столкнулись

- Отсутствие подходящих помещений (практически нет);
- Большие сложности для маленькой компании;
- Инертность мышления клиентов и партнеров;
- Эгоистичность монополистов рынка ☺

3. Технические решения

- **Электричество.** Начинали с APC Symmetra. Остановились на монолитных решениях. Два ввода в стойку. Используем APC Rack PDU. Система энергоснабжения состоит из комплекса, включающего в себя 5 источников бесперебойного питания (ИПБ), зарезервированных по принципу 4+1 (3 необходимых + 1 запасное) и одной дизель-генераторной установки (ДГУ). Мощность ДГУ составляет 150 кВт и рассчитана на одновременную работу всего оборудования дата-центра и на подзарядку батарей всех ИБП (Рисунок №1, №).

Охлаждение. Для поддержания температурного режима серверные помещения оборудованы системами приточно-вытяжной вентиляции и кондиционерами промышленного типа. Мощность системы кондиционирования составляет 125кВт. Серверные стойки расположены по принципу холодных и горячих коридоров, а также закрытие холодных коридоров (Рисунок №3).

- **Безопасность.** Дата-центр «Датахата» находится на закрытой территории. Все помещения и прилегающая территория круглосуточно охраняются. Пребывание клиентов и персонала в серверных залах и служебных помещениях контролируется системой видеонаблюдения которая интегрированна с системой охранной сигнализации. Возможна организация независимого online-видеонаблюдения с передачей видеоданных в службу безопасности клиента. СКУД – двери помещений ЦОД оборудованы электронными замками и считывателями карт.

4. Проблематика сегмента

- Отсутствие до недавнего времени альтернативных операторов в стране, предоставляющих доступ к внешним каналам;
- Незаинтересованность крупнейшего игрока рынка в участии единственного национального пиринга.

www.datahata.by

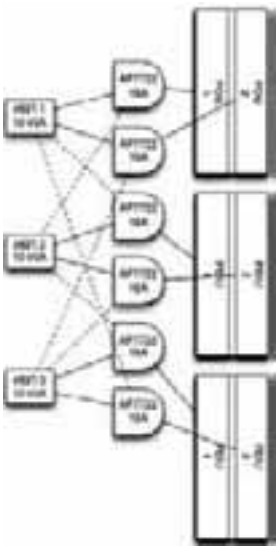


Рисунок №1

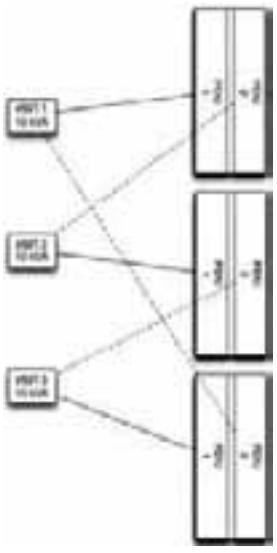


Рисунок №2

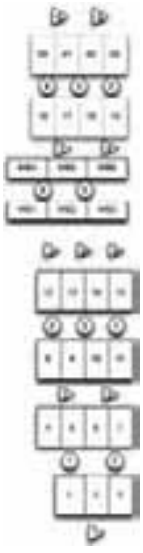


Рисунок №3

hoster.by

Безопасность в облаке: мифы и реальность

Алексей Русаков, начальник отдела облачных решений hoster.by

Облако на протяжении последних лет постоянно находится в центре дискуссий: его отличительные черты то возводятся в абсолютный культ и приравниваются к главной технологии будущего, то несправедливо критикуются. Однако актуальность облачных технологий, а в частности – облачного хостинга и построение на его основе IT-инфраструктуры предприятий, заключается именно в том, что это именно сегодняшний день, а не завтрашний или вчерашний. Это то, что сегодня работает оптимально и соразмерно поставленным перед современным бизнесом задачам.

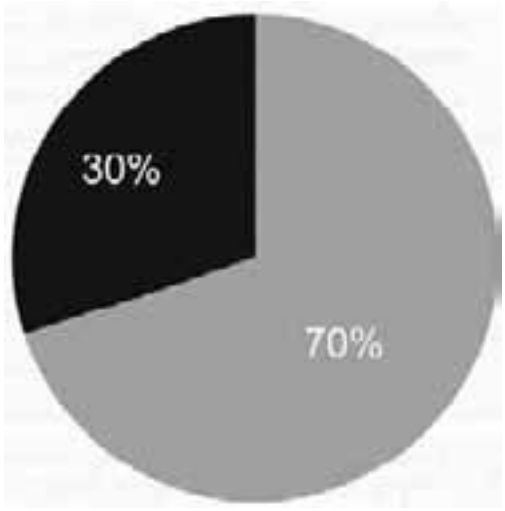
Безопасность облака – один из главных доводов скептиков. Он основан на убеждении в том, что данные не могут быть в безопасности, поскольку передаются через интернет. Однако большинство технических специалистов подтвердят, что в этом как раз сильная сторона облака. А уязвимости таятся там же, где и в работе любой другой технологии – человеческий фактор.

В нарушения мер безопасности из-за человеческого фактора входят в первую очередь неправильные настройки, непрофессионализм сотрудников и банальная халатность.

Пожалуй, главных нерешенных вопросов в теме облачной безопасности два. Первый – это отсутствие законодательной базы, описывающей работы с персональными данными (аналог ФЗ №152 в РФ). Второй – отсутствие системного понимания у большинства пользователей о том, из чего же состоит IT-безопасность как таковая.

Как правило, пользователи ограничиваются полумерами в виде собственного серверного оборудования и закупки дорогостоящего ПО, забывая при этом, что проблемы почти всегда зарождаются «изнутри» (от удаленного доступа или обиженного сотрудника до забытого стикера с записанным паролем). При этом до сих пор существуют страхи, что данные, передаваемые по зашифрованным каналам и хранящиеся в дата-центре на серверах провайдера в больше опасности, чем на компьютере или флешке, например, у собственного бухгалтера. К примеру, компания hoster.by является аккредитованным поставщиком услуг для организаций, которые работают со сведениями, составляющими государственную тайну. При этом нам периодически задают вопросы из разряда: «А ваши сотрудники будут иметь доступ к мои данным?».

Для комплексного решения вопроса защиты данных необходимо в первую очередь проводить аудит безопасности и оценку рисков. Это задает систему координат, в соответствии с которой можно думать над построением оптимальной защищенной инфраструктуры.



В случае переноса инфраструктуры в облако (в том числе переноса в него 1С) проводить какое-либо дополнительное обучение сотрудников не нужно. Данные и программное обеспечение будет работать в привычном режиме. Однако данные не будут храниться на рабочих компьютерах сотрудников. Поэтому никто, кроме авторизованных пользователей, просто физически не имеет доступа к данным.

Еще один аспект безопасности в облаке (и это скорее внутренний, технический аспект) – это сама система виртуализации. Она разделяет виртуальные машины на изолированные «контейнеры». То есть попасть из одного «контейнера» в другой просто невозможно, как и попасть из виртуальной машины к системе управления «контейнерами» (гипервизору).

www.hoster.by

Опыт подготовки специалистов по защите информации в БГУИР

Борботько Тимофей Валентинович – доктор технических наук, профессор кафедры защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР).

Справка ТБ

Борботько Тимофей Валентинович. Доктор технических наук, профессор. Профессор кафедры защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (БГУИР). Образование высшее – телекоммуникационные системы, в 2000 году закончил Высший государственный колледж связи. В 2009 году закончил докторантуру БГУИР по специальности «Методы и системы защиты информации, информационная безопасность». Опыт работы в области защиты информации с 2004 года по настоящее время.

В БГУИР накоплен некоторый опыт подготовки специалистов различного уровня в сфере информационной безопасности.

С 2001 г. в БГУИР открыто несколько учебных инженерных специальностей:

1. 1-38 02 03 «Техническое обеспечение безопасности» – подготовка инженеров-электромехаников, умеющих выполнять анализ потенциальных каналов утечки информации, наличие которых обусловлено применением технических средств шпионажа и утечкой информации посредством сетей телекоммуникаций, а также выбор наиболее оптимальных способов их защиты;

2. 1-98 01 02 «Защита информации в телекоммуникациях» – подготовка специалистов по двум квалификациям (специалист по защите информации, инженер по телекоммуникациям), обладающих теоретическими знаниями и практическими навыками исследования, разработки и сопровождения средств защиты и обработки информации в телекоммуникационных системах;

3. 1-39 01 04 «Радиоэлектронная защита информации» – подготовка инженеров по радиоэлектронике со специальными знаниями в области построения защищенных радиоэлектронных программно-аппаратных систем и устройств радионаблюдения, радиоэлектронной борьбы и криптологии, а также инженерно-технических средств;

4. 1-39 03 01 «Электронные системы безопасности» – подготовка инженеров-проектировщиков, способных проводить комплексное проектирование электронных систем безопасности, включающее определение угроз и рисков для защищаемого объекта; разрабатывать принципы обеспечения защиты и общую структурную схему системы безопасности; определение наиболее эффективных каналов передачи сигналов; выбор промышленно выпускаемых электронных и других технических устройств, совместно решающих задачу по обеспечению безопасности объекта.

С 2001 года введен единый для всех инженерных специальностей курс «Основы защиты информации и управление интеллектуальной собственностью», который содержит основные сведения по правовому, организационно-техническому и криптографическому обеспечению информационной безопасности информационных систем кредитно-финансовых и других специальных организаций.

Вторая ступень высшего образования – магистратура. С 2007 года в БГУИР обучается ежегодно не менее 35 магистрантов дневной и заочной форм обучения по специальности 1 98 80 01 «Методы и системы защиты, информационная безопасность». С 2010 года начата подготовка магистрантов дневной формы обучения на английском языке. Ежегодный набор на обучение составляет 8 15 человек из числа лиц иностранных граждан. Темы магистерских работ посвящены разработке технических и программно-аппаратных средств защиты информации.

В БГУИР ведется подготовка в аспирантуре по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», функционирует Совет по защите диссертаций по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Проводится ежегодная Белорусско-Российская научно-техническая конференция «Технические средства защиты информации» (г. Браслав), отдельные доклады в виде статей публикуются в журнале «Доклады БГУИР».

На базе Института информационных технологий и кафедры защиты информации БГУИР проводятся ежегодные курсы повышения квалификации по темам: «Защита информации в телекоммуникационных и автоматизированных системах», «Применение методов и средств криптографической защиты информации, в том числе электронной цифровой подписи», «Основы безопасности сетей» и др.

www.bsuir.by

Совершенствование подготовки специалистов по компьютерной безопасности в Республике Беларусь

Харин Ю.С., Матвеев Г.В.
НИИ прикладных проблем математики и информатики Белорусский государственный университет Минск, Беларусь.

Справка ТБ

Харин Юрий Семенович, директор Учреждения БГУ «НИИ прикладных проблем математики и информатики», зав. кафедрой математического моделирования и анализа данных факультета прикладной математики и информатики. Доктор физико-математических наук (1986), профессор (1987). Лауреат Государственной Премии РБ в области науки и техники (2002). Член-корреспондент НАН Беларуси (2004). Заслуженный деятель науки и техники РБ (2010).

Информация – высокоценный товар, который, как и всякий товар, надо производить (порождать), транспортировать (передавать), обрабатывать, хранить и защищать. **Защита информации** – важнейшая фаза этого жизненного цикла информации, требующая спе-циально подготовленных специалистов. Слабо подготовленный «защитник информации» может свести к нулю стойкость любой самой совершенной системы защиты информации.

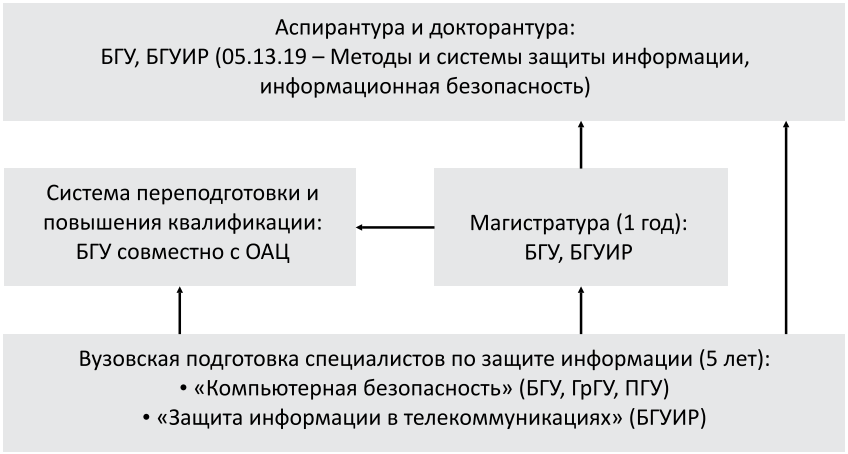
В стране имеется острая потребность в следующих категориях специалистов по защите информации:

- руководители подразделений защиты информации, отвечающие за состояние информационной безопасности, организацию и координацию работ по созданию комплексных систем защиты информационных ресурсов и электронного документооборота;
- специалисты по информационной безопасности, отвечающие за анализ рисков, связанных с использованием ИТ, выбор методов и средств защиты информации; администраторы средств защиты, отвечающие за эффективное функционирование средств защиты и средств контроля защищенности информационных ресурсов.

Подготовка специалистов по защите информации начата в БГУ в 1997 году.

Повышение квалификации работников республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь, в компетенцию которых входит обеспечение информационной безопасности этих органов (организаций), в соответствии с постановлением Совета Министров Республики Беларусь №646 от 31.05.2004 г. в Институте технологий информатизации и управления БГУ. ■

Система подготовки специалистов по защите информации в РБ:



Учебные пособия, изданные в Республике Беларусь:

Информация о компаниях

CERT.BY

Тел.: +375 17 309-24-64
E-mail: support@cert.by
Сайт: cert.by
Год основания: 2013 г.
Дополнительная информация:
Национальный центр реагирования на компьютерные инциденты Республики Беларусь. Основная задача центра – снижение уровня угроз информационной безопасности национального сегмента сети Интернет.
CERT.BY осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Республики Беларусь, а также реагирование на сами инциденты как в информационных системах государственных органов и организаций, так и у самостоятельно обратившихся субъектов национального сегмента сети Интернет.

CISCO

Республика Беларусь, 220034,
г. Минск, бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 подъезд, 2 этаж
Сайт: www.cisco.com, www.cisco.ru
Год основания: 1984 г.

EY (Эрнст энд Янг, ИООО)

Республика Беларусь, 220004,
г. Минск, ул. Короля, 51, 2 этаж, офис 30
Тел.: +37517 209-45-35
E-mail: inquiry@by.ey.com
Сайт: ey.com/belarus
Год основания: 1989 г. (история компании берет начало в 1849 г.)
Услуги:
Услуги в области аудита, налогообложения, сопровождения сделок и консультирования.

Falcongaze (Фалконгейз, ООО)

РФ, 119180, г. Москва, ул. Большая Полянка, 44/2, офис 525
Тел.: + 7495 640-29-22, +7499 638-39-71
E-mail:
- общие вопросы – contact@falcongaze.ru;
- отдел продаж – sales@falcongaze.ru;
- техническая поддержка – support@falcongaze.ru;
- контакт для СМИ – pr@falcongaze.ru.

Год основания: 2007 г.
Лицензии:
Лицензия ФСТЭК КИ 0072 №003596 от 16.03.2011 г., действительна до 16 марта 2016 г.
Сертификаты:
Сертификат ФСТЭК №2556 от 03.02.2012 г. Сертификат позволяет использовать систему SecureTower при создании автоматизированных систем до класса защищенности 1Г включительно, а также для защиты информации в информационных системах персональных данных до 2 класса включительно. Срок действия сертификата – до 3 февраля 2015 г.
Производство: система для защиты данных и мониторинга действий сотрудников SecureTower.
Услуги:
Защита конфиденциальных данных, мониторинг деятельности сотрудников, управление репутационными, операционными и правовыми рисками.
Поставка: система для защиты данных и мониторинга действий сотрудников SecureTower.
Выполненные проекты:
Система SecureTower занимает прочные позиции на рынке DLP-систем. Спектр потенциальных заказчиков программного комплекса SecureTower достаточно широк, поскольку любые компании и структуры, оперирующие массивами ценных данных, заинтересованы в их защите. На сегодняшний день систему Securetower успешно используют предприятия банковского сектора, учреждения здравоохранения и социального сектора, различного рода финансовые учреждения, промышленные компании, торговые коммерческие организации, а также транспортные корпорации. Наиболее значимыми внедрениями являются проекты, реализованные в таких компаниях как: Белорусское представительство международного 3PL оператора CTA Логистик, строительная компания ИЗОБУД, сеть туристических компаний «Велтра», ведущий интернет-дистрибьютор программного обеспечения компания Softkey, аудиторско-консалтинговая компания «Нексиа Пачоли», лизинговая компания «УРАЛЛИЗИНГ», Федеральное государственное унитарное предприятие «Главный радиочастотный центр», крупнейший банк Беларуси ОАО «АСБ Беларусбанк», а также банк ЗАО «Евробанк».
Дополнительная информация:
Система SecureTower два года подряд удостаивается звания «Лучшее ПО года» по версии журнала PC-magazine/RE, а также получает наивысшие оценки портала Anti-malware, одного из самых авторитетных СМИ, специализирующихся на информационной безопасности в России.

Schneider Electric

Республика Беларусь, 220006,
г. Минск, ул. Белорусская, д. 15, офис 9
Тел/Факс: +37517 226-06-74, +37517 227-60-34,
+37517 227-60-72, +37517 227-61-50
Сайт: www.schneider-electric.com
Год основания: 1836 г.
Дополнительная информация:
Компания Schneider Electric является мировым экспертом в области управления электроэнергией, ведущим разработчиком и поставщиком комплексных энергоэффективных решений для энергетики и инфраструктуры, промышленных предприятий, объектов гражданского и жилищного строительства, а также центров обработки данных.
Помимо разработки и внедрения энергоэффективных решений компания предлагает клиентам сервисное обслуживание, эффективную логистику, энергоаудит, передачу инновационных технологий и обучение.

Stonesoft, A McAfee Group Company

Stonesoft является разработчиком инновационных динамических решений в сфере обеспечения сетевой безопасности и непрерывности бизнеса.
РФ, 103045, г. Москва, ул. Трубная, 12, БЦ «Миллениум Хаус»
Тел.: +7495 787-99-36
E-mail: info.Russia@stonesoft.com
Сайт: www.stonesoft.com
Год основания: 1990 г.
Производство:
Продуктовый портфель компании состоит из первого в отрасли ИБ

динамического трансформера безопасности Security Engine, не имеющего себе равных межсетевого экрана следующего поколения (NGFW), интеллектуальной системы предотвращения вторжений IPS, а также шлюза защиты удаленного доступа SSL VPN. Уникальная в своем роде система управления Stonesoft Management Center обеспечивает централизованное управление всеми устройствами, а также мониторинг всей сетевой инфраструктуры из одной точки.

Услуги:

Stonesoft A McAfee Group Company предлагает своим заказчикам, частным и государственным организациям, нуждающимся в построении отказоустойчивых распределенных сетей, простые в управлении, соответствующие стандартам, динамичные решения по защите критически важных активов и обеспечению непрерывности бизнеса против современных быстроменяющихся угроз.

Поставка:

Универсальный шлюз безопасности Security Engine, межсетевой экран следующего поколения FWNG, система предотвращения вторжений IPS, шлюз защиты удаленного доступа SSL VPN, система управления SMC обеспечивает централизованное управление всеми устройствами.

Дистрибьютор компаний: NGSDistribution, ITGuard, Treolan.

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.

АльфаСистемы, ООО

Республика Беларусь, 220090,
г. Минск, Логойский Тракт, д. 22а, офис. 207
Тел.: +37517 262-84-64, 268-05-36
Факс: +37517 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); Spacecom (Япония); SC&T (Тайвань); Widearea Times Technology Co. (Китай); ITV (РФ), ISS (РФ); VideoNet (РФ).

БЕЗОПАСНЫЙ ДОМ, ОДО

220094, г. Минск, 2-й Велосипедный пер., д. 30, комн. 402
Тел./Факс: (017) 298-38-05(15), (029) 150-95-97
E-mail: odobd@mail.ru
Сайт: www.odobd.by
Год основания: 2006
УНП: 190682380
Контактные лица:
- Сидоренко Александр Владимирович, директор;
- Малец Сергей Федорович, ГИП;
- Янович Павел Станиславович, главный инженер.

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

Услуги:

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

Выполненные проекты:

ИП «Велком», ЗАО «Белорусская сеть телекоммуникаций», ЗАО «Projestos projektai» (Литовская Республика), ООО «Евроторг», СООО «Златка», ОАО «Франсабанк», ОАО «Белинвестбанк», ЗАО «Дельта Банк», ОАО «Белагропромбанк», ОАО «Технобанк», ООО «Аксис на Кирова», ООО «Нестле Россия», ЗАО «Торговый дом «ЛУКБЕЛОЙЛ», ЗАО «Универсам «Юго-Запад плюс», СООО «Маттиоли», УМСР-154 ОАО «МАПИД», ИООО «Орифлэйм косметикс», СООО «Белавтэкс», ИП «Ресторан Джомолунгма», ООО «ВкусСервис», ООО «СУШИ ВЁСЛА», ИП «ТА-Инжиниринг», ООО «ПРЕВАР», ООО «Лимкомсервис», СП «ВестТрансЛайн» ООО, ТПООО «Брест», ОАО «БЕЛРЫБА», ЧТУП «Ювелирная сеть 585», ЗАО «Торговый дом «ШагоВита», СП «САМБЕСТ» ООО, УП «Юнифарм», ЗАО «Федерация», ОАО «Торгодежда», КУП «Минскхлебпром», ГУ «Централизованная система детских библиотек», ЧУП «Поречье Белкоопсоюза», ГУ «НИИ онкологии и медицинской радиологии имени Н.Н.Александрова», УО «Национальный центр художественного творчества детей и молодежи» МО РБ, ТКУП «Минсктранс» филиал «Трамвайный парк», РУПСП «Птицефабрика «Дружба», ЗАО «ТрестБелПСП-строй», Высший Хозяйственный Суд Республики Беларусь, КУП «Минский метрополитен».

Белорусский государственный университет информатики и радиоэлектроники

Республика Беларусь, 220013,
г. Минск, ул. П.Бровки, 6
Тел/Факс: + 37517 292-32-35, + 37517 202-10-33
E-mail: kanc@bsuir.by
Сайт: www.bsuir.by
Год основания: 1964 г.

Дополнительная информация:

Ведущее в Республике Беларусь высшее учебное заведение в области информационных технологий, радиотехники, электроники и телекоммуникаций, широко известное в Европе, странах СНГ и во всем мире.
В настоящее время университет готовит инженерные кадры по 30 специальностям и 25 специализациям в области вычислительной техники, программного обеспечения информационных технологий, инженерно-психологического обеспечения информационных технологий, информатики, информационного обеспечения автоматизированных систем, искусственного интеллекта, автоматического управления, радиотехники, радиоэлектронных систем, микроэлектроники, телекоммуникаций, проектирования радиоэлектронных и электронно-вычислительных средств, электронного аппаратостроения, медицинской электроники, технических средств безопасности, метрологии, стандартизации и сертификации, экономики.

БЕЛТИМ СБ, ЗАО

Республика Беларусь, 220002,
г. Минск, пр-т Машерова, 25
Тел.: +37517 334-95-12, 334-99-11
E-mail: info@beltim.by
Сайт: www.beltim.by
УНП:190527159

Продукция: аппаратные средства защиты информации, техника обнаружения каналов утечки информации, устройства уничтожения информации, программное обеспечение, антитеррористическое и до-

смотровое оборудование, видео- и аудиорегистраторы, программно-аппаратные измерительные комплексы.
Услуги: аттестация объектов информатизации, выявление каналов утечки информации, защита информации от утечки по каналам ПЭМИН, защита объектов информатизации, защита вычислительных сетей, защита компьютеров, защита помещений, консалтинг, специальные исследования.

Группа информационной безопасности, ООО

РФ, 107023, г. Москва, Мажоров переулок, д. 14, строение 2, офис 2203
Тел.: +7 (495) 984-33-64
E-mail: info@group-ib.ru
Сайт: www.group-ib.ru
Год основания: 2003 г.
Лицензии:
Лицензия ФСБ РФ на работу со сведениями, составляющими государственную тайну (ГТ №0064472, регистрационный номер: 4490).
Услуги:
- мониторинг и предотвращение киберугроз;
- аудит информационной безопасности;
- криминалистические исследования в сфере высоких технологий;
- расследование киберпреступлений и мошенничеств с использованием высоких технологий;
- разработка инновационных программных продуктов по мониторингу, обнаружению и предотвращению возникающих киберугроз.

ДатаХата, ООО

Республика Беларусь, г. Минск, ул. Колхозная, 19а
Тел.: +37529 308-66-66
E-mail: info@datahata.by
Сайт: www.datahata.by
Год основания: 2011 г.
Услуги:
- размещение IT-оборудования;
- аренда IT-оборудования;
- хостинг;
- услуги администрирования.

Дополнительная информация: аренда ПО, регистрация доменных имен, место для хранения резервных копий (бэкапов), SSL-сертификаты.

Инсайд РУС, ООО

РФ, 194100, г. Санкт-Петербург, ул. Новолитовская, д. 15А,
Бизнец-центр «Аквилон», офис 402
Тел./Факс: +7812 331-09-67
E-mail: info@inside-rus.ru
Сайт: www.inside-rus.ru
Год основания: 2012 г.
Производство: защищенные криптографические микроконтроллеры компании Inside Secure.
Поставка: защищенные криптографические микроконтроллеры компании Inside Secure.
Дистрибьютор компаний:
Эксклюзивный дистрибутор микроконтроллеров Inside Secure.
Дополнительная информация:
Производство и применение защищенных криптографических микроконтроллеров компании Inside Secure. Поставка защищенных криптографических микроконтроллеров компании Inside Secure. Эксклюзивный дистрибутор микроконтроллеров Inside Secure.

Национальный банк Республики Беларусь

Республика Беларусь, 220008,
г. Минск, пр-т Независимости, 20
Тел.: +37517 218-38-94
Сайт: www.nbrb.by
Год основания: 1922 г.
Дополнительная информация:
Центральный банк и государственный регулятор банковской системы, владелец системы «Расчет».

НИИ прикладных проблем математики и информатики БГУ

Тел.: +37517 209-51-04
E-mail: apmi@bsu.by
Сайт: apmi.bsu.by
Год основания: 2000 г.
Лицензия: 01019/0531677 по август 2014 г., ОАЦ.

Услуги:
Экспертиза и сертификационные испытания программных средств криптографической защиты информации.
Выполненные проекты: СТБ 34.101.27, СТБ 34.101.31, СТБ 34.101.45, СТБ 34.101.47, СТБ П 34.101.60, СТБ 34.101.65, СТБ 34.101.66, СТБ 34.101.67.
Дополнительная информация:
Развитие актуальных научных направлений прикладной математики и информатики, научно-исследовательские и опытно-конструкторские работы, подготовка и повышение квалификации научно-педагогических кадров.

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

Республика Беларусь, 220088,
г. Минск, ул. Первомайская, 26/2
Тел./факс: +37517 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 Республики 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.

Сертификаты:
- Сертификат соответствия Государственного комитета по стандартизации Республики Беларусь, что система менеджмента качества оказания услуг по проведению научно-исследовательских и опытно-конструкторских работ в области технической защиты информации, аттестации объектов информатизации и систем защиты информации, проведению испытаний средств защиты информации, проектированию и монтажу систем защиты информации, охранной и пожарной

сигнализации, систем видеонаблюдения, контроля доступа, локальных вычислительных сетей, разработке и производству программных и программно-аппаратных средств защиты информации соответствует требованиям СТБ ISO 9001-2009.

- Аттестат аккредитации Государственного комитета по стандартизации Республики Беларусь, что испытательная лаборатория по требованиям безопасности информации соответствует критериям Системы аккредитации Республики Беларусь и аккредитована на соответствие требованиям СТБ ИСО/МЭК 17025.

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.

Разработки:

1. Устройство системы технических средств для обеспечения оперативно-розыскных мероприятий.
2. Аппаратно-программный комплекс «Авангард».
3. Носитель специализированный «Носитель».
4. Устройство защиты линий электропитания и заземления от утечки информации «Рокот».
5. Комплекс защиты информационных сетей «IP-барьер».
6. Программно-аппаратный комплекс средств для гарантированного уничтожения информации на магнитных носителях «Информация».
7. Программно-аппаратный комплекс «Филин».
8. Программный комплекс эталонных тестовых средств «Эталон».
9. Программно-аппаратный комплекс для выполнения ремонта средств вычислительной техники «Ограничение».
10. Аппаратный комплекс для транспортировки магнитных носителей «Транспорт».
11. Распределенная система радиомониторинга «Беседь».
12. Средство защиты информации от утечки по цепям электропитания ИБП «Стриж».
13. Автоматизированный мобильный комплекс «Сож».
14. Комплекс автоматизированный мобильный «Шум-3М».
15. Детектор поля.
16. Фильтр-ограничитель «Гомий».
17. Автоматизированный испытательный комплекс для измерения побочных электромагнитных излучений.
18. Программный комплекс «Криптотестер».
19. Аппаратура считывания «Мираж».
20. Сканер «Контролер».

Дистрибьютор компаний: ЗАО «Конструкторское бюро «ПРИБОР».

НОВАТЕХ СИСТЕМЫ БЕЗОПАСНОСТИ, ЗАО

Республика Беларусь, 220125,
г. Минск, ул. Городецкая, 38А, 3-й этаж
Тел.: +37544 718-53-50 velcom, +37533 664-89-02 МТС,
+37517 286-39-51/52/50
E-mail: info@novatekh.by, sales@novatekh.by
Сайт: www.novatekh.by

Год основания: 2006 г.
УНП: 190543080

Лицензия: Лицензия на право осуществления деятельности по обеспечению пожарной безопасности №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.

Производство и сертификаты:

Перечень товаров собственного производства и сертификатов:

Наименование оборудования	Сертификат		
	Дата выдачи	Действителен до:	№
Система охранной сигнализации ПКП-128 (с модулями)	20.01.2012	20.01.2017	BY/112 03.03.023 00553
Система пожарной сигнализации ППКП-128 (с модулями)	20.11.2012	19.10.2014	BY/112 02.01.033 00038
Приборы охранные ПКП-3,ПКП-4М,ПКП-4РДО,ПКП-4РДО-GSM,ПКП-4GSM (с модулями)	21.10.2011	21.10.2016	BY/112 03.03.023 00489
Прибор охранный ПКП-8РДО	27.06.2011	27.06.2016	BY/112 03.03. 023 00447
Приборы охранные ПКП-6,ПКП-8 (с модулями)	21.10.2011	21.10.2016	BY/112 03.03.023 00490
Приборы охранные ПКО-2,ПКО-2М (с модулями)	24.10.2011	21.10.2016	BY/112 03.03.023 00493
Модуль передачи извещений МПИ-GSM	21.10.2011	21.10.2016	BY/112 03.03.023 00491
Модуль передачи извещений МПИ-ETHERNET	27.06.2011	27.06.2016	BY/112 03.03.023 00449
Извещатель охраны периметра "Спрут-01"	24.10.2011	21.10.2016	BY/112 03.03.023 00494
Система передачи извещений "Новатех-РДО"	24.10.2011	21.10.2016	BY/112 03.03.023 00495
Прибор пожарный ППКП-8	26 11.2012	28.08.2014	BY/112 02.01.033 00041
Извещатель охранный ИНС-105, ИНС-106	21.10.2011	21.10.2016	BY/112 03.03.023 00487
Извещатель охранный ИНС-206	21.10.2011	21.10.2016	BY/112 03.03.023 00488
Извещатель охранный ИНС-110	15.04.2010	19.01.2015	BY/112 03.03.023 00233
Извещатель охранный ИНС-409	15.04.2010	19.01.2015	BY/112 03.03.023 00234
Извещатель охранный ИНС-307	27.06.2011	27.06.2016	№BY/112 03.03. 023 00448
Извещатель охранный ИНС-101	11.12.2012	11.12.2017	№BY/112 03.11. 023 00669
МПИ-GSM выносной / МПИ-Ethernet выносной, модули передачи извещений	08.08.2011	08.08.2016	№BY/112 03.03. 023 00461
ИПС-12/2 Источник питания сетевой	29.12.2012	28.12.2017	№ BY/112 02/01/033 00058

Услуги: разработка, производство и продажа оборудования пожарной и охранной сигнализации, систем радио- и GSM-охраны. Консультации по подбору оборудования и настройке систем охранной, пожарной сигнализации, систем видеонаблюдения.

Поставка оборудования: Basler, Axis.

Дистрибьютор компаний:

Представитель Dallmeier electronic в Республике Беларусь.

Авторизированный дистрибьютор по продаже, установке и гарантийному обслуживанию систем безопасности NOVUS® на территории Республики Беларусь.

Производитель бюджетной линейки видеонаблюдения 2x2.

Рамок, Производственно-торговое частное унитарное предприятие

220036, г. Минск, ул. Лермонтова, 29
Тел./факс: (017) 210-22-80, 213-67-00, (029) 613-67-00, (033) 313-67-00
E-mail: ramok@ramok.by
Сайты: www.RAMOK.by, www.BizSoft.by, www.ydom.by, www.kypi.by
Год основания: 1992
УНП: 100001879
Контактные лица: Яско Владимир Федорович, директор.
Лицензии:
- Лицензия на право осуществления деятельности по обеспечению безопасности юридических и физических лиц №02010/0444764, 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 №051/11T, 20.07.11г., LucatronAG (Германия); Сертификат №2011-QC, 03.12.2012 г., SMART-Home(США), Сертификат BiampSystems (США).

Производство: торговое оборудование, витрины, прилавки, мебель под заказ клиента.
Услуги: центр обслуживания кассовых аппаратов, ремонт кассовых аппаратов, монтаж видеонаблюдения, ОПС, СКУД, автоматизация торговли и услуг, озвучивание помещений.
Поставка: системы видеонаблюдения, сканеры штрих-кода, терминалы сбора данных, противокражное оборудование, кассовое оборудование, весовое оборудование, счетчики банкнот, детекторы валют, видеодомофоны, переговорные устройства, активные микрофоны, торговое оборудование, этикет-пистолеты, принтеры этикеток, программное обеспечение для автоматизации торговли и сферы услуг, оборудование для автоматизации дома, гостиницы, офиса.
Выполненные проекты: сеть магазинов «Оптика-24», сеть магазинов «Парфюмстандарт», сеть салонов «Интеркомпьютерсервис», сеть магазинов «Парничок», автосалон «Субару», Сеть аптек по Беларуси более 26 шт., сеть магазинов «Космо», сеть салонов «Евросеть» и др.
Дистрибьютор компаний: LucatronAG (Германия), SMART-Home (США), GoDEX (Тайвань), CapherLab (Тайвань), Vangold (Китай), ZKSoftwera (Китай), Protech (Тайвань), Planet (Тайвань), ОАО «КЗТА» (РФ), Fiscat (Китай).
Дополнительная информация: участие в выставках Tibo, HoReCa&RetailTech и др.

С-Терра Бел, ИП

Республика Беларусь, 220012,
г. Минск, ул. Чернышевского 10а, к.702
Тел/Факс: +37517 280-60-00, +37517 280-78-67
E-mail: info@s-terra.by
Сайт: www.s-terra.by
Год основания: 2008 г.
Лицензии:
Специальное разрешение (лицензия) выдано на осуществление работ и услуг по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, на основании приказа от 17 сентября 2008 г. №28 и зарегистрировано в реестре лицензий Оперативно-аналитического центра при Президенте Республики Беларусь за №1. Срок действия специального разрешения (лицензии) продлен на основании приказа от 13 августа 2013 г. №57 сроком на пять лет (до 17 сентября 2018 г.).
Производство:
Bel VPN продукты – программные и программно-аппаратные сетевые средства криптографической защиты информации, сертифицированные в Республике Беларусь и применяемые для защиты ведомственных (корпоративных) территориально-распределенных вычислительных сетей и удаленного доступа.
Услуги:
Предоставляет услуги по техническому сопровождению Bel VPN продуктов на весь период их эксплуатации.
Дополнительная информация:
Компания входит в Научно-технологическую ассоциацию «Инфопарк». Руководитель компании является представителем международного форума информационной безопасности «Инфофорум» в Республике Беларусь.
В июне 2010 года «С-Терра Бел» награждена Дипломом 6-го Евразийского форума информационной безопасности – «Инфофорум-Евразия» за «создание эффективных средств сетевой защиты информации на Евразийском пространстве».

Смартпроект, ООО

Республика Беларусь, 220073,
г. Минск, ул. Гусовского, д. 6, офис 2.6
Тел./факс: +37517 290-84-48 (многоканальный),
+37529 752-39-09 velcom, +37544 752-39-09 МТС
E-mail: info@smartproekt.by
Сайт: www.smartproekt.by
Год основания: 2008 г.
УНП: 190982560
Контактные лица:
- Волнистый Сергей Викторович, управляющий;
- Данилов Михаил Владимирович, коммерческий директор.

Услуги: техническое решение, разработка проектной документации, поставка оборудования, монтажные работы и сопровождение созданных систем безопасности: охранной сигнализации, видеонаблюдения, озвучивания, СКУД и противокражных систем.
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.
Выполненные проекты:
- Отделения ОАО «БПС Сбербанк» в Минске: система видеонаблюдения, СКУД;
- Отделение ОАО «Внешэкономбанк» в Минске: системы видеонаблюдения, СКУД и охранной сигнализации;
- Гипермаркет для детей «Буслик»: в Гродно, Витебске, Могилеве, Гомеле, Лиде, Орше, Минске (система видеонаблюдения, озвучивания, охранной сигнализации, СКУД);
- Магазины розничной торговли «Евроопт» в г. Гродно, г. Витебске, г. Гомеле, г. Могилеве, г. Могилеве (система озвучивания).

Торговые марки:
- AMC (Литва) оборудование для построения систем звуковой трансляции;
- NOVUS (Польша), системы видеонаблюдения.

Сфератрэйд, ОДО

Республика Беларусь, 220118,
г. Минск, ул. Машиностроителей, д. 29, оф. 117
Тел.: +37517 341-50-50, +37529 641-50-50, +37529 541-50-50
E-mail: info@secur.by
Сайт: www.secur.by
Год основания: 1995 г.
УНП: 100972915
Контактные лица: Малаховский Денис Святославович, директор.
Лицензии:
- №02300/50 на право осуществления деятельности по обеспечению пожарной безопасности в части торговли средствами противопожарной защиты. Выдана МЧС Республики Беларусь, действительна до 10.02.2016 г.;
- №02010/209 на право осуществления деятельности по обеспечению безопасности юридических и физических лиц. Выдана Министерством внутренних дел Республики Беларусь, действительна до 15.08.2021 г.

Услуги:
- технические консультации по вопросам обеспечения безопасности любого уровня сложности;

- обследование и экспертная оценка состояния технических средств безопасности на объектах административного, производственного и других назначений;
- составление технического задания и проекта;
- поставка оборудования;
- гарантийное и послегарантийное обслуживание поставляемого оборудования.

Поставка:
- IP и CCTV-системы видеонаблюдения;
- системы контроля и управления доступом;
- системы охранно-пожарной сигнализации;
- системы защиты товаров от краж;
- системы аварийного оповещения и звуковой трансляции;
- сопутствующие материалы для монтажа и др.

Дистрибьютор компаний: AXIOM, MOBOTIX AG (Германия), SALTO Systems S.L. (Испания), , Truen (Южная Корея), ZAVIO Inc. (Тайвань), NUUO (Тайвань), Roger (Польша), KT&C (Южная Корея), Fujifilm (Япония), Pinetron Co (Южная Корея), GSN Electronic (Израиль), Rielta (РФ), LOB (Польша), Elmes Electronic (Польша), QUIKO (Италия), JIS (Испания), PERCo (РФ), ITV|AxxonSoft (РФ), JSB Systems (РФ), AccordTec (РФ), Elesta (РФ), Bolid (РФ) и др.

Унибелус, СП ООО

Республика Беларусь, 220033,
г. Минск, ул. Нахимова, 10
Тел./факс: +37517 291-15-05, 230-72-40
E-mail: info@unibelus.com
Сайт: www.unibelus.by
Год основания: 1994 г.
УНП: 100834637

Контактные лица: Белова Ольга Владимировна, генеральный директор.

Производство: система трансляции и оповещения о пожаре «АРИЯ».

Услуги: от консультации и проектирования до пусконаладочных работ и последующего сервисного обслуживания всех слаботочных сетей.

Поставка: систем пожарной сигнализации, трансляции и оповещения, конференц-связи и синхроперевода, видеонаблюдения, контроля доступа, пожаротушения, профессионального озвучивания, охраны периметра, мультимедийных систем, локально-вычислительных сетей, охранной сигнализации, противокражной системы, системы диспетчеризации, телефония, часофикация, радиофикация, система автоматизации, комплексные интегрированные системы безопасности, системы управления и контроля инженерными сетями зданий.

Дистрибьютор компаний: Arecont Vision (США), Cisa (Италия), Технос-М+ (Россия), CEM Systems Great (Северная Ирландия), Autec (Германия), Openers&Closers (Испания), Aiphone (Япония), Green Center (Чехия), Samsung Techwin (Ю. Корея), JVC Professional Europe (Германия), CBC (Ganz, Computar), AVerMedia Information (Тайвань), Win4net (Ю. Корея), Daiwon Optical (Ю. Корея), Тахион (Россия), TOA (Япония), Tasker (Италия), JTS (Тайвань), DNH (Норвегия), CISCO (США), SRS (Украина), Эталон (Россия), OT-Systems (Гон Конг), КОМКОМ (Россия), Girikond (Россия), Isaberg Rapid (Швеция), Lantech (Тайвань), PELCO (Россия), AV Tech Corporation (Тайвань), Cominfo A.S. (Чехия), Enhance Technology GmbH (Германия), HID Global (Великобритания), Instek Digital Co., Ltd (Тайвань), Lantech Communications Global, Inc. (Тайвань), Mattig-Schauer GmbH (Германия), BFT (Италия), Etrovision (Тайвань), ТД «Паритет» (Россия), Полисервис НПФ ООО (Россия), РостЕвроСтрой (Россия), Риэлта (Россия), ТЕКО (Россия).

Хостер Бай, ООО

Республика Беларусь, 220005,
г. Минск, ул. В. Хоружей, 1А-6 этаж
Тел.: +37517 239-57-03, +37529 309-12-26 (доб. 3),
+37529 861-91-00 (доб. 3)
Сайт: www.hoster.by
E-mail: info@hoster.by
Год основания: 2000 г.

Лицензии:
Специальное разрешение (лицензия) №01019/78 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи. Выдано научно-производственному частному унитарному предприятию «НАДЕЖНЫЕ ПРОГРАММЫ».

Услуги:
Технический администратор доменной зоны .BY, крупнейший в стране регистратор доменов .BY.

Поставка:
Эксклюзивный поставщик защищенного хостинга для государственных органов.

ЭРВИ групп, ООО

РФ, 121471, г. Москва, ул. Рябиновая, д. 45А, стр. 24
Тел./факс: +7495 735-38-47; +7495 735-38-57
Сайт: www.rvi-cctv.by
Год основания: 2007 г.

ОГРН: 1086454000643
ИНН: 6454088952
КПП: 772901001

Контактные лица:
- Рыжков Алексей Владимирович, директор;
- Голубев Антон, руководитель отдела ВЭД.

Производство: полный комплекс продукции для CCTV и IP-видеонаблюдения:
- сетевые камеры видеонаблюдения;
- IP-видеорегистраторы (NVR);
- автономные цифровые видеорегистраторы с сетевыми возможностями;
- аналоговые видеокамеры с цифровой обработкой изображения;
- объективы для видеокамер;
- профессиональные мониторы видеонаблюдения;
- термокожухи;
- видеодомофоны;
- источники питания.

Услуги: поставка (продажа) оборудования, разработка, проектирование и послепродажное обслуживание.

Оборудование в проектах (наиболее значимые):
- Безопасный город Москва (более 40 000 видеокамер в местах массового скопления людей, дворовых территорий, подъездов, площадей, парков и т.д.);
- Государственная программа «Безопасный город»: г. Краснодар, г. Архангельск, г. Астрахань, г. Мурманск, г. Тюмень;
- Безопасный автобус, г. Москва («Мосгортранс», более 4000 автобусов);
- Безопасная школа: 1570 школ по Москве, 67 школ в Хабаровском крае, 51 школа в Сахалинской области, 37 школ в Республике Башкортостан, 50 школ в Воронежской области;
- Более 20 объектов здравоохранения г. Москвы, в том числе Московский родильный дом №17, Клинический родильный дом (г. Астрахань);
- Спецтранспорт МВД: ЦСН, ГИБДД, ППС (более 3000 автомобилей);
- более 1800 а/м инкассации Сбербанка РФ;
- ФСИН: более 400 автозаков;
- более 30 отделений «Сбербанка» РФ (филиалы в городах Москва, Северо-Кавказский ФО, в Астраханской, Саратовской, Белгородской, Калужской, Брянской, Владимирской, Архангельской областях и Краснодарском крае);
- более 40 отделений «ГазЭнергоБанк» в Калужской области;
- Банк «Зенит» (обеспечение системами видеонаблюдения инкассаторских а/м);
- «Газпромбанк» (обеспечение системами видеонаблюдения инкассаторских а/м);
- «Банк Москвы» (обеспечение системами видеонаблюдения инкассаторских а/м).

Дополнительная информация:
«ЭРВИ групп» – это группа управленцев, разработчиков и технических специалистов, деятельность которых направлена на создание более совершенных и адаптированных под задачи государства продуктов, обеспечивающих безопасность, как граждан России, так и различных объектов недвижимости.

Системы видеонаблюдения GRUNDIG -
немецкие технологии и качество

FOR A GOOD **REASON**
GRUNDIG

Для получения более подробной информации посетите
www.grundig-security.com

Официальный дистрибьютор в Республике Беларусь - компания «АльфаСистемы»
г. Минск, Логойский тракт 22а, офис 207
Тел./факс: (+375 17) 262 84 64, 268 05 36 / 265 12 59
info@cctv.by www.cctv.by

УНП 190598104

DIGIEVER

Все функции в одном устройстве DIGISTOR NVR

Совершенное сетевое видеонаблюдение с поддержкой разрешения Full HD и высоким качеством записи

- Поддержка функции мониторинга, удаленного мониторинга через веб-браузер и приложения на базе iOS и Android
- Разработан на базе стабильной и безопасной ОС Linux
- Интуитивно понятный интерфейс для мультиканального воспроизведения
- Быстрая настройка всего в 5 простых этапов
- Надежное управление привилегиями пользователей
- Управление различными происходящими событиями
- Продвинутое управление RAID дисками с возможностью их горячей замены
- Встроенный GPIO порт* (4 цифровых входа и 2 выхода)

СП «Унибелус» ООО официальный представитель DIGIEVER в Республике Беларусь
220033, Беларусь, г. Минск, ул. Нахимова, 10
Тел.:(017) 291 15 05, Факс: (017)230 72 40
GSM: (029) 7777 230, (029) 608 15 05
www.unibelus.by