ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, №3 (24)–2012
В НОМЕРЕ:

ОФИЦИАЛЬНЫЙ РАЗДЕЛ

БАНКОВСКАЯ БЕЗОПАСНОСТЬ. АКТУАЛЬНЫЕ ВОПРОСЫ БАНКОВСКОЙ БЕЗОПАСНОСТИ

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

СРЕДСТВА И СИСТЕМЫ ОХРАНЫ

БАНКОВСКАЯ БЕЗОПАСНОСТЬ. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

БАНКОВСКАЯ БЕЗОПАСНОСТЬ. БРОНЕАВТОМОБИЛИ

БЕЗОПАСНОСТЬ КВОИ (ИБ АСУ ТП)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ. DLP СИСТЕМЫ. ЭКСПЕРТНОЕ МНЕНИЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ. DLP СИСТЕМЫ

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»
Производственно-практический журнал
№ 2 (23) 2012, март-апрель 2012

Периодичность выхода: 1 раз в 2 месяца

Учредитель и издатель:
ООО «АэркомБел»

Главный редактор:
Сергей Адамович Драгун

Над номером работали:
Веременюк Дарья
Лисенкова Анна

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

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

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

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

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

Цена 35000 бел. руб. без НДС,
на основании п. 3.12 ст. 286
Особенной части Налогового Кодекса
Республики Беларусь

Подписано в печать — 21.05.2012 г.
Формат: 60x90 1/8
Бумага офсетная
Гарнитура Myriad Pro. Печать офсетная
Усл. печ. л. 8,5; 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

Банковский сегмент по-прежнему остается одним из самых перспективных с точки зрения выделения бюджетов на инженерно-техническую и информационную безопасность. Во многом этому способствуют международные стандарты, которым обязаны соответствовать банки. Главными угрозами для национального банковского сегмента являются внутренние угрозы, поэтому стабильно растет спрос на средства защиты от утечек информации внутри корпоративной сети. Видна тенденция к созданию банками комплексных систем мониторинга с интеграцией систем безопасности.

На государственном уровне продолжается разработка нормативных актов по защите критически важных объектов информатизации (КВОИ). При ограниченности ресурсов невозможно выстроить равномерную защиту. Защита КВОИ — это эффективный способ концентрации защиты в местах возможного максимального ущерба.

В нормативном регулировании сегмента информационной безопасности происходит процесс накопления количества разработанных документов в качество. Требуют доработки нормативные акты, регулирующие электронный документооборот. Специалисты сетуют на отсутствие национальной системы учета уязвимостей, без которой невозможно повысить качество систем. Учитывая актуальность перечисленных вопросов, эти и другие темы мы планируем обсудить, создав ряд специализированных информационных площадок научно-практических семинаров, посвященных проблемам обеспечения комплексной (информационной и инженерно-технической) безопасности объектов различных категорий.

На период сентябрь-октябрь-ноябрь 2012 г. редакцией запланировано проведение следующих научно-практических семинаров:

1. «ЦОД: повышение технической и экономической эффективности проектирования, внедрения и эксплуатации».
2. «Современные методы и средства обеспечения комплексной безопасности инфраструктуры и процессов «облачных» технологий».
3. «PCI DSS 2.0 и PA DSS 2.0 — требования и методы обеспечения безопасного функционирования платежных систем».
4. «Риски Fraud-мошенничества в деятельности операторов связи».

Приглашаем профильные компании выступить в статусе соорганизатора/партнера запланированных мероприятий. Специалистам предлагаем принять активное участие в экспертном формировании программ и докладов и в качестве слушателей.

Подробнее на сайте **www.aercom.by**

Следующий номер журнала посвящен пожарной безопасности. Рассматриваются вопросы:

Пожарная автоматика — новые средства и системы. Нормирование — основные положения и особенности применения ТКП 263-, 264-, 265-2011. Особенности проектирования пожарной автоматики с учетом изменений №1 в ТКП 45 — 2.02-190-2011. Молниезащита зданий, сооружений и инженерных коммуникаций. Средства и системы огне/био защиты и пр. вопросы.

С уважением, Драгун Сергей Адамович,
главный редактор журнала.

19-я международная выставка и конференция

ОХРАНА, БЕЗОПАСНОСТЬ И ПРОТИВОПОЖАРНАЯ ЗАЩИТА

ufi Approved Event

MIPS MOSCOW

15–18 АПРЕЛЯ 2013 ГОДА
МОСКВА, ВВЦ, ПАВИЛЬОН 75

с 2013 года на ВВЦ!

Охранное телевидение и наблюдение

Технические средства обеспечения безопасности

Пожарная безопасность. Аварийно-спасательная техника. Охрана труда

Защита информации. Смарт карты. ID-Технологии. Банковское оборудование

CARDEX 2013 IT Security

Организатор:

ITE

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

При поддержке:

МВД России

www.mips.ru

Требования Департамента охраны к оборудованию банкоматов и пунктов обмена валют средствами сигнализации и организация охраны

Бураковский Виталий Николаевич, заместитель начальника отдела эксплуатации управления средств и систем охраны, подполковник милиции.

Требования по оборудованию средствами сигнализации и организация охраны пунктов обмена валют (далее — ПОВ) изложены в Инструкции о мерах по защите обменных пунктов Национального банка Республики Беларусь, банков и небанковских кредитно-финансовых организаций от противоправных посягательств, утвержденной совместным постановлением Министерства внутренних дел и Правления Национального банка Республики Беларусь в декабре 2010 года.

Организационные и технические меры по защите ПОВ

Организационные меры

Защита ПОВ от противоправных посягательств определяется локальными нормативными правовыми актами по обеспечению безопасности обменных пунктов банка и включает в себя систему мероприятий. В частности разрабатываются инструкции, устанавливающие порядок действий работников обменных пунктов и работников службы инкассации по обеспечению личной безопасности и безопасности банковских ценностей в различных ситуациях; порядок осуществления в течение рабочего времени обменного пункта контроля со стороны руководства банка или уполномоченных руководителем банка или филиала работников банка за физическим состоянием работников обменного пункта, соблюдением ими требований по обеспечению личной безопасности, безопасности банковских ценностей и (или) осуществлению мониторинга за обстановкой в непосредственной близости от обменного пункта; порядок допуска внутрь конструкции обменного пункта проверяющих лиц и лиц, осуществляющих техническое обслуживание технических средств и систем охраны; порядок осуществления учета и контроля фактов передачи работниками обменных пунктов, иными уполномоченными работниками банка друг другу комплекта ключей от обменного пункта и сейфов, установленных внутри конструкций обменных пунктов, а также электронных идентификаторов и иных технических средств охраны, периодичность или условия, при которых в целях обеспечения условий для безопасного функционирования обменного пункта должны быть осуществлены смена кодов электронных идентификаторов и (или) замена замков от входной двери конструкции обменного пункта либо сейфа, установленного внутри конструкции обменного пункта.

Технические меры по защите ПОВ

Технические меры по защите обменных пунктов от противоправных посягательств включают систему мероприятий по обеспечению технической укрепленности конструкций обменных пунктов и сейфов, размещенных внутри них, оснащению их инженерно-техническими средствами защиты и техническими системами охраны.

Сигнализация

Каждый обменный пункт, за исключением передвижных обменных пунктов, подлежит обязательному оснащению: системой охранной сигнализации; ручной системой тревожной сигнализации; системой охранного телевидения.

Передвижные обменные пункты подлежат обязательному оснащению ручной системой тревожной сигнализации. По решению руководителя банка либо его филиала передвижные обменные пункты дополнительно могут оснащаться системами охранной сигнализации и системами охранного телевидения.

Вывод сигналов с установленных в обменных пунктах, в том числе в передвижных обменных пунктах, систем охранной сигнализации и ручной системы тревожной сигнализации: в зонах дислокации подразделений Департамента охраны должен осуществляться только на ПЦН; вне зон дислокации подразделений Департамента охраны может осуществляться на ПЦН либо иным способом, определенным законодательством Республики Беларусь.

Обменные пункты оборудуются системами охранной сигнализации для обеспечения охраны банковских ценностей во время обеденного и технологических перерывов (в периоды отсутствия работников обменных пунктов на рабочих местах), а при необходимости — для охраны обменных пунктов в нерабочее время.

Тактика оборудования конструкций обменных пунктов, внутреннего пространства, образованного ими, и установленных в них сейфов системами охранной сигнализации зависит от специфики осуществления их охраны, определяемой месторасположением обменного пункта и наличием иных условий, влияющих на эффективность его охраны.

Оборудование обменных пунктов, охрана которых обеспечивается только во время обеденного и технологических перерывов, системами охранной сигнализации осуществляется следующим образом: двери блокируются на

открытие; ограждающие строительные конструкции оборудуются объемными извещателями для обеспечения блокировки всей поверхности этих конструкций; кондиционеры в моноблочном исполнении, установленные внутри конструкций обменных пунктов, не закрепленные изнутри обменного пункта предусмотренным заводом-изготовителем способом или не защищенные снаружи инженерно-техническими средствами защиты, блокируются на выем, сейф блокируется на открытие магнитоконтактными извещателями.

Технические средства охраны дверей, кондиционера в моноблочном исполнении с объемными извещателями, сейфа подключаются к ППКО отдельными шлейфами сигнализации.

Необходимость оборудования других элементов обменного пункта (например, индивидуальной кабины для обслуживания клиентов, тамбура при входе в конструкцию обменного пункта) техническими средствами охраны, выделяемыми из системы охранной сигнализации периметра конструкции обменного пункта, указывается в техническом задании на проектирование технической системы охраны обменного пункта (далее — техническое задание).

Система охранной сигнализация должна обеспечивать возможность быстрой и безопасной сдачи конструкции обменного пункта под охрану с помощью установленного внутри нее пульта управления ("клавиатуры") или устройства доступа с программированием приемно-контрольного прибора на задержку срабатывания технических средств охраны. Минимально возможное время задержки срабатывания технических средств охраны определяется индивидуально для каждого обменного пункта в зависимости от местных условий и указывается в техническом задании.

Тактика оборудования обменных пунктов средствами ручной тревожной сигнализации должна обеспечивать возможность подачи сигнала тревоги работником обменного пункта как изнутри, так и снаружи обменного пункта (при входе или выходе из конструкции обменного пункта). В связи с этим обменные пункты в обязательном порядке должны оборудоваться: стационарными (проводными) тревожными извещателями (кнопками или педалями в зависимости от конструкции обменного пункта); беспроводными тревожными извещателями (радиобрелоками).

Дополнительно, при необходимости, обменные пункты оборудуются автоматическими тревожными извещателями, в том числе выполняющими также функции химических ловушек.

Тип используемых тревожных извещателей (например, ручной, ножной, с фиксацией или без нее, автоматический с химической ловушкой или без нее) указывается в техническом задании.

Контроль за состоянием ручной системы тревожной сигнализации обменных пунктов должен осуществляться как в период работы обменного пункта, так и в периоды обеденного и технологических перерывов.

Системы охранного телевидения (СОТ)

Обменные пункты оборудуются системами охранного телевидения в целях обеспечения безопасности работников обменных пунктов, работников службы инкассации и клиентов, сохранности банковских ценностей, осуществления контроля за соблюдением работниками обменного пункта и клиентами установленных правил осуществления банковских операций, контроля за обстановкой в непосредственной близости от мест расположения обменных пунктов, установления фактов (деталей фактов) участия клиентов в совершении банковских операций, установления и фиксирования фактов совершения противоправных посягательств и изображений лиц, их совершивших.

СОТ обменного пункта может быть: локальной, при которой все технические средства СОТ размещаются в помещении обменного пункта; сетевой, при которой видеосигналы передаются по каналам связи на удаленное автоматизированное рабочее место (далее — АРМ) для оперативного контроля за обстановкой в обменном пункте и вокруг него и видеозаписи событий.

Сетевые СОТ нескольких обменных пунктов, в свою очередь, могут объединяться в сети на уровне банков или их филиалов.

СОТ обменного пункта должна обеспечивать: выполнение целевой задачи по идентификации личности всех входящих в обменный пункт; контроль работниками обменного пункта в режиме реального времени обстановки в непосредственной близости от обменного пункта, и прежде всего перед входной дверью и перед передаточным узлом, с выполнением целевой задачи по различению объекта наблюдения; видеозапись и аудиозапись обстановки в обменном пункте, в том числе на рабочих местах работников обменного пункта (по решению банка); видеозапись изображений от телекамер на цифровые видеорегистраторы со скоростью не менее 5 кадров в секунду с разрешением, позволяющим обеспечить выполнение целевых задач каждой из телекамер в периоды работы обменных пунктов, обеденных и технологических перерывов, а также, при необходимости, в нерабочее время (например, по сигналам обнаружителей движения или средств охранной сигнализации); хранение записанной видеоинформации в течение не менее 7 суток; резервирование СОТ по питанию в течение не менее 0,3 часа; возможность санкционированного считывания видеоинформации (копирования на внешние носители) стандартными средствами.

Для идентификации человека изображение лица должно занимать не менее 30 процентов высоты экрана монитора (кадра) при разрешении не менее 450 телевизионных линий по горизонтали. При использовании IP-камер размер фронтального изображения головы человека по ширине должен занимать не менее 240 пикселей, что примерно соответствует изображению расстояния между глаз взрослого человека в 120 пикселей.

Для обнаружения человека его изображение должно занимать не менее 10 процентов высоты экрана монитора (кадра), при разрешении телекамеры не менее 450 телевизионных линий по горизонтали или, при использовании IP-камер, не менее 576 пикселей по вертикали.

При наличии у работника обменного пункта возможности с помощью панорамных дверных глазков, зеркал, видеодомофонов и иных приспособлений осуществления контроля за обстановкой в непосредственной близости от обменного пункта в целом или возле выхода из него допускается не производить с помощью СОТ видеозапись и контроль обстановки перед входной дверью.

При подготовке технического задания целевые задачи должны устанавливаться для каждой из телекамер или группы телекамер, выполняющих одну целевую задачу. В техническом задании в обязательном порядке должны указываться: режим видеозаписи, скорость видеозаписи, время хранения видеоинформации, требования к программному обеспечению, а также тип канала связи для передачи видеосигналов на АРМ (при его наличии).

В темное время суток, при тумане либо во время выпадения осадков для обеспечения номинальных условий работоспособности СОТ при просмотре и регистрации изображений с внешних телекамер должны предусматриваться либо искусственное освещение территории, непосредственно примыкающей к обменному пункту, либо подсветка объектов наблюдения, находящихся на наблюдаемой территории, в инфракрасном диапазоне (в зависимости от типов применяемых телекамер).

Основные технические решения по СОТ должны предусматривать организационные и технические меры, предотвращающие несанкционированный доступ к оборудованию СОТ, настройкам телекамер, режимам записи видеоизображения и управления периферийными устройствами системы, а также к архивам видеозаписи.

Обеспечение безопасности банкоматов

В 2009 году Департаментом охраны разработаны требования по оборудованию банкоматов средствами сигнализации и организации их охраны распространяются на банкоматы и технические устройства по приему наличных денег (далее — банкоматы), передаваемые под охрану подразделениям Департамента охраны Министерства внутренних дел Республики Беларусь (далее — подразделения охраны) или средства сигнализации которых подключаются на пульты централизованного наблюдения подразделений охраны для контроля.

Сейфовая часть принимаемых под охрану банкоматов должна выгораживаться перегородками (кроме случаев размещения банкомата в отдельном помещении) с целью блокировки средствами охранной сигнализации подступов к банкомату и защиты инкассаторов в период заправки банкоматов.

К перегородкам, стенам, дверям не предъявляются требования по технической укрепленности, их основная задача — обеспечить возможность блокировки подступов к сейфам банкоматов с помощью объемных извещателей.

В случае невозможности выгораживания сейфовой части банкомата перегородками, допускается принимать под охрану банкоматы при условии повышения оснащенности сейфа банкомата средствами охранной сигнализации и защищенности средств сигнализации от саботажа.

При принятии банкоматов под охрану должны в обязательном порядке предусматриваться организационные мероприятия по обеспечению осмотра банкомата группами задержания в случае срабатывания средств сигнализации и перезакрытию объекта охраны (совместно с заявителем определить порядок доступа на объект за счет истребования ключей от объекта, договоренности с арендатором о его выезде на объект для перезакрытия и т.п.).

При расположении банкомата в отдельном помещении или в случае выгораживания сейфовой части банкомата блокируются средствами охранной сигнализации: двери (роллеты) — на открытие (подъем); объем помещения (выгородки); сейф банкомата — ловушкой из магнитоконтактного извещетеля (на открытие двери) и вибрационных извещателей типа «Шорох-2» или «Vibro» (на пролом).

Вибрационные извещатели могут быть заменены блокировкой внутренних поверхностей сейфа фольгой (оклейкой), монтируемой на пластины из токонепроводящего материала.

Вибрационные извещатели настраиваются с учетом функционирования при вибрации, возникающей при работе механизма выдачи денег («Шорох-2» переводится в режиме II, «Vibro» калибруется в обучающем режиме при работе механизма выдачи денег).

Для усиления охраны в выгороженном помещении скрыто устанавливается кнопка подтверждения снятия из-под охраны. Кнопка подтверждения может также устанавливаться внутри корпуса банкомата. Время нажатия кнопки, программируемое в приемно-контрольном приборе, определяется исходя из особенностей помещения, размещения устройства доступа и конструктивных особенностей банкомата.

Отдельно стоящие банкоматы блокируются следующим образом: двери сейфа — на открытие магнитоконтактным извещетелем; стенки сейфа — сейсмическими извещателями типа GM 730, GM 760 или вибрационными «Шорох-2» (один — на дверь, остальные — на стенки) в режиме регистрации воздействия газорежущего и электродугового инструмента.

В зависимости от типа банкомата при высоком уровне вибрации, создаваемой механизмом выдачи денег для предотвращения срабатывания сейсмических извещателей из электронного блока банкомата на вход извещателей выводится сигнал (+5 В), появляющийся при формировании команды на запуск механизма выдачи денег, для уменьшения чувствительности сейсмических извещателей на время выдачи денег. При срабатывании вибрационного извещателя «Шорох-2» в режиме I (в режиме регистрации воздействия газорежущего и электродугового инструмента) при работе механизма выдачи денег его использование не допускается.

Количество устанавливаемых сейсмических и вибрационных извещателей определяется размерами сейфов и радиусом действия извещателей на блокируемой поверхности.

Монтаж сейсмических и вибрационных извещателей в сейфах производится в соответствии с рекомендациями производителей.

При блокировке банкоматов приемно-контрольные приборы могут устанавливаются внутри сейфа, внутри оболочки банкомата, снаружи оболочки банкомата или на стене.

В случае установки приемно-контрольного прибора вне блокируемого сейфа отдельностоящего банкомата должна быть произведена защита шлейфов сигнализации от саботажа.

При установке приемно-контрольного прибора на стене в выгороженном пространстве (помещении) от саботажа защищается шлейф блокировки сейфа банкомата. Для защиты от саботажа допускается использование металлорукавов.

Для привлечения внимания сигнал о срабатывании средств сигнализации должен дополнительно выводиться на светозвуковой оповещатель. ■

Вопросы организации системы безопасности банкоматов

Баталин Евгений Олегович, заместитель директора по техническим системам безопасности компании «Марко-Плюс»

Справка ТБ

Баталин Евгений Олегович. Образование высшее, окончил маниностроительный факультет БГПА в 2001 году. Работал в НП ООО «Акова» электромонтером связи, инженером-наладчиком, начальником участка. С 2007 — в службе безопасности ОАО «Приорбанк». С 2010 работает в ООО «Марко-Плюс» в должности заместителя директора по техническим системам безопасности.

Компания «Марко-Плюс» специализируется на установке и техническом обслуживании систем банковского самообслуживания (СБС): банкоматов, платежно-справочных терминалов и др. Одно из направлений работы компании — обеспечение безопасности объектов банковской инфраструктуры (установка и ТО систем безопасности: СВН, СКУД, охранной сигнализации и пр.). На обслуживании у компании находится порядка 340 банкоматов, 180 ПСТ и 2600 POS-терминалов. Штат специалистов сегмента физической безопасности 17 человек. Клиенты компании — ОАО «Приорбанк», ОАО «Белвнешэкономбанк», ЗАО «МТБанк», ЗАО «Цептер Банк», ЗАО "Трастбанк", ОАО «БПС-Сбербанк», ЗАО "Сомбелбанк", ЗАО «Кредэксбанк», ЗАО «Белорусский Банк Малого Бизнеса», ОАО «Газпромбанк», ЗАО «Альфа-Банк» и др.

ООО «Марко-Плюс» имеет большой наработанный опыт по монтажу, наладке и техническому обслуживанию систем безопасности банков и устройств банковского обслуживания. С недавнего времени специалисты компании ведут разработку собственного нормативного документа, определяющего порядок, установку средств и систем безопасности, порядок мониторинга и регламент ТО для банкоматов и платежных терминалов. О проблематике сегмента мы говорили с заместителем директора по техническим системам безопасности компании «Марко-Плюс» Баталиным Евгением.

Как Вы можете оценить достаточность нормативной базы, определяющей работы по установке, мониторингу и регламенту ТО банкоматов и платежных терминалов?

Существующая нормативная база описывает правила проектирования, монтажа и технического обслуживания для охраняемых объектов, передаваемых под охрану подразделениям Департамента охраны Министерства Внутренних дел Республики Беларусь. Для нас, как компании специализирующейся на банковском сегменте, существующих нормативных документов недостаточно, хотелось бы видеть правила оборудования банкоматов и ПСТ системами видеонаблюдения, системами контроля и управления доступом. Перечислять можно сколь угодно много. Я еще не видел документов, которые подробно описывали состав и порядок оборудования этих устройств, порядок организации системы мониторинга, кто и как должен организовывать процесс мониторинга, требования к каналам связи и пр. Нам такой регламент необходим, т.к. в случае ЧП или проверки, должен быть документ, четко разделяющий зоны ответственности и требования к оборудованию. Поэтому руководство нашей компании приняло решение разработать собственный стандарт (регламент), который описывает всю проблематику, возникающую при работе с устройствами банковского самообслуживания и который объединяет все в систему. Документ находится на стадии разработки.

Какие нормы, документы изучали и берете за основу при создании собственных регламентов?

За основу берем европейские стандарты (CEN) EN 1143-1, COBIT, ISO/IES 17799, ISO/IES 15408, российские стандарты ГОСТ Р 51558-2000 «Системы охранные телевизионные. Общие технические требования и методы испытаний». Отправной точкой были действующие нормативные документы Республики Беларусь, которые обусловливают общие положения. Принципиальные моменты — отсутствие расхождений с законодательством Республики Беларусь и прописанные технические требования не ниже существующих национальных норм. Для начала это будет внутренний регламент компании, затем планируем согласовать его с Департаментом охраны МВД для применения на объектах охраняемых подразделениями Департамента охраны МВД Республики Беларусь.

Основные разделы Вашего документа?

Общие положения будут содержать ряд правил и условий, обязательных к исполнению всеми участниками процесса, правила и порядок разработки технического задания, правила и порядок производства работ, тактико-технические характеристики устанавливаемого оборудования (не привязываясь к конкретным маркам), правила приёмки работ, порядок и правила технического обслуживания. При выборе оборудования предусмотрен индивидуальный подход к каждому заказчику. Планируется форма заявки на установку, где заказчик опционно сможет выбирать, какие блоки, узлы, функционал, системы ему необходимы в том или ином устройстве. Например, если банкомат находится в неохраняемой торговой точке, соответственно, предусмотрены самые жесткие условия его защиты, максимальная комплектация систем; если банкомат находится в охраняемом помещении банка с круглосуточным постом, то его защита минимальна.

Системы видеонаблюдения

Согласно существующим нормам банковские объекты поделены на зоны. В зависимости от зоны прописываются требования, решаемые

СВН в определенной зоне наблюдения: идентификация, различение, обнаружение и пр.; определяется, какой процент экрана должен занимать объект. В нашем регламенте мы также делим объект на зоны: охраняемая-неохраняемая, банковский/небанковский объект, т.д.

Мониторинг и снятие видео

Работоспособность банкомата контролируется круглосуточно, а в общем круглосуточный видеомониторинг возможен, но в нем нет необходимости. Обязательно будем прописывать требования по удаленному мониторингу и съему видеоинформации посредством организации GSM-канала, либо какого-то другого. Зачастую физически сложно приехать и снять запись с удаленных объектов, даже несмотря на прописанное по договору время реагирования и собственную сеть обслуживания.

Регистраторы

Пока используем аналоговые регистраторы с возможностью удаленной настройки, IP системы пока для банкоматов слишком дороги.

Время хранения

Есть разные требования: Департамент охраны требует минимум 7 дней, пожелания заказчиков от 30. Мы планируем хранить запись не менее 30 суток.

Обеспечение электропитания банкоматов

Больших проблем нет, как частные случаи — в ряде торговых объектах, где стоят банкоматы, на ночь обесточивается помещение, приходится ставить более мощный блок питания и чаще менять аккумуляторы.

Дополнительные технические средства защиты

Некоторые банкоматы в местах повышенного риска защищаются роллетами. Но, как правило, стараемся выбирать места установки банкоматов с минимальными рисками.

Охранные извещатели

Используются извещатели «Шорох-2». В принципе, работают хорошо, ложных сработок нет. По цене демократичны.

С Вашей точки зрения, хранение видео «в облаках» перспективно?

Основная проблема в такой схеме — защита информации. Должна быть отдельная сеть, не связанная с банковской, иначе система не будет соответствовать требованиям PCI DSS. Думаю, услуга по хранению видеонаблюдения «в облаках» будет востребована на удаленных объектах не банковского профиля с минимальными требованиями к безопасности объектов.

Ваше мнение по поводу сдачи банкоматов под охрану Департамента охраны?

Считаю, здесь проблема в крайне сложной организации процесса. К примеру, ситуация: произошла ночью сработка извещателя в банкомате. Выезжает группа. Должен быть дежурный сервисной службы для открытия аппаратной части банкомата; для того, чтобы зайти в сейфовую часть — инкассация; ответственный хозорган. Слишком много ответственных для одного банкомата, а если пересчитать на количество банкоматов и вероятность ложных срабатываний, получаются астрономические цифры. Для того, чтобы соблюсти требование нормативных документов по охране банкоматов подразделениями Департамента охраны, зачастую требуется возвести целую строительную конструкцию, в которой будет находиться непосредственно банкомат.

Проблемы установки внутри банкоматов сторонних устройств

Есть проблема в части размещения видеокамер. На старых моделях была проблема поставить регистратор, т.к. были установлены электронно-лучевые мониторы, занимающие много места, сейчас мониторы — жидкокристаллические, места хватает. Необходимо внимательно подходить к выбору регистратора, тестировать его на работу в жару. Внутри банкомата из-за работы печки высокие температуры, в т. ч. и зимой.

Что касается видеокамер, штатные, которые идут в банкоматах, не всегда обеспечивают различение человека, который подходит к устройству для выполнения транзакций. Одна камера не дает достоверную информацию. Есть дополнительные системы: счетчики, журналы, показывающие статистику, но тогда уже не остается места для камер — приходится заказывать дополнительные корпуса для видеокамер.

Беседовал Драгун Сергей

Требования PCI DSS к платежным системам и терминалам

Таран Дмитрий, специалист компании Softline

Первый банкомат появился осенью 1996 года, сегодня банкоматы стали универсальным инструментом для осуществления платежей. Однако вместе с ростом использования карточек увеличилось и количество мошеннических операций с их использованием.

Для борьбы с мошенничеством такого рода крупнейшие мировые платежные системы (Visa, Mastercard, Discover) создали отраслевой стандарт PCI DSS (Payment Card Industry Data Security Standard). Стандарт содержит требования по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Требования этого стандарта должны быть строго выполнены в процессинговых центрах, где обрабатываются данные платежных карт, и рекомендуются к выполнению банкам-эмитентам, выпускающими пластиковые карты.

Кроме требований PCI DSS банки используют и другие меры защиты банкоматов, информации по транзакциям, а также противодействия мошенникам.

Проблематика соблюдения требований PCI DSS в Республике Беларусь.

На текущий момент, в РБ должны соответствовать PCI DSS (по требованию VISA к октябрю 2011 года) 3 финансовых организации: Белорусский процессинговый центр, ОАО «Приорбанк», ОАО «Банк БелВЭБ». Основная проблематика приведения всех процессов обеспечения информационной безопасности в соответствие с PCI DSS заключается в необходимости реорганизации в компаниях существующей системы разграничения и контроля доступа к информации (ресурсам), выделении дополнительного финансирования для требуемой организации защиты ИТ-инфраструктуры и чувствительных данных.

С другой стороны, в банке могут быть внедрены все необходимые процессы по обеспечению безопасности данных платежных средств, и де-факто соответствовать PCI DSS, но все равно должно быть прохождение сертификации на соответствие стандарту. Сертификацию не проходят, так как на поддержание процессов обеспечения безопасности и на проведение аудита соответствия нужно ежегодно выделять финансирование.

Основные требования PCI DSS к ИТ-инфраструктуре и процессам обеспечения ИБ:

PCI DSS определяет 12 основных требований по 6 направлениям безопасности, которые должны осуществляться в организации:

• Построение и сопровождение защищённой сети

1. Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт.

2. Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности.

• Защита данных держателей карт

3. Обеспечение защиты данных держателей карт в ходе их хранения.

4. Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети.

• Поддержка программы управления уязвимостями

5. Использование и регулярное обновление антивирусного программного обеспечения.

6. Разработка и поддержка безопасных систем и приложений.

• Реализация мер по строгому контролю доступа

7. Ограничение доступа к данным держателей карт в соответствии со служебной необходимостью.

8. Присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре.

9. Ограничение физического доступа к данным держателей карт.

• Регулярный мониторинг и тестирование сети

10. Контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт.

11. Регулярное тестирование систем и процессов обеспечения безопасности.

• Поддержка политики информационной безопасности

12. Разработка, поддержка и исполнение политики информационной безопасности.

Особенности применения требований PCI DSS по защите банкоматов.

Защита банкоматов состоит из двух компонентов — защиты физической и защиты информационной. Основные составляющие информационной защиты — это безопасная среда передачи и шифрования данных (пункт 4), необходимость использования антивирусного обеспечения (пункт 5), ограничение доступа к банкоматам сотрудникам только в соответствии со служебной необходимостью (пункт 7).

Физическая защита банкоматов направлена на обеспечение сохранности наличных денежных средств.

Стандарт PCI DSS в основном направлен на организацию процессов обеспечения информационной безопасности в отрасли платежной индустрии и не

содержит конкретных рекомендаций по техническим средствам и мерам.

Белорусские банки организуют меры по информационной защите либо на основе собственных инструкций, либо на основе рекомендаций международных стандартов PCI DSS, ISO 27001, ITIL, СТО БР ИББС и т.д. Зачастую в банке организованы меры по защите и канала связи, и антивирусная защита, и другие меры, но они не находят отражения в локальных документах, так как из-за высокой нагрузки на ИТ-персонал организации, сотрудники не имеют возможности заниматься формализацией нормативных документов.

Защита канала связи с банкоматами.

Для защиты канала связи организуются выделенные каналы связи (банкомат-банк), используются средства VPN, обеспечивается шифрование данных на уровне "банкомат-процессинговый центр". Для разграничения доступа к приложениям банкомата используется межсетевое экранирование и средства контроля целостности программного обеспечения банкомата.

Правильная организация указанных мер позволят полностью обезопасить устройство от захвата злоумышленниками и перехвата потока данных держателя пластиковых карточек и информации по транзакциям. Мошенники почти не используют перехват и взлом информации по каналам связи, так как при шифровании информации получить доступ к ней практически невозможно.

Каналы связи, используемые в банкоматах РБ: Wi-Fi, GSM, Ethernet.

Банки, по мере возможности используют Ethernet, а резервные каналы на текущий момент переводят на 3G. Размещать банкоматы предпочитают в ЦБУ, дополнительных офисах и прочих защищенных помещениях. При установке терминалов в торговых точках, используют GSM, CDMA, GPRS.

Преимущественно используется Ethernet, резервные каналы на текущий момент переводят на 3G.

Есть проблемы в использовании медленных каналов связи (CDMA, GPRS — у них невысокая пропускная способность), но это не влияет на защиту банкомата, а создает трудности в работе самого банкомата.

Защита от мошенничества (скимминга).

Широкое использование у мошенников получило использование накладок на банкомат. Через накладку на картоприемник считывается информация пластиковой карточки, а накладка на клавиатуру (или используется миниатюрная видеокамера) позволяет узнать pin-код карточки владельца. В дальнейшем полученная информация используется для записи на заготовки пластиковых карточек (белый пластик) и снятия наличности через терминалы.

В последнее время банки начали выпускать пластиковые карты со встроенным чипом, что повышает степень защиты карточек и не позволяет использовать «белый пластик», но пока повсеместного распространения они не получили.

Такие карточки стоят дороже обычных, и клиент сам может выбирать какую карточку он хочет использовать. Проблема заключается в том, что дополнительная защита чипованной карточки реализуются не во всех банкоматах, а только в тех, которые имеют возможность делать дополнительную проверку по чипу. Из-за высокой стоимости банкоматов, банки не спешат менять парк терминалов, а действуют постепенно, например, с открытием новых офисов покупают новые банкоматы.

В России и Украине процесс перехода на «чипованные» карточки проходит тоже постепенно в связи с вышеуказанными причинами.

Защита программного обеспечения банкоматов.

Киберпреступники также используют вредоносное программное обеспечение для получения доступа к банкомату (вирусы и трояны). Но как утверждают производители банкоматов, это невозможно без участия сотрудников, обслуживающих банкомат. Поэтому в качестве дополнения к брандмауэру в банкоматах используются антивирусы или системы контроля целостности файлов.

Также с антивирусами может использоваться IPS (Intrusion Prevention System) — система предотвращения вторжений. Она не требует обновлений, поддерживая систему в заведомо рабочем состоянии, и не позволяет запускаться приложениям, которые не занесены в список доверенных. Решения, относящиеся к IPS, защищают также и память устройства, что предотвратит атаки типа «Переполнение буфера обмена».

Банки самостоятельно решают использовать или нет системы IDS/IPS (системы обнаружения/предотвращения вторжений), эти системы используются в основном в комплексе с антивирусом. В нашей стране чаще используются следующие системы IDS и антивирусы: Kaspersky, Symantec, Trend Micro, Dr.Web

Есть также специализированный софт, который предлагают производители банкоматов как альтернативу антивирусам.

Для предотвращения случаев сговора мошенника с сотрудником, обслуживающим банкоматы, банки вводят контрольные процедуры, например контроль обслуживания терминала сотрудником безопасности. Если банкоматы обслуживает сторонняя организация, контроль может осуществляться сотрудником банка.

В целом в Республике Беларусь защита банкоматов находится на высоком уровне.

Информзащита
Системный интегратор

Стандарты в информационной безопасности: панацея или плацебо?

Бабенко Алексей Андреевич, старший аудитор ЗАО НИП «Информзащита»

Справка ТБ

Бабенко Алексей Андреевич окончил факультет прикладной математики и кибернетики Томского Государственного Университета. Старший аудитор Департамента консалтинга и аудита компании «Информзащита», область компетенций — аудит и консалтинг в области приведения в соответствие со стандартами PCI DSS, PA-DSS, ИББС СТО БР, ISO 27001, требованиями 152-ФЗ, безопасности web-технологий. В 2010 году получил статус Qualified Security Assessor, в 2011 — Payments Application Qualified Security Assessor. Активный участник и спикер на различных конференциях, посвященных информационной безопасности. Участник команды SiBears в соревнованиях CTF. В свободное время предпочитает заниматься спортом (баскетбол, джиу-джитсу) и чтением книг.

Стремительное развитие информационных технологий в наши дни вслед за несомненными удобствами привело к появлению новых видов мошенничества и киберпреступлений. По пятам развития ИТ следует информационная безопасность. Приятная тенденция последнего времени — рост понимания ее важности и необходимости. Не последнюю роль в этом играют находящиеся на слуху громкие компрометации информационных систем, в один момент приносящие колоссальные финансовые потери. В отдельных случаях они и вовсе могут привести к необратимым для бизнеса последствиям. В результате, защита информации становится не столько делом организации, сколько критерием надежности для ее партнеров и клиентов.

Стандарты информационной безопасности призваны помочь компании создать требуемый уровень защиты информации, а так же являются критериями измерения уровня текущей защищённости и эффективности процессов управления информационной безопасностью. Кроме национальных стандартов на территории стран СНГ имеют достаточную известность два международных: стандарт ИБ ISO/IEC 27000 и стандарт безопасности данных инфраструктуры платежных карт PCI DSS.

Стандарты серии ISO/IEC 27000, разработанные и опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC), содержат рекомендации к системе управления информационной безопасностью. Сертификация осуществляется на основе требований, описанных в стандарте ISO/IEC 27001, и производится только аккредитованными компаниями-аудиторами.

Выполнение требований стандарта в странах СНГ не носит обязательный характер, поэтому его распространенность достаточно низкая. На апрель 2012-го года число компаний, обладающих действующими сертификатами соответствия ISO/IEC 27001, в странах СНГ составляло 21. Для сравнения, в Японии, где для ряда компаний сертификация обязательна, 4061 организация обладает действующим сертификатом. При этом стоит отметить, что общее количество компаний в СНГ, внедривших стандарты серии 27000, гораздо выше, поскольку множество организаций, осуществивших внедрение, ставят своей целью не сертификацию, а четко выстроенные процессы управления и подержания уровня информационной безопасности.

Стандарты серии 27000 часто являются первым шагом в развитии систем управления информационной безопасностью. Их использование в качестве ориентира — хорошая практика, которая позволяет построить эффективную систему менеджмента информационной безопасности.

Payment Card Industry Data Security Standard (PCI DSS, Стандарт безопасности данных индустрии платежных карт) был создан Советом по безопасности индустрии платежных карт (PCI SSC), организованным по инициативе пяти крупнейших мировых платежных систем — Visa, MasterCard, JCB, American Express и Discover. Основной целью создания стандарта являлось обеспечение единого уровня информационной безопасности для всех участников индустрии, обеспечивающей обслуживание платежных карт. Безопасность является одним из главных критериев при использовании технологий, связанных с финансами. Поэтому организация защиты данных платежных карт одна из приоритетных задач каждой платежной системы.

В отличие от стандартов серии 27000, стандарт PCI DSS обязателен для применения всеми организациями, обрабатывающими платежные карты. При этом требования к оценке соответствия зависят от суммарного объема обработанных транзакций: от самостоятельной оценки до прохождения сертификационного аудита. Последний проводится компанией, имеющей статус PCI QSA.

Еще одним существенным отличием PCI DSS является его большая детализация. При выполнении требований ISO 27001 защитные меры выбираются по результатам оценки рисков информационной безопасности и их достаточность оценивается сотрудниками организации. При реализации PCI DSS конкретные решения уже определены, а «маневр», в большинстве случаев, допускается только при выборе реализующих технологий.

Кроме того, что платежные системы Visa и MasterCard ввели требования по обязательному соответствию стандарту PCI DSS, были обозначены крайние сроки приведения к соответствию. Это привело к тому, что большинство крупных игроков индустрии платежных карт проделали работу по выполнению требований. В результате, это отразилось на общем уровне защищенности как отдельных участников, так и всей индустрии безналичной оплаты.

Стоит отметить, что стандарт может быть использован организациями, не связанными с индустрией платежных карт, при планировании системы информационной безопасности. Стандарт на постоянной основе обновляется и содержит актуальные меры и рекомендации по снижению угроз информационной безопасности.

Применение стандартов и соответствие их требованиям, несомненно, является хорошей практикой и большим шагом вперед при выстраивании системы информационной безопасности. Однако сам факт соответствия не всегда прямо пропорционален уровню защищённости. Для подтверждения можно вспомнить пример с компрометацией информационной системы крупнейшей в мире розничной сети Wal-Mart, которая на момент инцидента имела действующий сертификат соответствия PCI DSS. Объяснением такому факту могут служить несколько причин. Во-первых, сертификация осуществляется после проведения аудита, который представляет собой оценку состояния на текущей момент времени. В течение года, на который распространяется действие сертификата, в компании перестают работать процедуры, сделанные «для галочки», с целью пройти проверку. Во-вторых, не исключена ошибка самих аудиторов в определении области проверки, состава проверяемых компонентов и общих выводах.

Наконец, всегда стоит помнить, о том, что идеальной безопасности не бывает, и обеспечение безопасности — это постоянный процесс защиты от новых угроз. Стандарты не «волшебная пилюля», а лишь полезный инструмент в достижении максимального уровня защиты.

The Intelligent Surveillance Solution

Компания NUUO (продукты, разработки)

Справка ТБ:

Компания NUUO (Тайвань), основанная в 2004 году, по праву считается одним из мировых лидеров в разработке программных решений для систем интеллектуального видеонаблюдения. Профессиональные решения для видеонаблюдения NUUO, основанные на одновременной поддержке аналоговых и сетевых камер — гибридной технологии с системой интеллектуального поиска IVS, гарантировали компании успешный выход на рынок индустрии безопасности. Продукция NUUO проста и легка в установке, имеет удобный графический интерфейс и открытую платформу: совместима с камерами различных мировых производителей сетевого видеонаблюдения, таких как MOBOTIX, 3S, ZAVIO, VIVOTEK, ACTi, ArecontVision, Axis, Beward, D-Link, Dynacolor, Etrovision, EverFocus, Levelone, Lumenera, Panasonic, PiXORD, Planet, Samsung, Sony, Toshiba, и др. (более 1500 моделей).

Синьмэй, менеджер по продажам на территории России и СНГ.

Компания NUUO принимала участие в выставке MIPS-2012 в Москве, благодаря чему нам удалось подготовить интервью с Синьмэй, менеджером по продажам на территории России и СНГ.

Кем, когда и как создавалась компания NUUO?

Компания NUUO была создана на Тайване в 2004 году 3 друзьями. Один из них, инженер-программист, создал софт, который сейчас называется NVR IP+. Изначально это был простой софт без особых функций. Можно сказать, что компания NUUO — это разработчик программного обеспечения для интеграции систем видеонаблюдения. NUUO созвучно с английским «new», что означает новый. Офис находится в городе Тайбэе, столице Тайваня, на территории института иноваций при Тайваньском Государственном университете. Непрерывное сотрудничество NUUO и института инноваций в сфере новых технологий позволило NUUO познакомиться с лучшими студентами-программистами страны, многие из которых работают в компании по сей день.

Кроме разработки софта, какое оборудование производите?

Мы являемся производителем двух линеек сетевых видеорегистраторов — NUUO NVRmini 2 и NUUO Titan NVR. Первая линейка разработана для простых объектов до 16 сетевых видеокамер, вторая — для сложных больших объектов, требующих высокую производительность от сетевого видеорегистратора. NUUO Titan NVR может обрабатывать до 64 видеокамер и поддерживает максимальное разрешение 5 Мп. Так же NUUO производится несколько линеек плат видеозахвата NUUO DVR, которые при помощи программного ключа можно объединить с сетевой системой NVR IP+ в единую оболочку ПО — NUUO Tri-Brid System, тем самым получив гибридную систему из аналоговых и сетевых камер. А так как платы видеозахвата поддерживают аналоговые камеры высокого разрешения, получается система «трибридная».

NUUO большая компания?

NUUO — сплоченная команда, которая состоит из более 150 профессионалов, включая лучших инженеров-разработчиков, квалифицированных инженеров по обслуживанию клиентов, многонациональную команду руководителей, менеджеров по маркетингу и связям с общественностью. Торговая марка NUUO хорошо известна в области безопасности благодаря надёжности, производительности и использованию новых технологий. Продукция компании NUUO установлена в более 94800 проектах в 65 странах мира.

В каких основных нишах используются продукты NUUO (промышленность, коммерческий сектор, частные владения)?

Оборудование NUUO используется для проектов самых разнообразных отраслей: общественного транспорта, образования, правительственного сектора, банков, гостиниц, здравоохранения, казино и промышленных объектов.

В каких регионах NUUO наиболее широко известна и хорошо представлена?

Особо высокий спрос на нашу продукцию в США, Африке, Тайване. Сейчас активно занимаемся продвижением в России и странах СНГ.

Дайте краткую характеристику собственным продуктам?

Надежные, стабильные, высокопроизводительные и простые в использовании. Отличное соотношение цены и качества. Хорошо прописанный софт сводит количество ошибок к минимуму.

Вы поддерживаете стандарт ONVIF?

Безусловно, мы поддерживаем ONVIF, а также более 1500 моделей камер, не работающих в этом стандарте. К нашим регистраторам можно подключить практически любую камеру.

С какими линейками камер работает Ваше ПО?

Наше ПО поддерживает сетевые камеры всех ведущих мировых производителей, а также любые аналоговые камеры. Так же разработан отдельный продукт для камер Full HD (1920x1080) — плата видеозахвата SCB-8004HD.

Есть ли установки Вашего ПО на КВО (критически важные объекты)?

Существуют инсталляции на Тайване и в других странах. Но это конфиденциальная информация.

Есть ли у компании патенты на собственные разработки?

Мы создали новую технологию для ускорения записи, основанную на собственной файловой системе. Она называется File Ring. Система File Ring создана с нуля специально для работы с записями высокого разрешения. Она изменяет порядок записи и воспроизведения видеопотоков с жестких дисков, благодаря чему способна обрабатывать огромное количество данных, например, одновременно записывать до 64 камер (с разрешением 2 Мп) на видеорегистраторе Titan (H.264, 15 кадров/с, средний трафик).

Какую сертификацию прошла продукция NUUO?

Продукция прошла обязательную сертификацию ГОСТ — в России, CE — в Европе, KCC, FCC — в других странах.

Какие решения по видеоаналитике есть в Ваших продуктах?

Сейчас работаем над модернизацией технологии видеоаналитики IVS. На этом уровне у нас реализован интеллектуальный поиск в архиве, интеллектуальная реакция на тревоги. Когда появляется угроза, на экране отображается место, где происходит событие, и отправляется электронное сообщение на сервер, SMS- на телефон, звуковое оповещение. Когда нет сигнала от камеры, также по-

является предупреждение. Помимо этого, ведутся разработки в направлениях идентификации номеров автомобилей и распознавания лиц. Всего в ПО NVR IP+ применяется более 10 типов видеодетекторов и сценариев по видеоаналитике. Например, пропавший объект, незнакомый объект, потеря фокуса камеры, детекция движения и т.д. К концу году количество функций будет увеличено.

Существуют ли в продуктах компании инструменты защиты потокового видео от модификаций в центрах мониторинга (т.н. цифровая подпись)?

Да. Международный протокол MD5.

Есть инструменты защиты потокового видео?

Есть, например, программа, проверяющая, были ли изменения записи, которая называется «Verification tool». Это программа встроена во все наши продукты.

На каких операционных системах работают Ваши платформы?

Серверы написаны на платформах Windows, Linux. Клиенты серверов же работают на операционных системах Windows и Mac.

Маркетинг. Расскажите о дилерах компании и принципах формирования партнеров?

Мы тщательно подходим к выбору партнеров. Количество наших представителей зависит непосредственно от размера страны. Например, в Беларуси у нас только один официальный представитель — Группа компаний «Сфера». ГК «Сфера» работает в сфере безопасности с 1995 года и имеет богатый опыт. В этом году у нас подписан официальный контракт.

Как развиваются продажи в России?

В России мы начали работать не так давно, однако спрос на нашу продукцию уже достаточно большой.

Планы и тенденции развития компании?

IP-системы развиваются очень быстро. Сейчас мы работаем над интеграцией других систем безопасности на базе нашей платформы, например СКУД, распознавание номерных знаков автомобилей и др. систем.

Какие новинки представляете на выставке для России, Беларуси?

Из новинок мы представляем мощный сетевой видеорегистратор TitanNVR в настольном и стоечном исполнении, причем в стоечном — одно- и двухвысотным. Скорость записи 250 Мб/с, с возможностью подключения до 64 сетевых камер по 2 Мп каждая (максимально поддерживаемое разрешение — 5 Мп), внутри можно установить 4/8 съемных дисков по 3 Тб, также можно подключать внешний накопитель. Формат компрессии H264, MJPEG, MPEG-4, MxPEG.

Беседовал Драгун Сергей

Группа компаний «Сфера»
220118, г. Минск,
ул. Машиностроителей, 29-117
Тел./факс: (17) 341-50-50
info@secur.by
www.secur.by

УНП: 100972915

Решение задач по обеспечению комплексной безопасности Банков и Финансовых учреждений на базе системы VideoNet

Котов Дмитрий Викторович, начальник отдела проектных решений

На сегодняшний день обеспечение безопасности деятельности банковских и финансовых учреждений невозможно представить без комплексных мер, направленных на решение задач:

– по сохранению своих собственных активов;
– предотвращению краж материальных ценностей;
– предотвращение мошеннических действий с пластиковыми картами клиентов;
– защиту банкоматов от грабителей и вандалов;
– минимизацию рисков репутационных потерь при разборе спорных ситуаций с клиентами банка.

Кроме того, система безопасности должна обеспечивать возможность централизованного мониторинга, управления и просмотра архива с любой точки, где есть канал связи. В условиях, когда филиальная сеть крупных банков достигает нескольких сотен отделений и тысячи банкоматов и платежных терминалов, справиться с подобной задачей способны немногие.

О системе VideoNet

Система безопасности VideoNet уже много лет успешно применяется в этой отрасли бизнеса, постоянно развиваясь, предоставляя пользователям всё новые технологии для повышения уровня безопасности и качества проводимого онлайн и пост-анализа.

Система VideoNet имеет множество наград, среди которых: Диплом за «Лучший инновационный продукт» 2006/2009/2010 годов; Первое место номинации «Охранное телевидение и наблюдение» 200/2003/2011 годов. В 2004 году цифровая система безопасности VideoNet стала победителем Национальной отраслевой премии по безопасности «ЗУБР» в номинации «Лучший продукт в области CCTV (видеонаблюдения)», а в 2005 — победителем той же премии в номинации «Лучший продукт для обеспечения безопасности банков».

Среди постоянных потребителей системы VideoNet и решений на её основе: Сбербанк России (8 территориальных отделений), ВТБ-24, Газпромбанк, Банк Санкт-Петербург, Промстройбанк, Банк «Россия» и многие другие.

Во многом этот успех достигается благодаря постоянным инвестициям в развитие системы VideoNet, техническим инновациям, наличию большого опыта работы в этой отрасли и высококвалифицированным кадрам, способных создавать решения любой сложности с учётом индивидуальных особенностей Банка и финансового учреждения.

Система VideoNet может обеспечить безопасность всей структуры Банка, начиная от центральных офисов, до банкоматов и инкассаторских машин. Существующие специализированные решения Bank-Defender и Bank-Defender ATM позволяют обеспечить длительный срок хранения архива при высочайшем качестве изображения.

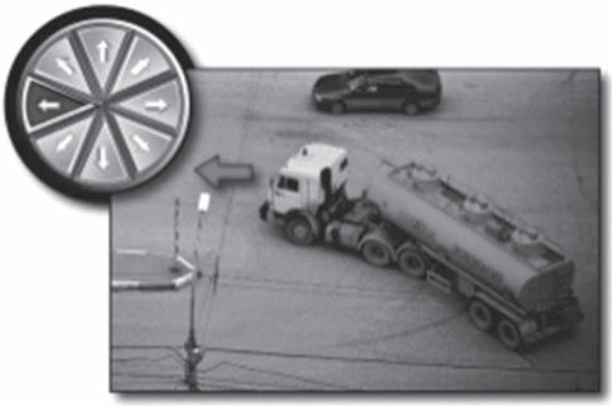
Технологии системы VideoNet в банковской сфере

Повышение эффективности охраны Банка невозможно без использования современных аналитических алгоритмов, призванных контролировать как внешние угрозы, так и внутренние; сосредоточив усилия на решении главных задач, отсекая всю второстепенную информацию. Именно такие уникальные алгоритмы применяются в системе VideoNet.

Внедрение на объектах Банка видеоаналитики системы VideoNet даст следующие преимущества:

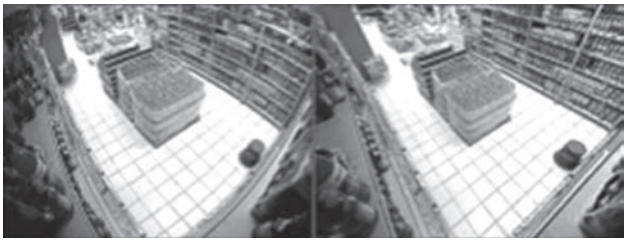
Детектора саботажа — позволяет контролировать не только действия людей, пытающихся вывести часть системы из строя путём отворота камеры, расфокусировки, закрытия объектива и пр., но и естественные помехи: запотевание объектива, потеря полезного сигнала.

Адаптивный детектор объектов — позволит контролировать внутреннюю территорию и помещения банка, сигнализируя службу безопасности обо всех подозрительных движениях в нерабочее время или в запретной зоне. Данный детектор особенно эффективно использовать в уличных камерах, т.к. его алгоритм устойчив к естественным помехам, таким как дождь, снег, колебания веток на ветру и пр.



Детекторы направления / пересечения — заложенные в эти детекторы алгоритмы позволяют эффективно решать задачи контроля за перемещением объектов в зоны ограниченного доступа как по пересечению зоны, так и по направлению этого пересечения.

Счетчик объектов — в некоторых случаях позволяет контролировать количество прошедших через зону контроля людей. Это так же может быть эффективным инструментом внутреннего контроля служб безопасности.



Фильтры ImageStabilizer и LensCorrection — корректируют естественные колебания уличной или внутренней камеры и сферические искажения, вызванные применением широкоугольных объективов.

Детектор звука — позволяет генерировать тревогу в случае появления шума, превышающего допустимую норму (например хлопок, удар и пр.)

Обработка изображения

В основе обработки и записи изображения в видеостанциях VideoNet заложен уникальный потоковый алгоритм компрессии, разработанный специалистами нашей компании — DVPack 2.0™ способный обрабатывать любые разрешения, вплоть до 5 Мп. Кодек DVPack 2.0™ оптимизирован с применением процессорных технологий SSE2/SSE3/SSSE3;

Основные преимущества кодека DVPack 2.0™

- Низкий размер кадра в сравнении с другими известными кодеками
- Высокое качество компрессированного изображения
- Высокое быстродействие

Возможности системы VideoNet в решениях для банков

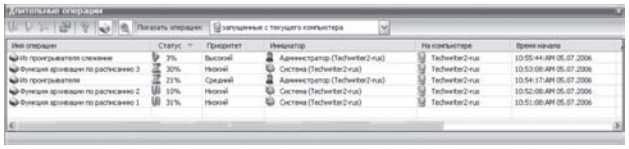
Интеграция с банкоматами и счетчиками банкнот

С целью качественного разбора спорных ситуаций с клиентами банка при работе с банкоматами, платежными терминалами или в рассчетно-кассовых узлах в системе VideoNet предусмотрены технологии внедрения текстовой информации (титров) в видеоряд, поступающей от программного обеспечения банкомата, счетчиков или сортировщиков банкнот. Такая

информация становится неотделимой частью изображения, что позволяет в дальнейшем использовать её как прямое доказательство в суде. Система VideoNet интегрирована с банкоматами всех лидеров рынка: NCR, Diebold, Wincor/Nixdor.

Сохранение конфиденциальной информации о карте клиента является важной составляющей репутации Банка. В системе VideoNet существует возможность создавать «невидимые» для системы участки изображения (зоны), что исключает просмотр PIN-кода, если клавиатура банкомата попадает в зону видимости камеры

Архивация и экспорт



Важной особенностью системы VideoNet является возможность как ручного, так и автоматического копирования или переноса данных на видеостанцию(и) долговременного хранения, а так же экспорт в avi формат для предоставления данных руководству или в правоохранительные органы. Данные операции осуществляются в фоновом режиме с возможностью контроля состояния, назначения приоритетов, запуска и остановки операций практически на любых каналах связи. Кроме того, экспорт в avi формат можно производить с автоматической записью на CD/DVD диск.

Система устойчивого мониторинга

Для создания централизованных постов наблюдения с большим количеством мониторов, подчиняющихся центральной видеостанции, была создана новая технология — «Сетевая матрица». Технология позволяет объединить мониторы на

множестве рабочих мест, участников сети VideoNet в единое информационное поле, представляющие для оператора головной видеостанции многомониторную конфигурацию, полностью ему подчиненную. Оператор получает возможность управлять режимами отображения на других мониторах системы, используя одну клавиатуру/мышь/пульт.

Несомненно, высокие технические характеристики и наличие различных инновационных технологий выгодно отличают продукт VideoNet от большинства других систем безопасности и видеонаблюдения. Однако и это не всё, на что стоит обратить внимание, потому как локализация, поддержка и сопровождение продукта являются важными факторами успешной работы системы безопасности на объекте. Быть в постоянном контакте с производителем, регулярно обновлять продукт, открывая доступ к новым техническим достижениям, получать консультации и технические решения от производителя для реализации самых сложных задач — всё это возможно прямо сейчас.

Краткий перечень преимуществ применения системы VideoNet для банков и финансовых учреждений:

1. Низкая стоимость хранения информации.
2. Автоматизация процесса контроля работоспособности камер, гарантия получения «полезного» сигнала, снижение затрат на обслуживание системы безопасности.
3. Организация получает гарантию сохранности данных клиента от доступа к ним обслуживающего персонала.
4. Организация получает достоверную видеоинформацию о проводимых клиентом действиях, факте получения денег и т.д. Полученная из VideoNet видеозапись может быть принята судом в качестве прямого доказательства.
5. Служба безопасности организации имеет возможность оперативно получить доступ к любой камере, подключенной к системе и видеоархиву по ней, не выезжая на удаленный объект.
6. Бесплатные обновления продукта и готовые решения от Корпорации «СКАЙРОС».

Построение системы на базе системы VideoNet позволит максимально повысить эффективность работы служб безопасности и предотвратить возможное нанесение ущерба организации.

Корпорация «СКАЙРОС»
www.skyros.ru; www.videonet.ru

Представительство
в Республике Беларусь
ООО «СТАЛВИСКОМ»
220007, г .Минск, ул. Володько, 12-102
Тел./факс: (017) 205-48-24
E-mail: sale@stalviscom.by
www.stalviscom.by

УНП: 191194104

3-6 СЕНТЯБРЯ
МИНСК, ПР-Т ПОБЕДИТЕЛЕЙ 20/2, ФУТБОЛЬНЫЙ МАНЕЖ,

20-Я МЕЖДУНАРОДНАЯ СТРОИТЕЛЬНАЯ ВЫСТАВКА

БУДПРАГРЭС 2012

> ГЕНЕРАЛЬНЫЙ ИНФОРМАЦИОННЫЙ ПАРТНЕР

МАСТЕРСКАЯ СОВРЕМЕННОЕ СТРОИТЕЛЬСТВО

Стройка Stroyka.by

подробнее

Дополнительную информацию можно найти на сайте www.budpragres.minskexpo.com

> ОФИЦИАЛЬНЫЕ ИНТЕРНЕТ-ПАРТНЕРЫ

ВАШ ДОМ TUT.BY www.vashdom.tut.by

дом.by

РУССТРОЙ интернет портал www.russtroy.ru

> ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

АС Архитектура и строительство

2012

Жилой интерьер

Загородный дом

Композит XXI век

Инфо Форум

Из рук в руки недвижимость

MEGA Stroy.by

Строительные товары Беларуси

Технологии безопасности

Знак Качества

МажорДом

Web Прораб

www.wtsport.by Оконный портал WINPORT

Строительная газета

> ОРГАНИЗАТОР

МинскЭкспо

тел.: (+375 17) 226 98 90

факс: (+375 17) 226 91 92

e-mail: budpragres@telecom.by

Распределенная система IP видеонаблюдения от EverFocus

Евдокимов Сергей Александрович,
региональный менеджер компании
EverFocus Electronics Corp.

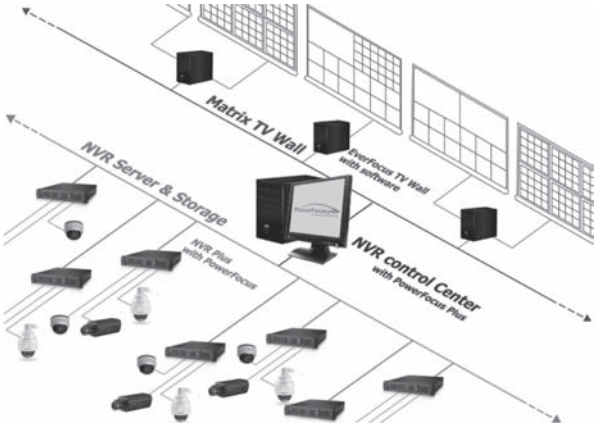
При построении системы видеонаблюдения на территориально распределенных объектах (банк, торговая сеть) очень важно наличие ЦОДа (центра обработки данных) с возможностью централизованного администрирования всей системы. Распределенную систему наиболее эффективно реализовать на базе IP видеонаблюдения.

IP видеонаблюдение от EverFocus позволяет решить задачи различной сложности и масштаба, обеспечив при этом гибкость, надежность и полнофункциональность системы.

Новая серия мегапиксельных камер EDN2210, ETN2110, EQN2171 и EQN2110 предназначена для установки в небольших офисах и помещениях (например, РКЦ) и максимально оптимизирована для обзорного видеонаблюдения. Серия оснащена встроенными Wi-Fi модулями, двусторонним аудиопотоком, встроенными микрофонами и динамиками, записью на micro SD карту, ИК подсветкой и поддержкой PoE. Все камеры имеют мегапиксельные объективы с фиксированным фокусом и углами обзора до 90°.

Для локальной записи видео на объекте используется бесплатное программное обеспечение — PowerFocus, которое устанавливается на промышленный сервер NVR Plus. PowerFocus — это сетевой менеджер для записи, просмотра и администрирования до 64 IP-камер одновременно. Создание мультиэкранов, привязка к загружаемым картам, различные режимы записи, многоуровневый доступ, управление IP PTZ устройствами. Реализована поддержка всех моделей IP-камер и IP-серверов EverFocus. Для увеличения объема хранения данных возможно подключение к серверу внешнего iSCSI RAID массива.

Ниже приведена структурная схема распределенной системы с неограниченным количество серверов и IP камер.



В центре обработки данных на отдельный ПК (сервер) устанавливается комплект платного программного обеспечения для центрального администрирования неограниченного числа NVR и IP камер — **PowerFocus Plus**. Для стабильной работы программы необходимо предусмотреть следующие параметры сервера: процессор Intel I7, 8Gb RAM, Gigabit Ethernet, объем жесткого диска не менее 80Gb.

PowerFocus Plus
for Network Video Recording

Особенности PowerFocus Plus:

- Поддержка неограниченного числа NVR
- Настройка неограниченного числа удаленных мониторных матриц (TV Wall)
- Полное управление уровнями: IP камера/ NVR/ TV Wall/ Удаленный клиент
- Встроенная видеоаналитика (подсчет проходов, виртуальная черта, детектор оставленных предметов)
- Удаленный сетевой доступ (клиент-Viewer) к разрешенному NVR
- Поддержка всех IP камер, IP серверов и NVR EverFocus
- Поддержка ONVIF
- Аудиоканал
- Четыре способа настройки записи (события, обычный, расписание, ручной)
- Цифровой ZOOM в реальном времени и при просмотре архива
- Многоуровневая и гибкая настройка политики безопасности
- Просмотр архива в мультиэкране (1-4)
- Настраиваемый интерфейс и мультиэкран до 64 окон
- Лицензионный USB ключ
- Разделение и управление всеми транслируемыми потоками с любой IP камеры и IP сервера
- Встроенный видеоконвертер для быстрого копирования архива (WMV)
- Поддержка всех IP PTZ камер EverFocus
- Поддержка пульта управления USB EKB200
- Настраиваемый SMPT сервер сообщений
- Резервное копирование настроек
- Загрузка файла карты объекта, расстановка и быстрый доступ к видео

Основным достоинством данной распределенной системы является ее гибкость: приобретая лицензию на PowerFocus Plus (лицензия на один ЦОД), пользователь имеет возможность добавлять к существующей системе неограниченное количество IP камер и серверов. Поддержка ONVIF и модули видеоаналитики делают PowerFocus Plus сильным инструментом в построении сложных систем видеонаблюдения.

EverFocus Electronics Corp.
12F, No.72, Sec.1, Shin-Tai Wu Rd, Taipei, Taiwan
Тел.: (29) 355-66-45
E-mail: sergey@everfocus.com.tw
www.everfocus.by

Официальный дилер
СООО «САТУРН-ИНФО»
220015, г. Минск, ул. Пономаренко, 35а, офис 616
Тел./факс: (017) 251-62-06; 256-25-23
(029) 656-17-50, (029) 756-17-18
E-mail: saturn@saturn-info.com
www.saturn-info.com

УНП: 100063951

В «Интеллект» интегрирована СКУД SALTO

Компания ITV | AxxonSoft произвела интеграцию системы контроля и управления доступом SALTO ProAccess SHIP в программный комплекс «Интеллект».

В результате интеграции список поддерживаемого «Интеллектом» оборудования включил беспроводные автономные и управляемые по радиоканалу электронные замки и цилиндры, онлайн (IP) и оффлайн контроллеры СКУД SALTO, электронные замки для шкафчиков и стеклянных дверей, а также специализированные решения SALTO для дверей эвакуационных выходов с устройствами «Антипаника».

Интеграция СКУД SALTO в программный комплекс «Интеллект» позволила:

- получать в «Интеллекте» события от СКУД SALTO, осуществлять программируемую реакцию на них в рамках интегрированной системы безопасности;
- синхронизировать списки сотрудников системы «Интеллект» с базой данных СКУД SALTO;
- видеть статус оборудования SALTO на поэтажных планах «Интеллекта», управлять этим оборудованием;
- осуществлять удаленную фотоидентификацию входящих при помощи системы видеонаблюдения, а также выполнять другие алгоритмы работы в рамках интегрированной системы безопасности.

СКУД SALTO

Беспроводная СКУД SALTO предназначена для комплексного решения задач организации контроля и управления доступом в помещения и на объекты любого типа и назначения. СКУД SALTO — простая и вместе с тем безопасная, не нуждается при развертывании в прокладке кабелей, в замене дверей и замков, установленных ранее. Монтаж и обслуживание системы требуют минимальных временных и материальных затрат.

СКУД SALTO позволяют объединить в одной системе классические проводные (IP) контроллеры доступа и инновационные электронные замки и цилиндры SALTO, как автономные, так и работающие в режиме реального времени по радиоканалу. Помимо этого, СКУД SALTO может включать специализированные устройства доступа для дверей эвакуационных выходов (с устройствами «Антипаника»), для цельностеклянных дверей, замки для шкафчиков и кабин, а также специальные энергосберегающие устройства, благодаря которым в единую СКУД можно включить любое устройство с питанием от электросети.

Использование сертифицированных алгоритмов шифрования для всей информации, передаваемой СКУД SALTO как по локальной сети, так и по беспроводному каналу, а также применение наиболее безопасных современных перезаписываемых RFID-носителей с аппаратной поддержкой криптографии данных делают СКУД SALTO одной из самых безопасных и надежных систем на рынке, полностью исключающей возможность манипуляций с данными или картами пользователей (клонирование карт).

Программный комплекс «Интеллект»

Программный комплекс «Интеллект» позволяет объединить разрозненные системы — ОПС, СКУД, видеонаблюдение и многие другие — в согласованно работающую инфраструктуру. Благодаря «Интеллекту» комплекс разрозненных систем безопасности превращается в единую информационную среду, обладающую способностью гибко реагировать на различные события.

О компании SALTO Systems

Разработчиком и производителем систем SALTO является испанская фирма SALTO Systems. Компания была основана в 2001 году с амбициозной целью создания новой концепции автономных систем контроля доступа. Сейчас электронные системы SALTO установлены более чем на 1 000 000 дверей в 7500 проектах в 70 странах мира. Среди объектов SALTO — гостиницы и офисные центры, государственные учреждения и университеты, аэропорты и конгресс-центры, санатории и госпитали, небольшие офисы и штаб-квартиры транснациональных корпораций.

О компании ITV | AxxonSoft

Образованная в 2003 году, компания ITV | AxxonSoft на сегодняшний день является крупнейшим разработчиком программного обеспечения для систем безопасности и видеонаблюдения в России. В компании работает более 250 специалистов, она насчитывает 29 офисов и представительств в России и за рубежом и более 2000 компаний-партнеров — инсталляторов и интеграторов систем безопасности и видеонаблюдения. Также ITV | AxxonSoft сотрудничает с ведущими российскими и мировыми производителями оборудования для систем безопасности.

Продукты компании служат основой решений в области обеспечения безопасности дорожного движения, железнодорожных перевозок, снижения потерь в розничной торговле, безопасности сетей банкоматов, сетей автозаправочных комплексов и во многих других сферах. Флагман продуктовой линейки ITV | AxxonSoft, многофункциональная программная платформа «Интеллект», используется, в частности, для создания систем класса «Безопасный город», которые внедряются более чем в 80 городах в России и за рубежом.

Официальным представителем компаний SALTO Systems S.L., Spain и ITV | AxxonSoft РФ в Беларуси является группа компаний «Сфера».

ГК «Сфера» имеет опыт успешной работы более 15 лет в качестве проводника как инновационных, так и зарекомендовавших себя решений в сфере безопасности.

Источник: www.saltosystems.ru

Беларусь 220118 г. Минск
ул. Машиностроителей 29-117 (5 этаж)
Тел./факс: +375 (17) 341 50 50
Velcom: +375 (29) 641 50 50
МТС: +375 (29) 541 50 50
E-mail:info@secur.by
www.secur.by

СИСТЕМЫ БЕЗОПАСНОСТИ ОрионПроект

Адресная подсистема охранной сигнализации в ИСО «Орион»

Развитие систем охранного видеонаблюдения и их широкая популяризация в последние годы отодвинули «в тень» проблематику обнаружения нарушителя с помощью традиционных охранно-тревожных извещателей. Однако, несмотря на значительные результаты, достигнутые разработчиками видеосистем в части видеоаналитики, автоматизации принятия решений и повышения чувствительности и разрешающей способности видеокамер, охранные извещатели во многих случаях остаются незаменимым техническим средством.

Путилин Игорь Павлович, заместитель Генерального директора по маркетингу

Вспомним несколько важных достоинств охранных извещателей:

– широкий перечень физических принципов обнаружения, позволяющий строить многорубежную систему охраны и выбрать наиболее эффективное решение под конфигурацию охраняемой зоны и условия эксплуатации;

– автоматическое обнаружение, исключающее человеческий фактор;

– высокая степень защищенности от саботажа, особенно в случае скрытой установки;

– формирование простых помехозащищенных сигналов тревоги с передачей по двухпроводным линиям связи на большие расстояния;

– относительно невысокая стоимость, особенно для приборов с установкой внутри помещений.

В зависимости от требуемой точности обнаружения места проникновения нарушителя применяются неадресные и адресные системы охранной сигнализации (ОС). В неадресных системах точность обнаружения определяется совокупностью охранных зон (т.е. защищаемых областей), контролируемых одним шлейфом сигнализации (ШС). В адресных системах место проникновения нарушителя определяется с точностью до места установки извещателя и его зоны чувствительности.

Преимущества адресных систем охраны

Адресные системы охраны, несмотря на более высокую начальную стоимость и сравнительно меньшую длину шлейфов сигнализации, обладают рядом важных преимуществ:

– определение места и способа проникновения;

– защита от подмены извещателя,

– невозможность умышленного шунтирования выходных контактов реле;

– питание извещателей по двухпроводной линии связи, без дополнительных источников питания,

– локализация короткозамкнутых участков шлейфа сигнализации с сохранением работоспособности остальных участков,

– возможность объединения нескольких адресных зон в локальный раздел охраны,

– визуализация места обнаружения нарушителя на планах охраняемых помещений.

Основные подходы к организации адресной ОС в ИСО «Орион»

В интегрированной системе охраны ИСО «Орион» адресная система охраны строится на базе контроллера двухпроводной линии связи С2000-КДЛ и широкой номенклатуры адресных извещателей и устройств (рис.1). Рассмотрим основные подходы к организации адресной ОС в ИСО «Орион».

На первом рубеже охраны для контроля проникновения через оконные и дверные проемы можно применить адресный охранный магнитоконтактный извещатель С2000-СМК, в том числе его модификацию С2000-СМК «Эстет» для металлических дверей. Усилить контроль на этом рубеже можно с помощью адресного поверхностного звукового извещателя С2000-СТ, предназначенного для обнаружения разрушения остекленных поверхностей, или создав зону обнаружения в виде «шторы» около дверного проема с помощью извещателя С2000-ШИК. Для обнаружения попытки проникновения посредством разрушения строительных конструкций устанавливается вибрационный извещатель С2000-В. Его чувствительный элемент способен одинаково хорошо обнаруживать разрушение стен из бетона, кирпича, дерева и ДСП.

Второй рубеж традиционно оснащается оптико-электронными извещателями с линзами Френеля. Много лет пользуются заслуженной популярностью недорогие, эффективные, с привлекательным дизайном приборы С2000-ИК и С2000-ПИК. Они имеют разные принципы монтажа — на стену и на потолок, что позволяет подстроиться под особенности формы помещений и внутренней обстановки. В объемной зоне действия «инфра-красных» оптико-электронных извещателей могут быть различные помеховые факторы, а так же возможность попытки проникновения в зонах под местом установки извещателя. Эти случаи учтены в модификациях прибора С2000-ИК: вариант С2000-ИК исп. 02 «игнорирует» присутствие мелких животных, а С2000-ИК исп. 03 имеет дополнительную «антисаботажную» зону обнаружения — непосредственно под извещателем.

Адресный совмещенный извещатель С2000-СТИК по принципу «2 в 1» позволяет одновременно контролировать объем охраняемого помещения и разрушение стекла, находясь как бы на границе двух условных рубежей охраны. Удобство применения таких приборов очевидно — экономия провода, упрощение монтажных работ, удобство обслуживания и эксплуатации.

На третьем рубеже для защиты металлических сейфов в ИСО «Орион» так же можно использовать С2000-В. Кроме этого, он может эффективно применяться для обнаружения взлома банкоматов.

Для формирования тревожного сообщения о нападении или грабеже в арсенале имеется тревожная кнопка «С2000-КТ». Ее скрытая установка и применение позволит вовремя вызвать сотрудников службы безопасности в таких случаях.

Логика работы адресной системы

Логика работы адресной системы такова. «С2000-КДЛ» опрашивает подклю-

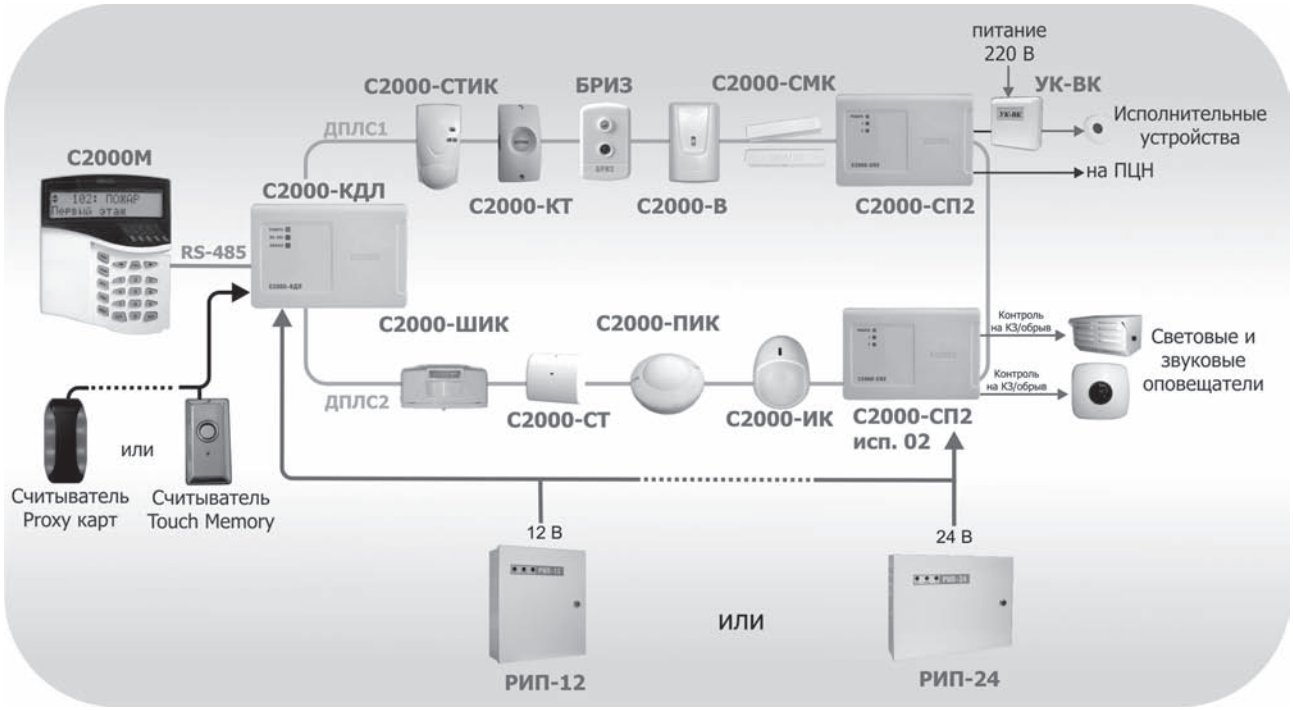


Рисунок 1. Адресная система охранной сигнализации

ченные к нему адресные устройства, и, когда извещатель обнаруживает нарушения контролируемой зоны (например, размыкание магнитоконтактного извещателя), он формирует тревожное извещения для «С2000-КДЛ», который принимает его и передаёт далее сетевому контроллеру (пульту и/или АРМу) информацию о соответствующем событии («Тревога входа», «Тревога проникновения»).

Для управления световыми и звуковыми оповещателями или для передачи тревожных сообщений на пульт централизованного наблюдения могут использоваться адресные сигнально-пусковые блоки «С2000-СП2» с двумя релейными выходами. Алгоритм работы любого релейного выхода можно запрограммировать, задавая программу работы и привязку к событию в системе. Для передачи тревожных сообщений на ПЦН, работающий по протоколу Contact ID, в ИСО «Орион» могут использоваться приборы передачи извещений по проводным и беспроводным линиям связи: С2000-ИТ, УО-4С, С2000-Ethernet, которые подключаются к системной магистрали RS-485 .

При необходимости в адресную линию контроллера «С2000-КДЛ» можно включать адресные расширители (С2000-АР2 и С2000-АР8), которые могут контролировать обычные неадресные извещатели с питанием от отдельного источника. Один С2000-КДЛ может контролировать до 127 адресных извещателей и других устройств, подключенных к его двухпроводной адресной линии связи (ДПЛС).

Однако достоинства ИСО «Орион» не ограничиваются наличием широкой номенклатуры приборов обнаружения нарушителя. В системе досконально продуманы и поддержаны сервисные функции: протоколирование событий, управление зонами охраны, интеграция разных подсистем безопасности.

Как известно, объекты различаются по назначению. Отсюда возникают отличия в алгоритмах постановки системы сигнализации на охрану и снятия с охраны. Эти процедуры не должны противоречить основным бизнес-процессам, быть, по возможности, удобными и простыми. С другой стороны, они должны учитывать специфику объекта и местную криминальную обстановку. Кроме этого, тревожные сигналы от охранной сигнализации могут передаваться на различные системы централизованного мониторинга — пульты охраны. С учетом этого в ИСО «Орион» предусмотрены 4 разных типа охранных шлейфов и широкий перечень программ работы релейных модулей (14 различных алгоритмов).

Осуществлять управление адресной системой охранной сигнализации можно как с пульта С2000М, так и с помощью ключей или Proxy-карт посредством соответствующего считывателя, подключенного к контроллеру двухпроводной линии «С2000-КДЛ». В память «С2000-КДЛ» можно занести до 512 кодов пользователей. К контроллеру можно подключать любые считыватели в протоколах Dallas Touch Memory или Wiegand (например, Считыватель-2, С2000-Proxy, Proxy-2A, Proxy-3A и т.д.).

Типы адресных зон в зависимости от вида подключаемых извещателей

В зависимости от типа подключаемых извещателей любой адресной зоне может быть присвоен один из четырех типов:

• «Охранный» — используется в зонах с отсутствием риска саботажа, с применением извещателей, не имеющих встроенного контакта контроля вскрытия корпуса. Тревожное сообщение формируется сразу после срабатывания извещателя. Поддерживается временная задержка при постановке на охрану.

• «Охранный с распознаванием нарушения блокировочного контакта извещателя» — полностью аналогичен «охранному» ШС, но имеет дополнительную функцию — контроль вскрытия корпуса извещателя. Это позволяет организовать защиту извещателей от саботажа. Например, в дневное время, когда шлейф снят с охраны, злоумышленник не сможет незаметно вскрыть корпус и повредить чувствительный элемент — будет сформировано тревожное сообщение.

• «Охранный входной» — используется в случае, если точка управления снятием с охраны находится внутри защищаемого помещения. Пользователю дается возможность после открывания входной двери и обнаружения этого нарушения извещателем дойти до считывателя и снять систему с охраны. Таким образом, для этого типа ШС предусмотрена задержка перехода адресной зоны охраны в тревогу после обнаружения ее нарушения.

• «Тревожный» — предусмотрен для подключения тревожных кнопок, которые устанавливаются в скрытых местах. При нарушении извещателя зона переходит в состояние «Тихая тревога», при котором сообщение передается без включения звуковой сигнализации.

Вспомогательным типом шлейфа сигнализации может быть «технологи-

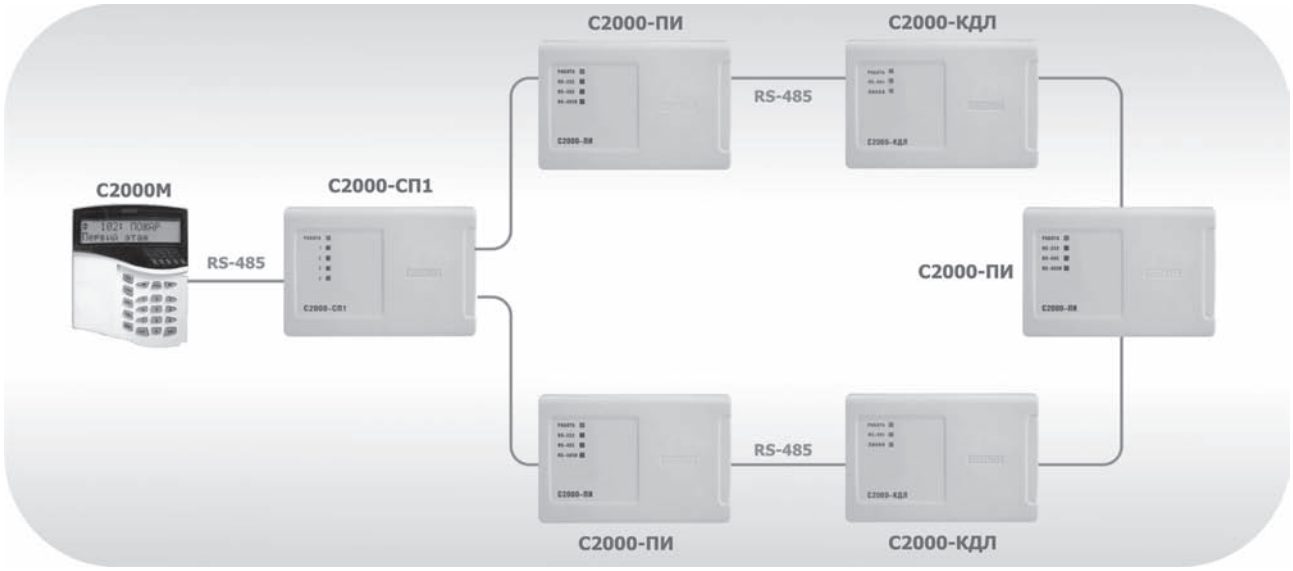


Рис.2. Кольцевая топология магистральной линии связи RS-485

ческий», который можно использовать для постоянного контроля состояния элементов ограждений и техукрепленности, таких как рольставни и пр.

Для гибкого управления постановки на охрану и снятия с охраны, помимо типа для адресной зоны, можно настроить дополнительные параметры: «Задержка взятия под охрану», «Автоматическое перевзятие», «Без права снятия с охраны», «Групповое взятие/снятие».

В ИСО «Орион» предусмотрена возможность отключения индикации в адресных извещателях. Если не отключить сервисный светодиод в извещателе, то в снятом с охраны состоянии извещатель продолжает свою работу, индицируя обнаружение без формирования сигнала тревоги. Особенно это заметно в помещениях с пребыванием и движением людей. Отключение индикатора позволяет скрыть информацию о зоне действия извещателя от стороннего наблюдателя. При этом режим работы индикатора можно легко восстановить, например, для проведения работ по техобслуживанию ОС.

Топология адресной линии связи

Топология адресной линии связи играет важную роль при проектировании. На рисунке 1 топология изображена кольцевой, но адресная линия контроллера «С2000-КДЛ» может быть так же радиальной или с ответвлениями. Так же при проектировании значимым является вопрос надежности при эксплуатации, в частности, сохранение работоспособности ОС при случайном или умышленном повреждении адресного шлейфа — обрыве или коротком замыкании. Кольцевая форма адресной линии, очевидно, решает проблему работы системы при обрыве шлейфа в одной точке. Для локализации короткозамкнутых участков ДПЛС необходимо использовать блоки разветвительно-изолирующие "БРИЗ". Так же данные блоки рекомендованы к использованию при организации ответвлений ДПЛС для исключения взаимного влияния разных участков в случае неисправности. При возникновении короткого замыкания участок цепи между двумя блоками БРИЗ (в кольце) или после блока (в ответвлении) изолируется.

Магистральная линия связи RS-485 ИСО «Орион» так же может быть защищена за счет кольцевой топологии, как показано на рисунке 2.

Данная схема позволяет сохранить полную работоспособность системы при одном обрыве линии интерфейса RS-485 и частичную работоспособность при нескольких обрывах. Однако следует учитывать, что время работы в аварийном режиме зависит от максимального возможного количества переключений реле в модуле С2000-СП1.

Особые сервисные удобства адресная система охранной сигнализации приобретает при использовании персонального компьютера со специализированным программным обеспечением, который используется совместно, или вместо пульта С2000М. Для организации автоматизированных рабочих мест в ИСО «Орион» может использоваться программное обеспечение АРМ «С2000» и АРМ «Орион Про». На экране монитора оператор имеет возможность не только видеть план помещений, но и расстановку извещателей. В случае адресной системы охраны, обнаружение нарушителя будет отображаться в виде иконки тревоги конкретного прибора, поэтому оператор будет информирован о месте проникновения и может использовать эту оперативную информацию в служебных целях.

В АРМ «Орион Про» заложены широкие возможности построения автоматизированных сценариев управления системой охраны. Запускаются такие сценарии по тревожному событию и могут включать в себя множество команд на включение любых релейных выходов в ОС, а так же управление элементами интегрированных подсистем видеонаблюдения и контроля доступа.

Например, с помощью сценария управления и технологических шлейфов легко добиться решения такой задачи: после снятия раздела с охраны проконтролировать, чтобы в течение заданного времени все рольставни на путях эвакуации были подняты, и подать звуковой сигнал, если это условие не выполнено. Предупредительный сигнал также включится, если какая-то рольставня будет опущена в течение дня.

В адресную линию для контроля эксплуатационных режимов и обнаружения протечек в серверных и аппаратных могут быть включены датчики температуры и влажности С2000-ВТ. Для контроля температуры так же можно использовать адресный пожарный извещатель С2000-ИП. Контролируемые параметры в адресно-аналоговом виде передаются в контроллер С2000-КДЛ. Они могут быть использованы в ИСО «Орион» для построения графиков или формирования аварийных сообщений.

Таким образом, при построении адресной системы охранной сигнализации сохраняются принципы модульности, наращиваемости и взаимосвязи приборов, присущей ИСО «Орион», а ее применение дает широкие возможности сотрудникам службы безопасности построить эффективную и надежную систему мониторинга и обнаружения с интеграцией с другими системами безопасности на объекте.

ЧСУП «ОрионПроект»
220131, г. Минск,
пер. Измайловский 1-ый, д. 51, офис 8б
Тел.: (017) 290-04-58
E-mail: info@orionproject.by
www.orionproject.by

УНП: 191107028

ROVALANT

Развитие СМ «Нёман»

Программно-аппаратный комплекс СМ «НЕМАН» предназначен для построения многоуровневых распределенных систем удаленного мониторинга стационарных и мобильных объектов (Автотранспорта и персонала) с обеспечением контроля пожарной, охранной, тревожной, радиационной, экологической, аварийной обстановки.

СМ «НЕМАН» позволяет автоматизировать процесс регистрации, обработки, хранения, отображения всей поступающей информации (в том числе и видео) на компьютерных терминалах дежурных операторов с указанием местоположения объектов на электронной карте, производить контроль и управление мобильными силами и средствами быстрого реагирования на возникновения чрезвычайных ситуаций, а также производить контроль действий дежурных операторов и запись переговоров по голосовым каналам связи.

Статистика.

По состоянию на 2012 год СМ «Нёман» имеет примерную статистику инсталляций по сегментам:

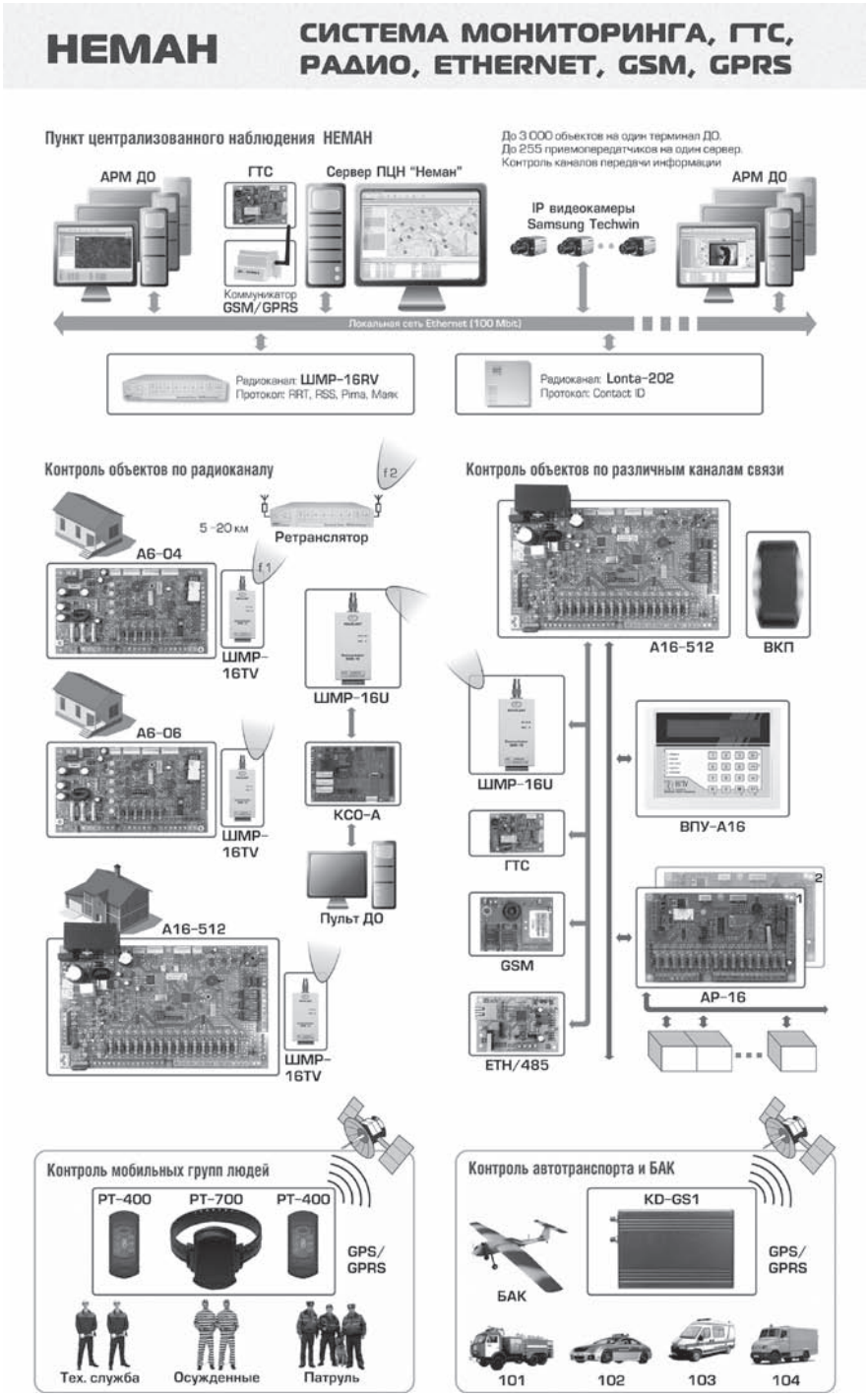
Связь	ИП «Велком» — 70 объектов.
Транспорт	БелЖД (с использованием мультиплексоров HUAWEI) Лида — около 30 объектов, Брест-Барановичи, Молодечно — установлен пульт
Торговля	Порядка 20 магазинов в г. Рогачеве (GPRS-канал)
Банки	ОАО «Беларусбанк» (более 100 объектов), Банк «Москва-Минск»

Каналы связи. Развитие тенденции.

В последнее время при организации систем мониторинга большее значение приобрели оптоволоконные каналы связи. Повышается значимость дублирования передачи сообщений по нескольким каналам связи: радио-Ethernet, GSM-Ethernet, проводные-беспроводные. Проведена опытная эксплуатация СМ "НЕМАН" на базе Октябрьского отдела охраны г. Минска.

При построении системы мониторинга на БелЖД использовались мультиплексоры компании HUAWEI.

Компания «Ровалэнт» может выступать интегратором оборудования, работающего на различных каналах связи, в том числе и всех существующих радиоканальных систем, уже установленных в РБ, на единый пульт МЧС.



СМ «Нёман» поддерживается работа всех уровней мониторинга — от объектового до республиканского. Реализован вариант применения СМ "НЕМАН" для охраны банкоматов. Основные преимущества реализации СМ «Нёман» — это совместимость оборудования различного уровня, гибкие настройки под конкретные задачи, работа по любым каналам связи с поддержкой протоколов сторонних производителей и пр.

На сегодняшний день в СМ «Нёман» интегрированы сторонние системы АСОС "Алеся" (РБ), Lonta (РФ) и при использовании модуля RRT Flex — любое радиоканальное оборудование.

220007, г. Минск, ул. Вододько, 22
Тел.: (017) 228-17-73, (017) 228-16-80
Отдел продаж: (017) 228-17-75, (017) 228-17-72, (017) 228-16-95
Факс: (017) 228-16-96
E-mail: Sales@rovalant.com
Сайт: www.rovalant.com

УНП: 190285495

Особенности применения охранных извещателей в банковской сфере

Образцов Сергей,
директор по развитию
ЗАО «Риэлта»

Справка ТБ

Образцов Сергей Викторович, окончил Ленинградский электротехнический университет в 2003 году. Сразу после учебы пришел в компанию «Риэлта». Работал в должностях инженера-разработчика, заместителя начальника отдела разработок, в этой должности участвовал в создании большого количества новых изделий. Сейчас директор по развитию ЗАО «Риэлта».

О компании

Закрытое акционерное общество "Риэлта" успешно работает в области разработки и производства технических средств охранной сигнализации с 1993г. На сегодняшний день ЗАО "Риэлта" является одним из ведущих предприятий России в этой области. Залогом успешной деятельности компании является целый ряд факторов. Высокий научный потенциал сотрудников, развитая экспериментальная база, профессиональный уровень организации серийного производства, современное технологическое, измерительное и испытательное оборудование позволяют предприятию в короткие сроки и на высоком техническом уровне проводить разработки и освоение новых изделий, постоянно наращивая объёмы производства. Наше предприятие сегодня — это широкий спектр охранных извещателей, приемно-контрольных приборов, устройств для видеонаблюдения, источников питания, автоматических выключателей освещения, приемников ИК-излучения. На предприятии внедрена система менеджмента качества ИСО 9001.

Если спросить любого злоумышленника, какой объект он хотел бы ограбить, то практически каждый ответит: Банк. Сколько фильмов снято про ограбления банков! И действительно, банк — это то место, где хранится большое количество ценностей, а количество самих банков в современных городах неуклонно растет. Можно, конечно, в каждом банке держать большой штат охраны, но это весьма накладно, да и кто будет следить за самой охраной?

Кроме непосредственно банков с их сейфовыми хранилищами, всё большее распространение получают такие устройства как банкоматы и терминалы приема платежей. Они устанавливаются в совершенно разных местах, и приставить к каждому из них охранника практически невозможно.

Поэтому повсеместно в мире основой безопасности банков являются технические средства охраны. Чем же оборудование охранной сигнализацией банка отличается от квартиры или офиса? Ведь там же устанавливаются такие же объемные инфракрасные и магнитоконтактные извещатели, а также датчики разбития стекла. Банк — это как раз то место, где возможны попытки «квалифицированного» ограбления, т.е. весьма вероятно, что вор будет заранее готовиться к краже, изучать средства охранной сигнализации и пытаться придумать способ их обойти. Поэтому для охраны банков следует применять самые современные технические средства. Во многих странах регламентированы более жесткие требования к охранной сигнализации для банков. Например, в Европе все помещения подразделяются на категории в зависимости от важности объекта. Банки, музеи и другие особо важные объекты относятся к самой высокой 4 категории. Одним из требований для охранных извещателей 4 категории является наличие функции антимаскирования. Антимаскирование — это способность извещателя обнаруживать попытки его нейтрализации нарушителем посредством экранирования (маскирования) с помощью материала, блокирующего прохождение контролируемого сигнала. Если обычный инфракрасный извещатель закрыть коробкой, или закрасить его линзу бесцветным лаком, или залепить замазкой входное отверстие микрофона датчика разбития стекла, то извещатель будет сообщать на пульт охраны, что все в «норме», а обнаружить воздействие не сможет. ЗАО «РИЭЛТА» — единственная компания на территории СНГ, которая выпускает охранные извещатели с функцией антимаскирования. Они способны обнаружить попытку маскирования и незамедлительно передать сообщение об этом на пульт охраны. К таким извещателям относятся извещатель охранный оптико-электронный «Фотон-16» и извещатель охранный поверхностный звуковой «Стекло-4».

Существует еще один тип извещателей, который широко применяется для охраны ценностей в банковских хранилищах и находит все более широкое применение в платежных терминалах и банкоматах, которые могут находиться не только на охраняемой территории банка, но и на улицах, станциях метрополитена, в торговых центрах и т.д. Это охранные поверхностные **вибрационные извещатели**. Они предназначены для обнаружения преднамеренного разрушения защитных и строительных конструкций хранилищ материальных ценностей, а также для обнаружения взлома, повреждения и (или) хищения банкоматов, сейфов и других банковских средств защиты. В художественных кинофильмах злоумышленник проделывает отверстие в стене, полу или потолке хранилища банка и похищает его содержимое. Именно для обнаружения таких попыток проникновений, а также для обнаружения попыток вскрытия сейфов (в т.ч. и сейфов банкоматов) и предназначен извещатель охранный поверхностный вибрационный «Шорох-2». Злоумышленник не успевает не то что вскрыть сейф или пробить отверстие в стене и вынести материальные ценности, но даже проникнуть в помещение. Уже в первые секунды его действий извещатель передает сигнал тревоги на пульт охраны. Группе задержания остается только прибыть на объект и задержать вора на месте преступления с целым набором вещественных доказательств.

Принцип действия извещателя «Шорох-2» основан на регистрации вибраций, возникающих при попытках разрушающего воздействия на охраняемую конструкцию. Извещатель «Шорох-2» обнаруживает широкую гамму разрушающих воздействий различными инструментами:

- Ручной ударный инструмент: мо-

лотки, кувалды, ломы, зубила и т.п.;

• Электрический режущий: электрические дисковые пилы, углошлифовальные машины и т.п.;

• Электрический ударный: отбойные молотки и т.п.;

• Электрический вращательный с ударом: электродрели с перфорацией, перфораторы и т.п.;

• Электрический неударный: электродрели, в т.ч. аккумуляторные;

• Ручной режущий: пилы, напильники и т.п.;

• Термический режущий: газорежущее, электродуговое оборудование и т.п.;

• Ручной режущий: ручные коловороты, дрели с ручным приводом и т.п.

Надежное обнаружение перечисленных воздействий достигаются за счет применения специализированного чувствительного элемента и сложной микроконтроллерной обработки сигналов.

Проанализируем наиболее возможные способы вскрытия сейфа:

1. Вскрытие путем высверливания замкового механизма (способ требует знания конструкции сейфа, высокой квалификации вора и достаточно длительного времени.);

2. Вскрытие с помощью углошлифовальных машин (способ быстрый, не требует высокой квалификации, но очень шумный);

3. Вскрытие с помощью газорежущего оборудования, например, ацетиленовой горелки (способ быстрый и относительно бесшумный).

Самым сложным для обнаружения как раз и является газорежущее воздействие. Очень малое количество вибрационных извещателей способно обнаруживать такое воздействие, хотя его применение при реальных ограблениях, например, вскрытие банкоматов, достаточно широко распространено. Извещатель "Шорох-2" уверенно обнаруживает такое воздействие на защищаемую конструкцию, что подтверждается многократными натурными испытаниями.

В таблице 1 приведена площадь, контролируемая одним извещателем "Шорох-2".

При организации охраны банковских хранилищ извещатели устанавливаются на потолке и стенах хранилища открыто, либо на полу в специальных лючках. При необходимости дверь в хранилище также может защищаться извещателями «Шорох-2». Причем защита охраняемой площади может выполняться как со 100% перекрытием (рис.1), так и с охватом не менее 75% площади охраняемой поверхности (рис.2). А1 — извещатель «Шорох-2», R– выбранный радиус действия извещателя.

Извещатель охранный оптико-электронный «Фотон-16»
Имеет три исполнения, отличающихся различными зонами обнаружения (объемная — 12 м, линейная — 20 м и поверхностная — 15 м). Сферическая линза Френеля и микропроцессорная обработка сигнала позволяют обеспечить равномерную чувствительность по всей зоне обнаружения и высокую помехоустойчивость. Для обеспечения антимаскирования используется активный ИК-канал на основе трех излучающих ИК-светодиодов и двух приемных фотодиодов, что обеспечивает обнаружение маскирования любой части линзы. Уникальные схемотехнические и алгоритмические решения обеспечивают обнаружение маскирования различными материалами в соответствии с европейскими нормами EN 50131. Также извещатель имеет контроль напряжения питания, «память тревоги», термокомпенсацию, тампер-контакт и поворотный кронштейн в комплекте.

Извещатель охранный поверхностный звуковой «Стекло-4»
Предназначен для обнаружения разрушения всех видов стекол: обычного, закаленного, узорчатого, армированного, многослойного и защищенного полимерной пленкой (ламинированного), стеклянных пустотелых блоков, а также стандартных одно- и двухкамерных стеклопакетов. Максимальная дальность действия — 6 м. Минимальная контролируемая площадь стекла — 0,1 м2. Также извещатель имеет контроль напряжения питания, «память тревоги», режим настройки, тампер-контакт и поворотный кронштейн в комплекте.

Извещатель охранный поверхностный вибрационный «Шорох-2»
Предназначен для обнаружения преднамеренного разрушения строительных конструкций в виде бетонных стен и перекрытий, кирпичных стен, деревянных конструкций, фанеры, конструкций из древесностружечных плит, типовых металлических сейфов, шкафов и банкоматов.

• Одноблочное исполнение.
• Расширенный диапазон обнаруживаемых воздействий, включая газорежущее, электрорежущее, электродуговое воздействия.
• Автоматический выбор алгоритма работы микропроцессора в зависимости от вида разрушающего воздействия.
• Три режима тестирования, позволяющих произвести регулировку чувствительности для трех групп инструментов при установке на объекте.
• Световая индикация состояния извещателя и помеховых вибраций охраняемой конструкции.
• Возможность управления режимами индикации в зависимости от принятой тактики охраны на объекте (автоматически восстанавливаемая или фиксированная индикация извещений о тревоге).
• Отключение индикации при необходимости маскирования извещателя.
• Контроль напряжения питания.
• Контроль вскрытия корпуса (тампер-контакт).
• Извещатель выдает тревожное извещение размыканием шлейфа сигнализации контактами исполнительного реле.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ	
Чувствительность к вибрации	0,1–1,6 м/с^2
Напряжение питания постоянного тока	9 — 17 В
Потребляемый ток	25 мА
Степень защиты оболочки	IP30
Габаритные размеры	100x40x30,5 мм
Диапазон рабочих температур	-30 — +50° С
Масса	0,2 кг

Таблица 1

Вид охраняемой конструкции	Контролируемая площадь, м^2, не менее	Конфигурация охраняемой зоны
Сплошная бетонная, кирпичная или деревянная конструкция	12	Окружность радиусом 2,0 м
Металлический шкаф, дверь, кожух блока механизмов банкомата	6	Вся внешняя поверхность при максимальном удалении границ охраняемой зоны 1,4 м
Металлический бронированный (засыпной) сейф, блок хранения денег банкомата	3	Вся внешняя поверхность при максимальном удалении границ охраняемой зоны 1,0 м

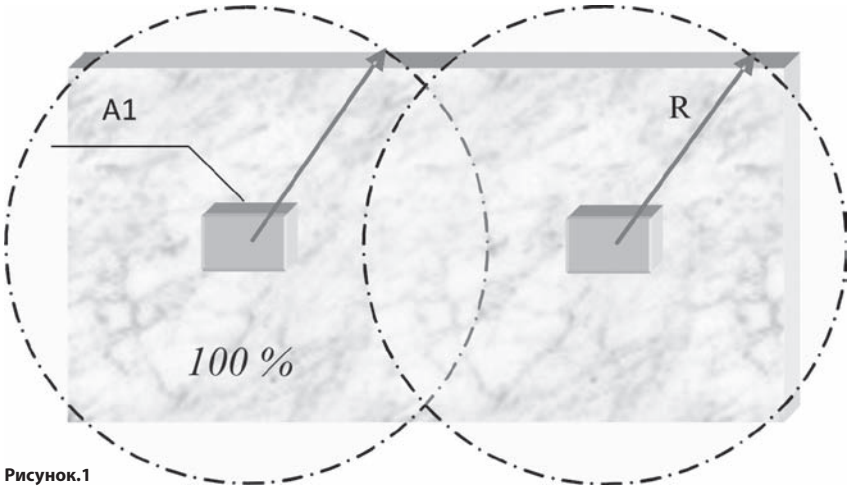


Рисунок.1

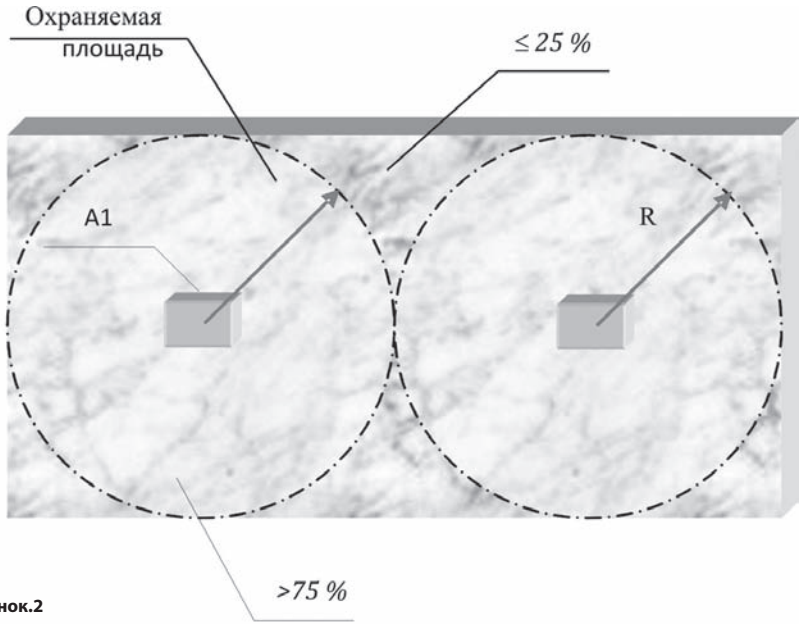


Рисунок.2

При охране больших площадей (таких как стены, потолки и т.д.) иногда более удобно использовать извещатель «Шорох-2-10», который по обнаружительной способности полностью аналогичен извещателю «Шорох-2», но имеет многоблочную конструкцию. В нем один блок обработки сигналов обрабатывает сигнал с нескольких (до 10 штук) датчиков вибрации. Информация от датчиков вибрации передается на блок обработки сигналов посредством двухпроводной линии связи. Такая установка позволяет сократить количество соединительных проводов и снизить стоимость оборудования.

При креплении вибрационных извещателей очень важен надежный механический контакт между извещателем и охраняемой конструкцией. Например, категорически запрещается крепить вибрационные извещатели на двухсторонний скотч или применять пластмассовые дюбеля, так как эти способы крепления плохо передают вибрацию. На кирпичной или бетонной поверхности рекомендуется использовать только те металлические анкеры, которые идут в комплекте поставки. При креплении на металлическую поверхность рекомендуется применять либо винты, либо клей. При использовании клеевых составов очень важно четко соблюдать технологию нанесения клея и рекомендации производителя по применяемым типам клея.

В условиях повышенной помеховой вибрационной обстановки, например, при охране банкоматов в вестибюлях станций метрополитена или при близком расположении от трамвайных путей, необходим особый подход при установке извещателя «Шорох-2». Для обеспечения возможности установки извещателя в таких условиях предусмотрена возможность уменьшения чувствительности от максимального значения на 20 дБ. Но при этом очень важно после изменения регулировок проводить проверку чувствительности извещателя.

В извещателе «Шорох-2» предусмотрен специальный режим тестирования, который позволяет проверить обнаружение конкретного вида воздействия на охраняемую конструкцию.

Извещатель «Шорох-2» заслуженно является одним из самых популярных средств охраны ценностей, находящихся в банковских хранилищах, банкоматах, платежных терминалах, сейфах и т.д. Он практически не имеет аналогов по соотношению цена — обнаружительная способность. При современном развитии и доступности различных инструментов, которые могут применяться для проникновения в охраняемую зону, установка извещателя «Шорох-2» не только целесообразна, но и существенно снижает риски ограбления. Извещатель имеет все необходимые сертификаты и разрешительные документы для применения на территории Республики Беларусь и включен в перечень ТСОС, разрешенных к применению МВД РБ. Гарантийный срок составляет 5 лет.

Официальным представителем в Республике Беларусь является группа компаний «Сфера». www.secur.by

ЗАО «Риэлта»
197101, Санкт-Петербург,
ул. Чапаева, д.17
Тел.: +7 (812) 2332953, 498-19-71
www.rielta.ru
E-mail: rielta@rielta.ru

Необходимость и внедрение темпокасс в банки Республики Беларусь

Бучнев Александр Николаевич, генеральный директор группы компаний «Банковский информационный центр»

Международная практика прогрессивного банковского обслуживания для ряда операций подразумевает формат «open space», где общение с клиентом максимально открытое и дружелюбное. Для безопасности таких операций разработаны специализированные устройства — темпокассы, электронные кассиры и пр. Проводя обзор среди банковских специалистов, мы выяснили, что над введением нового формата задумываются многие отечественные банки. Что мешает активному внедрению устройств и что предлагают поставщики, мы выясняли на страницах данного обзора.

Справка ТБ

Бучнев Александр Николаевич в 1984 году окончил Минский радиотехнический институт по специальности «Конструирование и производство электронно-вычислительной аппаратуры», квалификация инженер-конструктор-технолог. 1977-1979 гг. — служба в вооруженных силах.

Трудовую деятельность начал в 1975 году в качестве техника в НИИ средств автоматизации, после окончания института занимал инженерные должности в НИИ «Агат», ЦКБ «Стандарт», а с 1991 по 1996 г — должность начальника отдела технического обслуживания Минского областного управления статистики. В настоящее время генеральный директор группы компаний «Банковский информационный центр».

Какова международная практика применения темпокасс?

Широкое распространение это оборудование получило в Европе. Например, в Италии очень распространены рециркуляционные темпокассы Roller Cash. На территории СНГ данное оборудование тоже начало распространяться. В Украине наблюдается тенденция роста открытых рабочих мест: за прошлый год было продано более тысячи Roller Cash. В России тоже интенсивно используют темпокассы, а также электронные кассиры (на выдачу денег).

Что сдерживает активное применение темпокасс в Республике Беларусь?

На сегодняшний день основным сдерживающим фактором является нормативно-правовое обеспечение. Банки не могут организовать открытое рабочее место, т.н. «open space», потому что нужна аттестация в Национальном Банке, а документов, четко регулирующих данный вопрос, нет. Например, согласно письму Национального Банка Республики Беларусь от 27.01.2011 года «Об использовании темпокасс» банки имеют право сами принимать решения об установке темпокасс вне кассовых кабин «при условии **персональной ответственности руководителей банков** за создание необходимых условий труда, обеспечивающих безопасность работников банков, совершающих операции с ценностями». В то же время дается рекомендация все же устанавливать темпокассы в кассовых кабинах, оборудованных в соответствии с законодательством Республики Беларусь.

Немаловажным моментом является вид деятельности банка. Если банк преимущественно проводит валютно-обменные операции, то темпокасса в данном случае не очень удобна и актуальна, т.к. под рукой должно быть большое количество денег в разной валюте. В данном случае лучше использовать автоматическое устройство типа Roller Cash. Если бизнес банка больше рассчитан на прием денежной наличности (прием депозитов, оплата услуг и пр.), тогда темпокасса будет уместной.

С Вашей точки зрения, какие еще устройства могут быть востребованы в данном сегменте в ближайшее время?

Пока в Беларуси нет ресайклеров. Но у нас уже есть проект по первому внедрению данного оборудования в банк. Здесь не так все просто, потому что нужно прописать образ белорусских рублей для распознавания их устройством, т.к. устройство автоматически проверяет подлинность банкнот.

Вы рассчитывали объем рынка, импортируя оборудование?

Объем рынка сложно просчитать. Как правило, банки уже имеют свои расчетно-кассовые центры, ведя речь о строящихся банках, тоже сложно оценить объем, т.к. их количество сильно варьируется. Например, полтора года назад был интенсивный рост банков, в прошлом году он сильно сократился, в данный момент снова наблюдается развитие строительства.

Сопровождение и актуальность технического обслуживания темпокасс?

Если мы говорим о простой темпокассе, то вообще не требуется никакого обслуживания. Что касается Roller Cash, то нужна поддержка программного продукта и минимальное техническое обслуживание. На все оборудование дается гарантия. ■

Автоматизированное депозитное хранилище AVM — уникальная самообслуживаемая автоматическая система с круглосуточным доступом к депозитным ячейкам

Барановский Валерий Валерьевич, директор
ООО «НОРДМАН» (эксклюзивный представитель
в Республике Беларусь группы компаний «Europeum»).

В период финансово-экономического кризиса и его последствий сами банки вынуждены искать альтернативные технологические решения, которые позволят получать стабильную прибыль и будут более привлекательными для их клиентов.

Автоматизированное депозитное хранилище AVM позволяет решать данные задачи и является перспективным видом банковского оборудования на современном рынке. Мировым лидером в производстве и эксплуатации депозитных хранилищ AVM является Концерн **Gunnebo** (Швеция), 80% продаж в Европе и странах СНГ. Концерн **Gunnebo**, более известный как **"Розенгренс" (Rosengrens)**, был основан в 1847 году и более 150 лет производит сейфовое оборудование.

Принцип работы

Автоматизированное депозитное хранилище AVM — это самообслуживаемый автомат, позволяющий иметь доступ к депозитным ячейкам 24 часа в сутки 7 дней в неделю, и представляет собой систему аналогичную "автоматизированному складу". Оно включает в себя контейнер, обеспечивающий компактное размещение и сохранность депозитных ячеек, и один или несколько клиентских терминалов. Контейнер размещается в подготовленном хранилище или поставляется вместе со сборно-разборным хранилищем V класса защиты от взлома. Контейнер и клиентские терминалы располагаются как на одном, так и на нескольких уровнях. Специальное подающее устройство (роботизированный автомат) обеспечит доставку депозитной ячейки из контейнера к клиентскому терминалу. В ячейке можно хранить предметы весом до 20 кг. Два из трех существующих вариантов AVM (вариант «мини» и «миди») являются устройствами типа „plug & play" — работают сразу после подключения. При смене локализации банковского отдела устройство может быть легко демонтировано и перенесено в другое место. Клиент имеет возможность использовать конфиденциальный и анонимный доступ к хранимым ценностям в любое время дня и ночи. Идея 24-часового доступа к ячейкам — это шаг в будущее и быстроокупаемая инвестиция для банка.

Система доступа

AVM имеет уникальную систему автоматического доступа к депозитным ячейкам. Доступ клиента к ячейке может осуществляться с разрешения банковского служащего с помощью электронного банковского ключа либо в режиме самообслуживания, когда клиент использует индивидуальную банковскую магнитную карточку и свой ПИН код. После положительной идентификации клиента автомат ищет запрашиваемую ячейку из ряда, находящегося в сейфе или сейфовом хранилище, и подает ее к месту обслуживания клиента, где он имеет безопасный и конфиденциальный доступ к содержимому своей ячейки. После осуществления операции клиент дает команду системе, и ячейка возвращается на свое штатное место в хранилище. В качестве дополнительных средств идентификации может использоваться устройство идентификации по отпечаткам пальцев. Каждая ячейка имеет так же и механический замок, ключ от которого клиент должен иметь при себе.

Конструкция

Автоматизированное депозитное хранилище AVM конфигурируется в соответствии с требованиями Заказчика и монтируется по месту, что позволяет максимально использовать полезное пространство помещения, где оно размещается. В зависимости от варианта AVM может быть оборудовано различным количеством депозитных ячеек от 30 до 2000 шт. Все поставляемое оборудование соответствует общеевропейскому стандарту ISO 9001 и имеет российские сертификаты.

В настоящий момент в Республике Беларусь нет действующих автоматизированных депозитных хранилищ AVM. Несколько проектов по их размещению рассматриваются в некоторых ведущих банках страны, в частности: ОАО "АСБ Беларусбанк", ОАО "БПС-Сбербанк", ОАО "Белинвестбанк" и ОАО «Белвнешэкономбанк». По опыту европейских банков можно сказать, что возможность обеспечения круглосуточного доступа к своим депозитным ячейкам привлечет значительное количество новых клиентов, что, в свою очередь, позволит быстрее окупить стоимость данного оборудования и начать получать чистую прибыль. Кроме того, немаловажное значение имеет и имиджевая составляющая размещения такого рода устройства в банке. К настоящему времени в европейских банках установлено и работает более 5000 автоматизированных хранилищ различных типов и их количество стремительно увеличивается. ■

Модификации AVM

	AVM		
	Mini	Midi	Maxi
Модель			
Ячеек	50-100	100-300	150-2200
Инсталляция	Поставка в готовом виде	Поставка в готовом виде	Монтаж на месте
Сейфовая оболочка	Железобетонная оболочка V класса защиты	Железобетонная оболочка V класса защиты	Железобетонные панели V класса защиты
Конфигурация	Стандартная	Под заказ	Под заказ

Темпокассы — обзор предложений

Характеристики оборудования	Группа компаний «Банковский информационный центр»		ООО «Нордман»			ООО «Измет»				
Производитель	Q-ex, модель Euromulti (EM)	Q-ex, модель Euromulti Simple (EMS)	EK 1520 "Koval Systems a.s.", Словакия	EK 1552 COMPACT "Koval Systems a.s.", Словакия	EK 1500 S EURO "Koval Systems a.s.", Словакия	Paritet-K, Украина	DoCash Tempo M1, DoCash (Россия)	DoCash Tempo 6	DoCash Tempo	DoCash Tempo M
Фото										
Сертификация (РФ, EN)	+	+	ISO 9001:2000 ISO 14001:2004	ISO 9001:2000 ISO 14001:2004	ISO 9001:2000 ISO 14001:2004	+	+	+	+	+
Габаритные размеры (ШхГхВ)	690x500x530	690x500x530	470x570x525	470x590x680	470x590x670	450x600x650	410x538,5x492	460x530x670	524x537x596	410x530x545
Вес, кг	80	80	57	95	85	70	40	45	80	45
Класс взломостойкости (по ГОСТ)	0-1	0-1	1	0	0	0	1	1	1	1
Тип замков (механич., электронно-механич., электрон.)	механич., электронно-механич.	механич., электронно-механич.	механич.	электрон.	механич.	электронно-механич.	электронно-механич.	1 электронно-механич. и 2 механич.	электронно-механич.	электронно-механич.
Класс электробезопасности (по ГОСТ)	нет данных	нет данных	нет данных	нет данных	нет данных	–	нет данных	нет данных	нет данных	нет данных
Толщина стенок корпуса (мм)	3	3	3	2	2	2	4	4	2	2
Количество ящиков для денег	2-5	2-3	1	2	2	2 (для наличности на сдачу, для депонирования наличности)	2	3	3	2
Количество номиналов для депонирования	от 4-х	от 4-х	4	4	4	от 2-х	3	4	5	3
Емкость ящика для денег	+ 396x114x241	+ 396x114x241	+ 15x200	+ 15x200	+ 15x200	–	+	+	+	+
Временная задержка открытия ящиков (сек/мин)	0-99 мин	0-100 мин	0 сек-32 мин	0 сек-90 мин	15 сек-32 мин	до 30 мин (настраивается пользователем)	от 0 до 30 (60) мин	от 0 до 30 (60) мин	от 0 до 30 мин	от 0 до 30 мин
Тип активации темпокассы	ключ PIN-код доступа на 9 кассиров и 1 руководителя. Доступ для одного более кассиров одновременно.	ключ	ключевым замком	электронная панель: ввод личного PIN-кода	ключевым замком	с помощью смарт карт стандарта Em-Marine.	ключ	ключ	ключ	ключ
Индикация	ЖКИ	+	подсоединяется к системе сигнализации банка	присоединяется к внутрибанк. комп-ой сети и сигнализации	Подсоединяется к системе сигнализации банка	LCD дисплей с подсветкой	+	+	+	+
ПО управления	+	–	–	ПО в комплекте	–	–	+	+	+	+
Удаленное управление	+	–	–	–	–	–	+	+	+	+
Питание (В/Гц)	220 В	220 В	220-240В 50/60 Гц, адаптер на 12V	220-240В 50/60 Гц, адаптер на 12V	220-240В 50/60 Гц, адаптер на 12V	100-260В/47-64 Гц	220 В/50 Гц	220 В/50 Гц	220В/50 Гц	220 В/50 Гц
Резервная батарея (В)	12 В; 1,2 А	опция	–	оснащена аккумулятором	–	бесперебо. система пит-я на 24ч работы, возможность увелич-я рез-го питания в 2 раза	нет данных	нет данных	нет данных	нет данных
Потребляемая мощность	не более 70 Вт	не более 70 Вт	Нет данных	Нет данных	Нат данных	75 Вт	не более 70 Вт	не более 70 Вт	не более 70 Вт	не более 70 Вт

Современные средства безопасного хранения

Компания «Измет» внимательно отслеживает новые тенденции развития банковских средств для безопасного хранения. Предлагаем белорусскому рынку ряд эффективных и современных решений, сочетающих в себе высокую надежность и уникальные методы монтажа и установки хранилищ на объекте, что значительно расширяет возможности их применения в помещениях различного типа.

Сборно-разборные взломостойкие банковские сейфы 1-8 класс

Сейфы кассовые бронированные предназначены для обеспечения сохранности ценностей и санкционированного доступа к ним. Сейфы соответствуют всем обязательным требованиям СТБ 51.2.01-99 и ТУ У 28.7-214881112.001-2001, предназначенные для использования банковскими учреждениям.

Сейфы кассовые бронированные бывают 1,2,3,4,5,7,8 класса, Класс 5 — наиболее востребован в банковском секторе Беларуси.

Класс 5

Преимущество сборно-разборных банковских сейфов компании «Измет» в доставке и установке в любых труднодоступных местах: цокольные этажи, узкие проходы, высокие этажи, крутые лестницы, двери.

Сейфы могут дополнительно комплектоваться ключевыми или комбинационными замками по желанию клиента.

Особенности

- Защитный слой сейфа состоит из специальной бетонной смеси Densit. Благодаря использованию этой смеси вес сейфа уменьшается в 1,5-2 раза (в зависимости от размеров сейфа).
- Замок защищен от выбивания и высверливания.
- Сейфы данного класса имеют сборно-разборную конструкцию.
- Наличие специальных устройств (система перезапирателей, накладка из нержавеющей стали), которые обеспечивают надежную защиту ригельной системы при попытке взлома.
- Уникальная конструкция рукоятки сейфа исключает вскрытие силовым воздействием на нее.
- Используется дополнительный защитный механизм — каленое стекло, которое закрывает замочную область и разрушается при попытке сверления или вскрытия с помощью газового резака (в результате происходит блокировка ригелей).
- Сейфы имеют отверстия для анкерного крепления к полу, а также отверстия для подвода кабеля сигнализации и специального приспособления для пломбирования (согласно требованиям СТБ 51.2.01-99).

Модель	Габаритные размеры, мм			Внутренние размеры, мм			Объем, л	Масса, кг	Доп. харак-ки
	высота	*ширина*	*глубина*	*высота*	*ширина*	*глубина*			
CL V.65/65.K.K	650	650	650	450	450	380	77	556	1 полка
CL V.70.K.K	700	720	770	500	520	490	129	715	1 полка
CL V.115/65.K.K	1150	650	650	950	450	380	163	884	1 полка
CL V.100.K.K	1000	720	770	782	520	490	200	780	1 полка
CL V.155/65.K.K	1550	650	650	1350	450	380	231	1148	2 полки
CL V.130.K.K	1300	720	770	1082	520	490	275	965	2 полки
CL V.150.K.K	1500	720	770	1282	520	490	326	1110	2 полки
CL V.175/85.K.K	1750	850	700	1550	650	430	433	1620	3 полки
CL V.180.K.K *	1900	960	825	1700	760	520	672	1750	3 полки
CL V.180.2.K.K *	1900	1760	940	1700	1560	760	2015	3240	3 полки

Сейфы-хранилища со встроенным депозитарием (минидепозитарий)

Благодаря сборно-разборным сейфам-хранилищам теперь в любом, даже самом минимальном отделении банка, можно оборудовать депозитарий без соответствующего строительства укрепленного хранилища.

Сборно-разборная конструкция сейфов-хранилищ позволяет беспрепятственно устанавливать их в любом месте.

Особенности депозитных ячеек:

– двери ячеек и передняя часть корпуса изготовлены из стали толщиной 6 мм

– дополнительные усиления особо ответственных зон двери и корпуса

– ригельные системы производства «La Gard» (США) и «Carl Wittkopp» (Германия)

– скрытые петли дверей гарантируют дополнительную защищенность

Замки:

Ячейки оборудованы специальными депозитными замками «Steinbach &

Vollman» (Германия), отпираемые двумя ключами:

Базовая комплектация ключами (рекомендуется производителем):

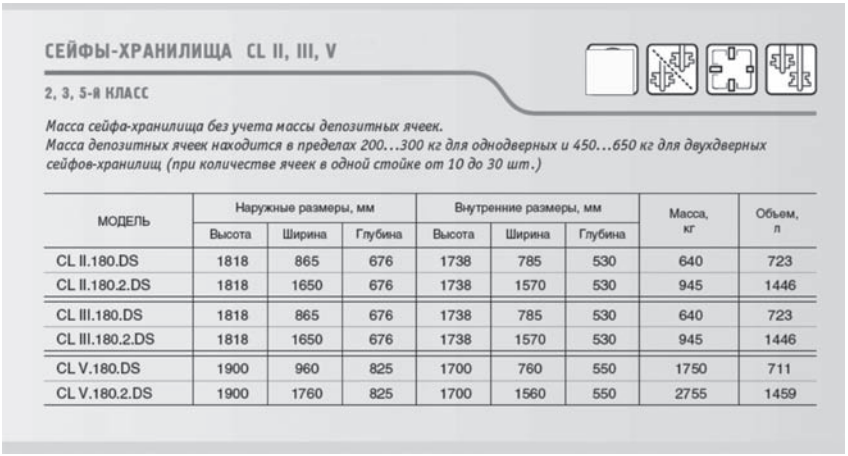
– 2 ключа клиента для каждой ячейки

– 2 ключа банкира (один клиент) для всего количества ячеек

Возможен заказ дополнительных комплектов ключей банкира (оговаривается в техническом задании).

Компания «Измет» поставляет депозитные ячейки высокого качества как в виде стандартных стоек, так и по индивидуальному проекту с ячейками других размеров и высотой ячеек т 50 мм до 500 мм с шагом 25 мм.

Возможно изготовление номерных шильдов с логотипом и символикой заказчика.



СЕЙФЫ-ХРАНИЛИЩА CL II, III, V

2, 3, 5-Й КЛАСС

Масса сейфа-хранилища без учета массы депозитных ячеек.
Масса депозитных ячеек находится в пределах 200…300 кг для однодверных и 450…650 кг для двухдверных сейфов-хранилищ (при количестве ячеек в одной стойке от 10 до 30 шт.)

МОДЕЛЬ	Наружные размеры, мм			Внутренние размеры, мм			Масса, кг	Объем, л
	Высота	Ширина	Глубина	Высота	Ширина	Глубина		
CL II.180.DS	1818	865	676	1738	785	530	640	723
CL II.180.2.DS	1818	1650	676	1738	1570	530	945	1446
CL III.180.DS	1818	865	676	1738	785	530	640	723
CL III.180.2.DS	1818	1650	676	1738	1570	530	945	1446
CL V.180.DS	1900	960	825	1700	760	550	1750	711
CL V.180.2.DS	1900	1760	825	1700	1560	550	2755	1459

Модульное банковское хранилище — преимущества современных технологий

Компания «Измет» предлагает банковские хранилища двух типов: модульные и комбинированные. Выбор типа конструкции зависит от многих факторов, прежде всего, места монтажа и требуемого класса хранилища.

В условиях, когда хранилище монтируется и на фундаменте, и на межэтажном перекрытии, наиболее целесообразным является применение модульной конструкции, где защитную оболочку образуют модули, соединенные в замок друг с другом и обеспечивающие необходимый класс хранилища.

Компания «Измет» предлагает новинку — уникальную технологию «Densit security», которая позволяет получить супертонкую и легкую конструкцию модульного хранилища.

Уменьшение толщины защитного слоя при сохранении его взломостойкости — одна из основных закономерностей и тенденций производителей современных средств банковской защиты. К этому стремится любой производитель, использующий передовые технологии. Меньшая толщина защитного слоя является явным достоинством конструкции в целом, так как в результате заказчик хранилища получает ряд неоспоримых преимуществ:

• Увеличение полезного внутреннего объема хранилища, либо уменьшение внешних габаритов.

• Снижение веса конструкции хранилища, что позволяет, в свою очередь, уменьшить нагрузки на фундамент здания и перекрытие, на котором оно установлено.

• Возможность повысить класс построенного хранилища, выполнив внутреннее или внешнее усиление тонкими панелями высокого класса (что более эффективно, чем при применении панелей традиционной толщины).

Бесспорно, только применение передовых технологий позволило компании «Измет» добиться успехов в уменьшении толщины защитного слоя и организации поставок модульных сейфов и хранилищ, что подтверждено сертификатами соответствия испытательных центров: «Орган по сертификации БНТУ» и «Технический институт сертификации и испыта-

ний». Модульные хранилища, поставляемые ООО «Измет» соответствуют всем обязательным требованиям СТБ 51.2.01-99. Конструктивно хранилища состоят из двух основных элементов: оболочки хранилища и дверного блока. Оболочки и двери сертифицируются отдельно. Класс хранилища определяется по наиболее слабому из этих двух элементов.

Мы уверены, что наши клиенты смогут по достоинству оценить преимущества современных технологий и выгоду для банка вследствие их применения.

Конструкция

По типу конструкции оболочек хранилища делятся на модульные и комбинированные.

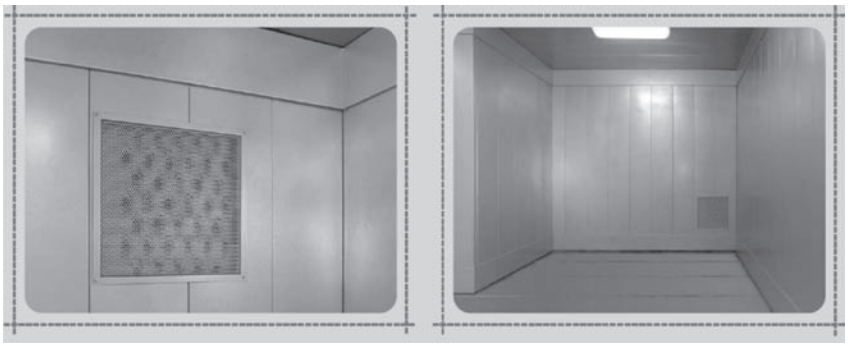
Комбинированные хранилища являются результатом реконструкции существующих хранилищ с целью повышения класса и приведения их в соответствие с действующими в Беларуси нормами.

Хранилище ценностей комбинированное представляет собой железобетонную конструкцию, которая сооружается комбинированным способом и объединяет в себе элементы монолитные и модульные (СТБ 51.2.01-99). Модульные элементы могут устанавливаться как снаружи, так и внутри монолитной части хранилища, образуя единую защитную оболочку.

Конструктивные особенности панелей усиления допускают применение анкерного крепления к внутренней оболочке существующих хранилищ без дополнительных поддерживающих колонн и балок.

Малая толщина панелей усиления «Densit» существенно расширяет возможности усиления хранилищ со стороны наружной поверхности оболочки.

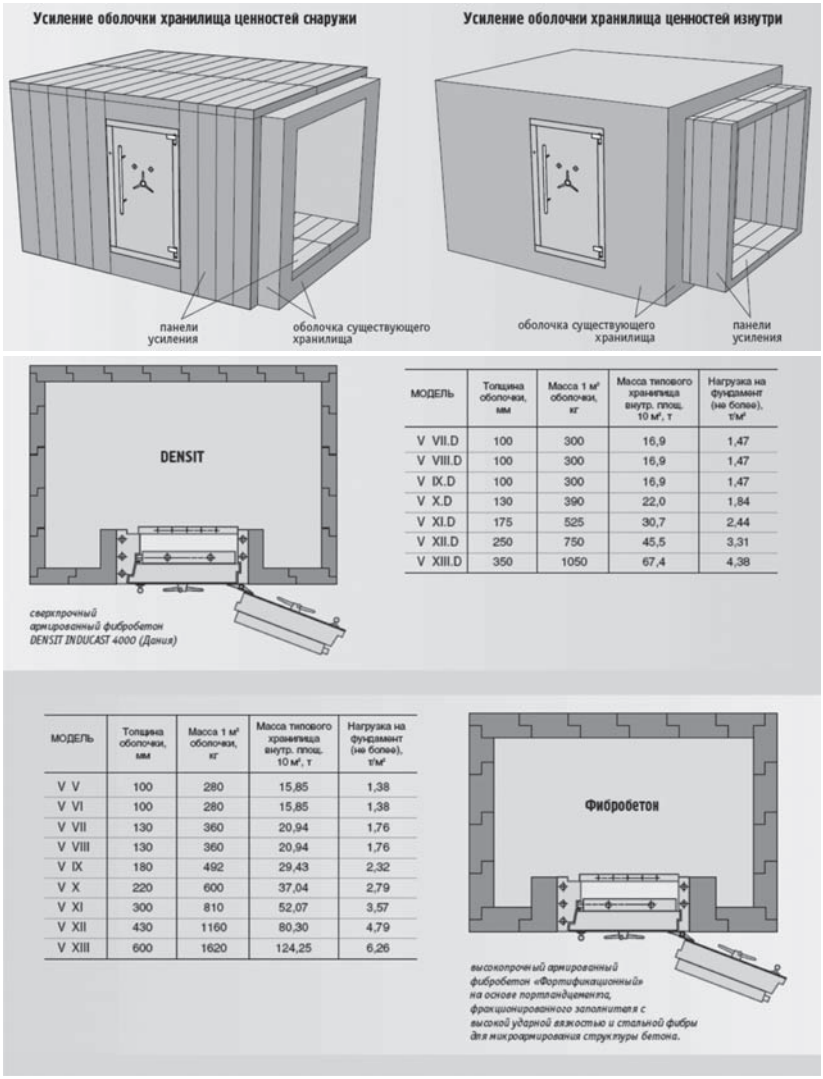
Применение тонкостенных особо прочных панелей усиления часто является единственной реально выполнимой возможностью реконструкции действующих хранилищ с целью повышения класса.



Реконструкция существующих банковских хранилищ в рамках разработанной нашим предприятием программы позволяет получить банкам следующие преимущества:

- Снижение финансовых затрат, связанных с приведением существующих хранилищ в соответствии с требованиями СТБ 51.201-99 «Сейфы, хранилища ценностей».
- Возможность усиления практически любого существующего хранилища без существенного увеличения нагрузок на строительные конструкции здания.
- Отсутствие необходимости установки в усиляемых хранилищах дополнительных поддерживающих колон и балок.
- Возможность реконструкции существующих хранилищ в сложных строительных условиях (зданиях, являющихся историческими или архитектурными памятниками, на перекрытиях этажей зданий и просадочных грунтах).
- Сохранение (или незначительное уменьшение) полезного объема хранилищ в процессе реконструкции.
- Возможность выполнения мероприятий по реконструкции хранилищ в действующих учреждениях банков без прекращения их работы.

Хранилище ценностей модульное представляет собой сборную железобетонную конструкцию, монтируемую на месте эксплуатации из предварительно изготовленных в заводских условиях строительных элементов (СТБ 51.2.01-99). Является самостоятельным строительным объектом.



МОДЕЛЬ	Толщина оболочки, мм	Масса 1 м² оболочки, кг	Масса типового хранилища внутр. площ. 10 м², т	Нагрузка на фундамент (не более), т/м²
V VII.D	100	300	16,9	1,47
V VIII.D	100	300	16,9	1,47
V IX.D	100	300	16,9	1,47
V X.D	130	390	22,0	1,84
V XI.D	175	525	30,7	2,44
V XII.D	250	750	45,5	3,31
V XIII.D	350	1050	67,4	4,38

МОДЕЛЬ	Толщина оболочки, мм	Масса 1 м² оболочки, кг	Масса типового хранилища внутр. площ. 10 м², т	Нагрузка на фундамент (не более), т/м²
V V	100	280	15,85	1,38
V VI	100	280	15,85	1,38
V VII	130	360	20,94	1,76
V VIII	130	360	20,94	1,76
V IX	180	492	29,43	2,32
V X	220	600	37,04	2,79
V XI	300	810	52,07	3,57
V XII	430	1160	80,30	4,79
V XIII	600	1620	124,25	6,26

Варианты модульного или комбинированного хранилища

ООО «Измет»
220026, РБ, г. Минск,
проезд Подшипниковый, 9-21
Тел.: (017) 284-64-00 (многоканальный);
(29) 33-33-018; (29) 260-40-60
E-mail: izmet@izmet.by
Сайт: www.izmet.by

УНП: 690325966

Белорусское производство бронеавтомобилей — опыт и традиции

Справка ТБ: *ООО «ПрактикСервис» — белорусский производитель специальных бронированных автомобилей для инкассации денежной выручки и перевозки ценных грузов в Республике Беларусь. Предприятие создано в марте 2005 года, зарегистрировано в г. Сморгонь Гродненской области.*

Первые годы предприятие работало как официальный дилер ООО НПФ «Практик» (г. Дзержинск Нижегородской области, Российская Федерация) — производителя специальных бронеавтомобилей для инкассации денежной выручки и перевозки ценных грузов. В то время с 2005 года по 2008 банкам Республики Беларусь поставлялись специальные бронированные автомобили производства НПФ «Практик» на базе «Газелей», «Соболей», «УАЗов». Заказчиками и потребителями выступили ОАО « АСБ Беларусбанк», ОАО «БПС-Сбербанк», ОАО «Белинвестбанк», ОАО «БелГАЗпромбанк», ОАО «Белвнешэкономбанк», УП «Москва-Минск», ЗАО «Минский транзитный банк». Было поставлено около 100 спец. бронеавтомобилей.

Но время диктовало свои условия. Накапливался опыт и пришла необходимость создать собственное производство. Предприятие стало самостоятельным производителем специальных бронированных автомобилей для инкассации денежной выручки и перевозки ценных грузов в Республике Беларусь.

В течение 2009-2010 гг налажено производство специальных бронеавтомобилей на базе «Фольксваген Т5 Kasten» «Практик-19276» и его модификаций по 2-му классу стойкости к воздействию стрелкового оружия и производство специальных бронеавтомобилей «Практик-19277» на базе «Фольксваген Caddy Maxi Kasten» по 2-му классу.

С января 2011 года при тесном сотрудничестве с компанией ЧТСУП «Сифтранс», официальным дилером компании Пежо на территории РБ за четыре месяца освоено производство 2-х моделей спец. бронеавтомобилей «Практик-PR1610» и «Практик-PR1620» на базе автомобилей Peugeot Boxer и Peugeot Expert.

Результатом работы с октября 2008 по июнь 2012 г. стало производство и поставка банкам Республики Беларусь 174 специальных бронированных автомобилей. Заказчики — ОАО «АСБ Беларусбанк», ОАО «БПС-Сбербанк», ОАО «Белинвестбанк», ОАО «Белагропромбанк», ОАО «Белгазпромбанк», ЗАО «Минский транзитный банк», РУП «Белпочта», Государственная фельдъегерская служба Республики Беларусь, ОАО «Паритетбанк».

Численность предприятия на конец 2011 года составила 35 человек. Специалисты ООО «ПрактикСервис» имеют высокую квалификацию. Слесаря сборщики 4-5 разряда. В штате опытные ведущие конструктора, инженеры по электрооборудованию спец. бронеавтомобилей.

Особо надо отметить, что становление ООО «ПрактикСервис» как производителя бронеавтомобилей происходило при непосредственном участии российских партнеров по технологии и конструкции ООО НПФ «Практик» и при личной помощи генерального директора ООО НПФ «Практик» г. Дзержинск (Россия, Нижегородская область) Константина Константиновича Лайши (уроженца Беларуси).

Под заказ потребителя спец. бронеавтомобили могут оснащаться любым необходимым оборудованием для инкассации. ООО «ПрактикСервис» поддерживает гарантийное обслуживание всех поставленных автомобилей в период гарантийного срока.

Специальные бронеавтомобили производства ООО «ПрактикСервис» проходят испытания и получают сертификат соответствия в органах по сертификации Республики Беларусь.

В 2011 году предприятием осуществлен интересный проект по бронированию автомобиля «КАМаЗ» по 5-ту классу стойкости к воздействию стрелкового оружия.

Способы бронирования базовых автомобилей

1. Установка на шасси цельносварного бронированного кузова

Данная схема позволяет минимизировать вес бронеавтомобиля, так как в этом случае отсутствует (или почти отсутствует) кузов базового автомобиля. Ранее эта концепция пользовалась спросом, но затем от нее практически полностью отказались, так как внешний облик автомобиля не радовал глаз, а стоимость цельносварного бронированного кузова была высокой.

2. Установка бронезащиты снаружи автомобиля на кузов

Автомобили, в которых применена эта схема, имеют наиболее нагруженное шасси, большую площадь броневой защиты, утяжеляющей внешнюю оболочку кузова. Такая схема может быть хороша только при явном запасе грузоподъемности базового шасси и большой жесткости кузова.

3. Скрытое бронирование базового шасси

Бронезащита при использовании данной схемы находится внутри кузова автомобиля, визуально ее наличие не определяется. При этом крепление бронезащиты внутри кузова машины может быть выполнено в двух вариантах:

• болтовым соединением элементов бронезащиты внутри кузова базового автомобиля;

• цельносварным соединением элементов бронирования, созданием цельносварной бронекапсулы.

Необходимо отметить, что надежность сваренных конструкций и собранных с помощью резьбовых соединений одинаковая. Органами сертификации проверяются наиболее уязвимые места: соединения или переход с одного на другой вид бронирования (места соединения стальных листов бронезащиты и остекления). В процессе сертификации проводится подтверждение соответствия требованиям стандарта по стойкости к воздействию стрелкового оружия изготовленной конструкции в целом. Согласно СТБ 51.3.01-96 предусмотрено шесть классов стойкости специальных автомобилей к воздействию стрелкового оружия. Первый класс определяет стойкость автомобиля к воздействию пули из пистолета Макарова и револьвера типа «Наган». Второй класс обеспечивает стойкость к воздействию пули из пистолета Токарева (ТТ). Третий и четвертый классы пулестойкости обеспечивают защиту от воздействия автоматического оружия (автомат АК-74, АКМ). Пятый класс стойкости к воздействию стрелкового оружия предполагает защиту от винтовки СВД.

Материалы и технологии

ООО «ПрактикСервис» применяет металлическую броню из высокопрочных сплавов. Бронезащита устанавливается на винтовых и болтовых соединениях внутри кузова автомобиля. Она легко снимается и ставится на место. Соединение обеспечивает надежное крепление брони, исключает люфт деталей и связанный с ним посторонний звук при движении автомобиля. В случае обстрела автомашины соединение удерживает броневую защиту по месту крепления. Данный способ установки защиты броневой обеспечивает высокую ремонтопригодность автомобиля.

Металлическая броня — специальная сталь марок Ц85 и А3 производится и поставляется из России. Состав сплава и технология получения засекречены. Броневые конструкции специального автомобиля должны обеспечивать защиту от воздействия пуль стрелкового оружия при круговом обстреле.

Для остекления автомобиля применяются стекла пулестойкие. Официальное определение пулестойкого стекла — «многослойное светопрозрачное изделие, способное задержать попавшие в него пули, выпущенные из ручного огнестрельного оружия или осколки от разорвавшихся ручных гранат».

При производстве спец. автомобилей используются многослойные пулестойкие стекла соответствующего класса защиты производства российских компаний ООО НПФ «Практик», ЗАО «Стеклолюкс», ООО «Магистраль ЛТД».

ООО «ПрактикСервис» имеет собственные производственные площади, позволяющие выполнять значительные объемы работ. В производстве применяется токарное, фрезерное оборудование, плазменная резка и другое оборудование.

Перспективы развития ООО «ПрактикСервис»

1. Освоение максимально широкого модельного ряда бронеавтомобилей, которые пользуются спросом у потребителя, а именно:

- на базе модели VW T5 создать 4 модификации (длинная база — стандартная крыша, короткая база — стандартная крыша, длинная база — средняя крыша, короткая база — средняя крыша);
- на базе модели VW Caddy — 2 модификации (короткая база, длинная база);
- на базе модели VW Crafter — 3 модификации (короткая база — стандартная крыша, средняя база- стандартная крыша, средняя база — высокая крыша);
- на базе модели Пежо Boxer — 2 модификации (средняя крыша, низкая крыша);
- на базе модели Пежо Expert — 3 модификации (короткая база — низкая крыша, короткая база- высокая крыша, длинная база — высокая крыша);
- на базе Форд Connect — 1 модификация;
- на базе модели Форд Транзит — 2 модификации (VAN 330, VAN 350).

2. Освоение производство спец. бронеавтомобилей для инкассации по 3-му классу защиты и в перспективе вести работы по созданию бронеавтомобилей модульного типа.

Кроме того, имеются наработки по двум направлениям, не связанным с бронированием, — создание и постановка на производство 2-3-х моделей маршрутных такси и автомобиля скорой помощи.

Для решения данных задач на предприятии создана конструкторско-технологическая группа, на которую и возложена задача разработки конструкторско-технологической документации. На сегодняшний день практически завершены работы по разработке проектно-сметной документации на расширение производственной базы.

Уже в течение 2012 года планируется инвестировать в собственное производство около 1 миллиарда рублей в текущих ценах и дополнительно создать до 15 рабочих мест.

В основе работы предприятия ООО «ПрактикСервис» лежит принцип: «Потребитель всегда прав». ■

	Характеристики					
Модель специального транспортного средства	Специальный бронированный автомобиль «Практик-19277»	Специальный бронированный автомобиль «Практик-PR1910» «Практик-PR1911» «Практик-PR1912» «Практик-PR1913»	Специальный бронированный автомобиль «Практик-PR1920» «Практик-PR1921» «Практик-PR1922»	Специальный бронированный автомобиль «Практик-R1610» «Практик-R1611» «Практик-R1612»	Специальный бронированный автомобиль «Практик-PR1620» «Практик- PR1621»	Специальный бронированный автомобиль «Практик-PR1710»
						
Модель базового автомобиля	«Volkswagen Caddy Maxi»	«Volkswagen Transporter»	«Volkswagen Crafter»	«Peugeot Expert»	«Peugeot Boxer»	«Ford Transit Connect»
Информация о № и дате выдачи сертификата, срок действия	на каждую партию	на каждую партию	на каждую партию	на каждую партию	на каждую партию	на каждую партию
Класс стойкости к воздействию стрелкового оружия (№ сертификата, дата выдачи, срок действия)	2-й класс СТБ-51.3.01-96	2-й класс СТБ-51.3.01-96	2-й класс СТБ-51.3.01-96	2-й класс СТБ-51.3.01-96	2-й класс СТБ-51.3.01-96	2-й класс СТБ-51.3.01-96
Колесная формула	4x2	4x2	4x2	4x2	4x2	4x2
Полная масса автомобиля, кг	2315	3200	3500	2902/2932/2963	3500/3300	2340
Снаряженная масса базового автомобиля/бронированного автомобиля, кг	1940	2470/2390/2650/2560	2850/2780/2660	2290/2370/2420	2995/2800	2080
Масса перевозимого бронеавтомобилем груза (вкл. экипаж), кг	375	730/810/550/640	650/770/890	612/562/543	505/500	260
Количество посадочных мест (вкл. водителя)	4	4	4	4	4	4
Распределение полной массы по осям (на переднюю/ заднюю)	1110/1215	1650/1720	1650/1850	1300/1361	1700/1800 1600/1900	1130/1290
Габаритные размеры, мм (длина, высота, ширина)	4975x1950x1794	5391x2170x1904 4991x2170x1904 5391x2300x1904 4991x2300x1904	5910x2700x1993 5910x2500x1993 5245x2500x1993	4813x2140x1895 5143x2140x1895 5143x2450x1895	5550x2522x2100 5550x2254x2100	4571x2200x1795
Внутренний объем, м^3 (салона, грузового отсека)	до 4,2	до 6,7/5,8/6,7/7,8	До 7.5/9,0/11	до 5,0/6,0/7,0	до 11,5/10,0	До 3,7
Максимальная скорость, км/ч, не менее	110	120	120	120	120	110
Внешний габаритный радиус поворота, м	6,2	6,6/5,95/6,6/5,95	6,15/6,15/6,8	6,1	6,2	5,95
Тип двигателя	TDI	TDI	TDI	TDI	TDI	TDI
Рабочий объем, л	1,6-2,0	2,0	2,0	2,0	3,0	1,8
Номинальная мощность двигателя, кВт (л.с.)	75(102)-103(140)	75(102)-103(140)	80(108)-100(135)	88(120)	115,5(157)	66(90)
Максимальный крутящий момент, Нм (об/мин)	250-320(1900-2500)	250-340(1500-2500)	300-340(1500-2250)	300 (2000)	400(1800)	220(1700-2500)
Применяемое топливо	дизельное	дизельное	дизельное	дизельное	дизельное	дизельное
Расход топлива, л/100 км (по шоссе/ по городу)	6/9	7/11,2	8,7/11,7	6,6/9,4	8,3/11,0	5,5/7,2
Наличие и виды доработок базовых шасси под требования новых условий применения (усиление подвески, применение шин повышенной грузоподъемности и т.д.)	Усиленная подвеска	Усиленная подвеска	Усиленная подвеска	Усиленная подвеска	Усиленная подвеска	Усиленная подвеска
Гарантийные сроки, месяцы (пробег, км)	24 мес. без пробега	24 мес. без пробега	24 мес. без пробега	24 мес. без пробега	24 мес. без пробега	24 мес. без пробега

БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Системы комплексной безопасности критически важных объектов информатизации

Маликов Владимир Викторович. Начальник цикла технических и специальных дисциплин Учреждения образования «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь, подполковник милиции, кандидат технических наук.

Согласно п. 14 Концепции национальной безопасности Республики Беларусь обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (КВОИ) является одним из основных национальных интересов в информационной сфере Республики Беларусь.

Проблема безопасности КВОИ заключается в следующем: создатель объекта и его составляющих, в том числе средств автоматизации, стремится к обеспечению наибольшей эффективности объекта. Однако, ввиду наличия угроз информационной безопасности КВОИ, разработчик систем защиты независимо от его решений вынужден снижать эффективность объекта. Для того чтобы степень снижения эффективности лежала в рамках допустимых значений, целесообразно выполнение следующих мероприятий: внедрение новых систем защиты и модернизация существующих должна быть экономически целесообразной, что требует разработки методик оценки их эффективности.

В целях определения соответствия функциональных характеристик КВОИ требованиям, установленным эксплуатационной документацией на КВОИ и техническими нормативными правовыми актами, необходимо проведение внутренних и внешних аудитов систем защиты.

Для методического обеспечения проведения аудитов необходима разработка:

– целевых критериев эффективности систем защиты КВОИ путем выделения группы критически важных показателей и определения эффективных значений их параметров;

– краткого каталога требований к основным структурным уровням системы защиты КВОИ, основанного на тематических классификационных шаблонах составных компонентов системы безопасности.

Обеспечение комплексной безопасности КВОИ на качественно новом научно-теоретическом и практическом уровне возможно только при сопряжении нормативно-правовых, организационно-технических и технических мероприятий, что позволит эффективно решить ряд задач в рамках Концепции национальной безопасности Республики Беларусь и безопасности государства в целом.

Научно-практический семинар
«Безопасность критически важных объектов»

В рамках X Белорусско-российской научно-технической конференции «Технические средства защиты информации» 30 мая 2012 г. в БГУИР состоялся научно-практический семинар «Безопасность критически важных объектов». Главная тема семинара была посвящена рассмотрению вопросов обеспечения безопасности АСУ ТП как важного элемента КВО.

Рассматриваемые вопросы: нормативно-правовое, организационно-техническое, техническое обеспечение безопасности КВО (КВОИ). Приведенные ниже материалы являются сокращенными и переработанными версиями докладов на семинаре. ■

Проблемы обеспечения безопасности критически важных инфраструктур

Картель Владимир Федорович, директор Государственного предприятия «НИИ ТЗИ»

Информационные системы и их сети являются неотъемлемыми компонентами таких критически важных инфраструктур, как управление государством, энергетика, транспорт, банковская сфера, жизнеобеспечение населения и др. Критически важные объекты информатизации (КВОИ) этих инфраструктур во многих странах уже стали объектами кибернетических атак отдельных нарушителей, криминальных групп, государственных структур. Воздействие на КВОИ сектора экономики в настоящее время является одним из основных направлений враждебных действий в отношении любого государства.

КВОИ представляют собой широкое множество компьютерных систем и средств, управляющих критически важными процессами или уникальным оборудованием на объектах отраслевых инфраструктур, нарушение функционирования которых может иметь существенные отрицательные последствия по многим аспектам.

Успешная кибернетическая атака на КВОИ может привести к тяжелой техногенной катастрофе, большому экономическому ущербу, гибели людей, нарушению систем управления государством, обороной и, в конечном итоге, к нарушению национальной безопасности.

Понятия «кибернетическая атака», «информационная война» стали признаками главной проблемы сегодняшнего дня — обеспечения безопасности кибернетического пространства страны.

Анализ безопасности национальных инфраструктур показал, что большинство жизненно важных отраслей экономики уязвимы к возможным кибернетическим атакам.

Отсюда вытекают стратегические цели обеспечения национальной безопасности в рассматриваемой области:

– идентификация и обеспечение гарантий защиты тех инфраструктур, систем управления и их активов, которые считаются критически важными для национальной безопасности;

– государственный контроль за обеспечением защиты КВОИ критически важных инфраструктур;

– обеспечение безопасности критически важных инфраструктур и их активов путем последовательного выполнения специальных мероприятий по созданию совместной окружающей среды, в которой органы власти и управления на всех уровнях (государственном, региональном, локальном) и негосударственный сектор могут лучше организовать их защиту;

– своевременное предупреждение субъектов информационного пространства страны об опасности кибернетических атак и оказание помощи при защите или восстановлении тех критических инфраструктур и их КВОИ, которые сталкиваются с определенной неизбежной угрозой.

Защита критических инфраструктур и КВОИ от незаконного вмешательства в их функционирование является основной задачей поддержания внутренней экономической, политической стабильности и национальной безопасности в целом. Проблема обеспечения безопасности КВОИ таких инфраструктур должна рассматриваться по нескольким основным направлениям.

Основные направления обеспечения безопасности КВОИ

Создание системы правовых нормативных актов, обеспечивающих организацию действенной системы управления безопасностью критических инфраструктур.

Эта система должна устанавливать обязанности государства и владельцев инфраструктур по обеспечению нормального функционирования, защите критически важных объектов этих инфраструктур от кибернетических и иных атак, защите населения и окружающей среды от техногенных катастроф, связанных с авариями на объектах этих инфраструктур.

В Республике Беларусь решение этой задачи начато с принятия Концепции национальной безопасности, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. N 575. В ней впервые обеспечение надежности и устойчивости функционирования КВОИ отнесено к основным национальным интересам в информационной сфере, а нарушение функционирования КВОИ — к основным потенциальным либо реально существующим угрозам национальной безопасности. Несовершенство системы обеспечения безопасности КВОИ признается существенной внутренней угрозой национальной безопасности.

В развитие положений Концепции национальной безопасности приняты ряд нормативных правовых актов, одним из которых является Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». В соответствии с Указом создается Государственный реестр КВОИ, утверждено Положение об отнесении объектов информатизации к критически важным, обеспечении и контроле их безопасности.

Вместе с тем следует отметить, что законодательное поле Республики Беларусь еще не соответствует современным требованиям правовой охраны объектов критически важных инфраструктур, а документы, регламентирующие деятельность по обеспечению информационной безопасности критически важных инфраструктур и их объектов, в должном объеме еще не разработаны.

Создание системы правовых нормативных технических актов (ТНПА), устанавливающих современные требования к обеспечению безопасности КВОИ на всех этапах их жизненного цикла.

В развитие Указа Президента Республики Беларусь № 486 Институтом (НИИТЗИ) в 2011 году по поручению Оперативно-аналитического

центра при Президенте Республики Беларусь выполнена научно-исследовательская работа «Киберзащита», в рамках которой разработан ряд ТНПА, устанавливающих классификацию КВОИ по уровню безопасности, общие требования к их защите и профили защиты в соответствии с классами безопасности, учитывающие повышенные требования к надежности функционирования и готовности компьютерных систем при обращении к ним.

Особое внимание в республике уделяется проблеме информационной безопасности строящейся АЭС. Защита КВОИ АЭС, к которым относятся компьютерные системы контроля и управления реактором, обеспечивающими системами и коммуникациями, системы, относящиеся к защите реактора, системы охраны и др. является основой обеспечения безопасности станции в целом, защиты населения и окружающей ее среды от выбросов ядерных материалов, вызванных нарушением функционирования этих систем и управляемого ими оборудования.

Следует признать, что положения национальных стандартов, разработанных в Республике Беларусь, а также стандартов, реализованных путем прямого введения стандартов ИСО (серии 27000, 15408 и др.) ориентированы на достаточно простые в архитектурно-технологическом и организационно-административном плане объекты. Это обстоятельство — дополнительный источник уязвимостей КВОИ, которые в большинстве отраслевых инфраструктур являются специальными промышленными компьютерными системами.

Поэтому при разработке стандартов для АЭС использованы лучшие достижения мировой практики, представленные в стандартах и руководствах международных и национальных организаций (МЭК, МАГАТЭ, ISACA и др.), в большей степени ориентированных на промышленные системы управления.

АЭС относится к особо опасным и режимным предприятиям. Поэтому следует рассмотреть вопрос разработки и аттестации ее систем контроля и управления, важных для безопасности, и их компонентов с применением требований военной приемки.

Необходима также разработка нормативных документов, учитывающих мировой и национальный опыт обеспечения безопасности критически важных промышленных объектов и специфику инфраструктур национального экономического сектора (энергетика, промышленность, транспорт, жизнеобеспечение населения и т.п.), содержащих требования по реализации и контролю эффективных мер защиты автоматизированных систем управления такими инфраструктурами и их технологическими процессами.

Разработка новых методов и средств защиты КВОИ

Основное внимание должно быть уделено повышению надежности и расширению функциональных возможностей средств защиты КВОИ. Гарантия безопасного функционирования КВОИ в значительной степени обеспечивается качеством обслуживания и мониторингом безопасности КВОИ в процессе их эксплуатации. Это, в свою очередь, требует использования современных подходов к организации защиты, в частности, предупреждения несанкционированного доступа к его активам и быстрого восстановления функционирования КВОИ в случае реализации угрозы.

Потенциальным направлением исследований в этой области должны стать проекты по созданию автоматизированных систем мониторинга безопасности, позволяющие обнаруживать угрозы КВОИ, оценивать их корреляцию и реагировать на них в режиме реального времени.

Сертификация персонала

Персонал, работающий на КВОИ, должен быть сертифицирован на профессиональную компетентность в соответствии с ролью каждого в задаче обеспечения качества функционирования и безопасности КВОИ. Институтом разработаны два стандарта, касающиеся требований и порядка сертификации персонала для критически важных систем, которые могут применяться для организации и оценки качества подготовки персонала КВОИ.

Важную роль в процессе информационной безопасности КВОИ инфраструктур играет осведомленность административного персонала в вопросах безопасности.

Соблюдение правил информационной безопасности является сегодня важнейшим компонентом «культуры безопасности» любого предприятия.

Международное сотрудничество

Создание «виртуальной аналитической среды», которая соединит в одно целое тех, кто осуществляет сбор, распределение, анализ и использование информации об угрозах критически важных инфраструктур и способах противодействия им, сегодня может стать основой инвестиционной и технической политики в области использования компьютерных технологий во всех отраслях.

Ее создание особо важно для наших стран, поскольку наши критические инфраструктуры (электроэнергетика, передача нефти и газа и др.) взаимосвязаны, носят трансграничный характер и их надежное функционирование важно не только для Республики Беларусь и России, но и для других стран.

Вместе с тем следует учитывать, что международное сотрудничество в области кибернетической безопасности будет существенно сдерживаться отсутствием согласованных законов и соответствующего инструментария для преследования нарушителей и принудительного исполнения норм международного права.

Таким образом, при создании системы противодействия кибернетическим атакам на КВОИ критических инфраструктур необходимо:

– проведение системных научных исследований и прикладных работ в данном направлении при активном участии государственных и коммерческих структур, работающих в данной области;

– тесное взаимодействие государственных органов, организаций и бизнес структур на национальном и международном уровне при проведении мероприятий, направленных на поиск источников угроз, атак и защиту КВОИ;

– комплексный подход к обеспечению информационной безопасности подконтрольных объектов, предполагающий скоординированную систему мер и мероприятий, моделей, механизмов и инструментальных средств на всех уровнях его реализации (правовом, административном, программно-техническом и др.);

Эти задачи решаются в заданиях Союзной программы и соответствующих программ Республики Беларусь.

Государственное предприятие "НИИ ТЗИ"
220088, г.Минск,
ул.Первомайская, д.26, к.2
Тел.: (17) 294-01-71
Факс: (17) 285-31-86
E-mail: info@niitzi.by
www.niitzi.by

Актуальные вопросы технической защиты информации в системах физической защиты объектов критической инфраструктуры

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

Справка ТБ

Барановский Олег Константинович, образование высшее, радиофизик, в 1998 г. окончил Белорусский государственный университет. Имеет академическую степень магистра естественных наук, кандидат физико-математических наук. Опыт работы в области защиты информации с 1998 г. по настоящее время.

Еще относительно недавно вопрос безопасности объектов критической инфраструктуры государства решался по двум основным направлениям: защита от несанкционированного доступа на объект и обеспечение надежного функционирования автоматизированных систем управления технологическими процессами. Однако развитие и распространение информационных технологий, глобализация информационно-телекоммуникационных сетей обусловили появление нового типа угроз безопасности объектов — удаленного взлома и нарушения режимов функционирования объектов информатизации, отвечающих за управление и обеспечение безопасности экологически опасных и (или) социально значимых производств.

Акцентирование на государственном уровне внимания на проблему безопасности критически важных объектов, систем и инфраструктур реализовано Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь». В настоящее время действует **ряд нормативных правовых актов Республики Беларусь, регулирующих правовые отношения, возникающие при идентификации, регистрации, обеспечении безопасного функционирования, проведении внешнего контроля за состоянием технической защиты информации критически важных объектов информатизации (КВОИ):**

Указ Президента Республики Беларусь от 25.10.2011 № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 г. № 96 «О некоторых мерах по реализации указа Президента Республики Беларусь от 25 октября 2011 Г. № 486»;

Постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении инструкции о порядке проведения внешнего контроля критически важных объектов информатизации».

Кроме того установлены основные технические требования к обеспечению защиты информации КВОИ:

СТБ П 34.101.52-2012 «Информационные технологии. Методы и средства безопасности. Критически важные объекты информатизации. Классификация»;

СТБ П 34.101.53-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса А1-у»;

СТБ П 34.101.54-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса А2-у»;

СТБ П 34.101.55-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса Б1-у»;

СТБ П 34.101.56-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса Б2-у»;

СТБ П 34.101.57-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса В1-у»;

СТБ П 34.101.58-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса В2-у»;

СТБ П 34.101.59-2012 «Информационные технологии и безопасность. Задание по безопасности. Методические указания по разработке».

Несмотря на то, что Указом № 486 выделены типы объектов информатизации, которые могут быть отнесены к критически важным, у владельцев и ответственных республиканских органов государственного управления возникают затруднения при определении отраслевых критериев принятия решения.

Так, если с объектами информатизации, осуществляющими функции информационной системы или обеспечивающими предоставление значительного объема информационных услуг, имеется относительная ясность, то к объектам информатизации, обеспечивающим функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов нельзя относить только автоматизированные системы управления такими производствами и процессами.

Устойчивость функционирования экологически опасных производств (объектов критических инфраструктур) поддерживается системами жизнеобеспечения и безопасности. Вместе с тем до сих пор методологически не проработан вопрос безопасности критически важных объектов, систем и инфраструктур в целом.

Непременным элементом системы безопасности экологически опасных

производств как критически важных объектов (нарушение штатного режима может привести к чрезвычайной ситуации техногенного характера) является система физической защиты.

Ориентировочный состав и требования к средствам физической защиты приведены в ТКП 360 2011 (02300) «Положение об общих требованиях к системам физической защиты ядерных объектов»:

– система охранной сигнализации;
– тревожно-вызывная сигнализация;
– система контроля и управления доступом;
– система наблюдения и оценки обстановки;
– система оперативной связи и оповещения;
– система телекоммуникаций;
– подсистема защиты информации;
– подсистема электропитания.

Каждый функциональный элемент системы физической защиты информации является обязательным с учетом особого статуса критически важных объектов. При этом обоснование объемов реализуемых мер в подсистеме защиты информации должно основываться на модели нарушителя.

Создание иностранными государствами подразделений, в функции которых входит вывод из строя элементов критических инфраструктур других стран, применение в республике импортных средств защиты информации и технических (программно-технических) средств физической защиты, требует принятия адекватных мер по противодействию угрозам информационной безопасности различных систем обеспечения функционирования критически важных объектов.

Одновременно наблюдается тенденция интеграции систем жизнеобеспечения и безопасности объектов в комплексные системы безопасности на основе IP-технологий. Это позволяет по-новому управлять безопасностью объектов на основе анализа большого числа связанных с безопасностью событий.

В данном контексте актуальными являются задачи обеспечения информационной безопасности процессов мониторинга и реагирования на события в области безопасности.

Характерной особенностью современных систем «интеллектуального» анализа состояния безопасности является наличие большого числа датчиков, регистрирующих параметры состояния физической среды защищаемого объекта.

Обобщенная схема процесса получения, обработки данных и реагирования на фактическое состояние критически важного объекта представлена на рисунке 1. Показания с измерительных датчиков собираются с применением коммуникационной инфраструктуры и агрегируются для их дальнейшей обработки в средствах оценки состояния безопасности объекта.

Рисунок 1 — Схема процесса мониторинга и управления безопасностью физического объекта

Характеристика фактического состояния критически важного объекта может представлять собой число, вектор, матрицу. С применением средств и систем управления безопасным состоянием объекта подаются команды на датчики мониторинга и управления физическими параметрами среды объекта.

Безопасность информации обеспечивается путем поддержания конфиденциальности, целостности, доступности и сохранности информации. Характерной особенностью защиты систем мониторинга и управления физическими процессами или объектами является гарантия подлинности критичных активов — данных, субъектов и процессов.

Подлинность активов обеспечивается созданием доверенной среды — гарантиями, что комплекс программно-технических средств и линии связи находятся в необходимой безопасной конфигурации. Кроме того, используются надежные алгоритмы аутентификации данных, взаимодействующих субъектов и алгоритмов обработки данных.

Предпринимаемые меры должны обеспечивать защиту от таких видов атак, как:

– перехват информации;
– компрометация ключевой информации (утеря, несанкционированный доступ к криптографическим ключам);
– атака «человек в середине» («man-in-the-middle»), позволяющая подменять передаваемые данные или управляющие команды.

Не менее опасными являются атаки вида «отказ в обслуживании», основными способами реализации которых являются:

– лавинообразное переполнение сети передачи данных пакетами вплоть до ее перегрузки;
– посылка неверных данных, например, контроллеру управляющего датчика, что может привести к аварийной остановке или некорректному функционированию сервисов безопасности;
– блокирование трафика в сети, что может привести либо к потере доступа к измерительным датчикам, либо к механизмам управления безопасностью.

При реализации мер защиты критически важных объектов следует учитывать, что их эффективность не может быть обеспечена только путем закрытия отдельных угроз (пакета угроз) из модели нарушителя с применением имеющихся на рынке средств защиты информации. Необходимо учитывать уязвимости конкретных применяемых моделей оборудования и версий программного обеспечения.

Вопросы обеспечения безопасности критически важных объектов, систем и структур в целом многогранны и слабо проработаны ввиду относительной новизны проблемы и нечеткости границ объектов защиты. Для интенсификации усилий по развитию методов и средств информационной защищенности систем управления и обеспечения безопасности критически важных объектов, особенно экологически опасных и (или) социально значимых производств и (или) технологических процессов, необходим толчок в форме громкого инцидента в области информационной безопасности.

Государственное предприятие "НИИ ТЗИ"
220088, г. Минск
ул. Первомайская, д.26, к.2
Тел.: (17) 294-01-71
Факс: (17) 285-31-86
E-mail: info@niitzi.by
www.niitzi.by

Информзащита
Системный интегратор

Особенности обеспечения информационной безопасности АСУ ТП

Спасенных Елизавета,
компания «Информзащита»

Справка ТБ

Спасенных Елизавета Михайловна, менеджер по развитию бизнеса ЗАО НИП «Информзащита». Высшее образование: специалист по защите информации (НИЯУ МИФИ); экономист-менеджер в ИТ отрасли (НИЯУ МИФИ). Значительный опыт работы консультантом на проектах по защите персональных данных, анализу рисков, разработке нормативных документов, защите АСУ ТП, анализу эффективности бизнес-процессов и др.

Каждый сотый объект информационных систем подвергался кибератакам. Каждый тринадцатый подозревается в наличии реализованной уязвимости. Безопасность каждого третьего подвергается сомнению специалистами, которые не знают, были ли их ресурсы атакованы, или нет. Таковы результаты исследования компании Symantec[1] в области защиты критически важных объектов.

То же исследование содержит результаты анализа уровня защищенности по различным направлениям обеспечения безопасности. В соответствии с ним, российские компании существенно проигрывают западным по степени реализации мер по защите сетей, мониторингу событий безопасности, контролю доступа и аудиту информационной безопасности. Аналогичная тенденция прослеживается и в области осведомленности о защищенности автоматизированных систем управления технологическими процессами (АСУ ТП).

Обеспечение информационной безопасности АСУ ТП предполагает некоторые специфические аспекты. Они связаны с условиями эксплуатации систем и долгим жизненным циклом используемых технологий. На практике это влечет за собой:

– использование нетиповых физических топологий

– большое число устройств специального назначения с ограниченной функциональностью

– большое количество устаревшего оборудования

– сложности установки антивирусных средств

– недостаточные механизмы авторизации, аутентификации, логирования, мониторинга и т.д.

Учет особенностей функционирования АСУ ТП существенно затрудняет создание эффективной системы защиты. Однако это вовсе не означает, что реализовывать меры защиты не нужно. Возможные последствия от угроз, связанных с использованием вредоносного программного обеспечения, известные инциденты со Stuxnet и Duqu свидетельствуют об обратном. Построение комплексной системы защиты АСУ ТП позволяет минимизировать риски информационной безопасности.

Построение системы защиты должно начинаться с понимания назначения, функционала и особенностей работы АСУ ТП. На первом этапе составляются перечень бизнес-процессов, реализуемых системой, описания информационных потоков, выявляются «узкие» места, потенциальные угрозы и нарушители. К последним могут относиться обслуживающий персонал, аудиторы и контролеры, администраторы и ИТ персонал центрального офиса, лица, официально допущенные в контролируемую зону, разработчики, хакеры, лица, осуществляющие коммерческую разведку и другие.

Затем выявляются факторы, которые способствуют реализации угроз нарушения свойств доступности, целостности и конфиденциальности информации, обрабатываемой в АСУ ТП. На практике самыми распространенными уязвимостями являются:

– предоставление удаленного доступа в технологическую сеть

– несоблюдение правил сегментации сети

– недостаточные требования по безопасности к службе поддержки и разработчикам

– ошибки администрирования и известные уязвимости программного обеспечения

– возможность установки модифицированной прошивки PLC или несанкционированной смены настроек

– использование паролей по умолчанию

– недостаточное использование средств аутентификации, шифрования, контроля целостности и т.д.

Результатом анализа бизнес-процессов, угроз, уязвимостей и потенциальных нарушителей должны стать требования к обеспечению информационной безопасности. Они должны основываться не только на особенностях работы АСУ ТП и бизнес-процессов, но также учитывать требования законодательства и регуляторов. Целесообразно использовать рекомендации международных стандартов и практик. Сформированный подход к обеспечению информационной безопасности АСУ ТП должен быть комплексным и включать требования к реализации организационных, технических, физических и технологических мер защиты.

На основании сформированных требований осуществляется проектирование системы защиты и ее дальнейшее внедрение. Проектируемая система должна охватывать все уровни функционирования АСУ ТП:

– IP сети — на данном уровне должны использоваться стандартные механизмы защиты сетевой инфраструктуры (межсетевое экранирование, антивирусная защита, патч- менеджмент, IPS, VPN, DMZ и другие). Выбор средств защиты определяется на основании предъявленных требований к мерам, средствам и процессам обеспечения информационной безопасности АСУ ТП.

– PLC, датчики, устройства и инструменты, обеспечивающие реализацию технологического процесса. Защита на данных уровнях, осуществляется в соответствии со стандартами безопасности производителей оборудования и общим подходом к обеспечению информационной безопасности АСУ ТП.

С целью совершенствования системы защиты необходимо обеспечить регулярное проведение аудита, анализа рисков, анализа эффективности мер защиты. Данные процессы должны охватывать все направления, которые могут прямо или косвенно влиять на защищенность АСУ ТП. Это позволит своевременно реагировать на новые угрозы и уязвимости АСУ ТП.

Внедрение комплекса организационных мер, технических средств и процессов управления информационной безопасности АСУ ТП позволит минимизировать риски, связанные с прямыми финансовыми и репутационными потерями, остановками или нарушениями технологического процесса, ущербом окружающей среды, а также возможными человеческими жертвами.

ЗАО НИП «ИНФОРМЗАЩИТА»
127018 Москва, ул. Образцова, д. 38
Тел.: (495) 980-2345
E-mail: market@infosec.ru
www.infosec.ru

[1] Статистика 2010: Защита объектов критической инфраструктуры в России и мире. Угрозы и их последствия на примере кибератаки на ядерный завод в Иране

SIEMENS

Современные методы и средства обеспечения безопасности и защиты информации КВО на основе решений Siemens

Степанов Александр Васильевич, ведущий специалист отдела промышленности

В последнее время безопасность систем автоматизации в промышленности широко освещается в печати и не всегда в положительном свете. Разумеется, вопрос промышленной IT-безопасности привлекает повышенное внимание пользователей систем. Насколько велика опасность и какую стратегию защиты выбрать?

Безопасность систем автоматизации оставалась одним из наиболее важных вопросов еще до недавних крупных хакерских атак. Производители и пользователи всегда были хорошо осведомлены о возрастающих рисках в связи с увеличением сетевых коммуникаций и открытости технологий. Однако в повседневной работе об этом часто забывают. Информационная безопасность включает в себя гораздо больше, чем просто установку системы защиты доступа. Не менее важны информированность пользователей и всеобъемлющая концепция защиты от возможных атак и угроз.

Концепция «эшелонированной защиты»

Суть данного подхода состоит в концепции «эшелонированной защиты» — понятии, которое на самом деле является военным термином. В отношении IT-технологий эшелонированная защита включает набор мероприятий, создающих ряд препятствий для злоумышленников, для преодоления которых требуется большое количество времени и интеллектуальных ресурсов. Такие мероприятия варьируются от постоянной защиты доступа и контролируемого управления производственными процессами до строгого управления паролями. Кроме этого, они, разумеется, включают все известные технические меры, защищающие систему от внешних и внутренних угроз, например, от ошибок оператора и неавторизированного доступа.

Первый уровень защиты в большей мере связан с физической, нежели информационной безопасностью. Возникают вопросы: существует ли контроль доступа на территорию предприятия, и каким образом он осуществляется? Закрыты ли серверные помещения? Надежно ли защищены сетевые соединения? Кто должен, а кто может иметь доступ к системе? Подобные основные вопросы должны быть частью любой концепции безопасности. Не менее важны четкие и подробные инструкции для сотрудников, чтобы при повседневном использовании системы исключить риск распространения вирусов, например, троянских программ через USB-носители.

Следующие два уровня безопасности являются базовой частью архитектуры системы автоматизации. К ее центральной функции относится сегментирование техпроцессов на отдельные ячейки безопасности, которые продолжают функционировать даже в случае временной потери связи с другими подсетями. К тому же, все коммуникации с внешним миром должны происходить через организацию DMZ (демилитаризованных зон) во избежание прямого доступа к системе. Безопасность ячеек контролируется системой ограничения доступа. Связь между отдельными ячейками осуществляется через защищенное соединение с помощью VPN-каналов.

Пример сегментации сети с помощью концепции защиты ячеек аппаратным способом

Коммуникационные процессоры (CP) для ПЛК и ПК с функцией "Security Integrated" (firewall, VPN) могут быть использованы для защиты контроллеров и ячеек автоматизации наряду с сетевыми устройствами безопасности (SCALANCE S).

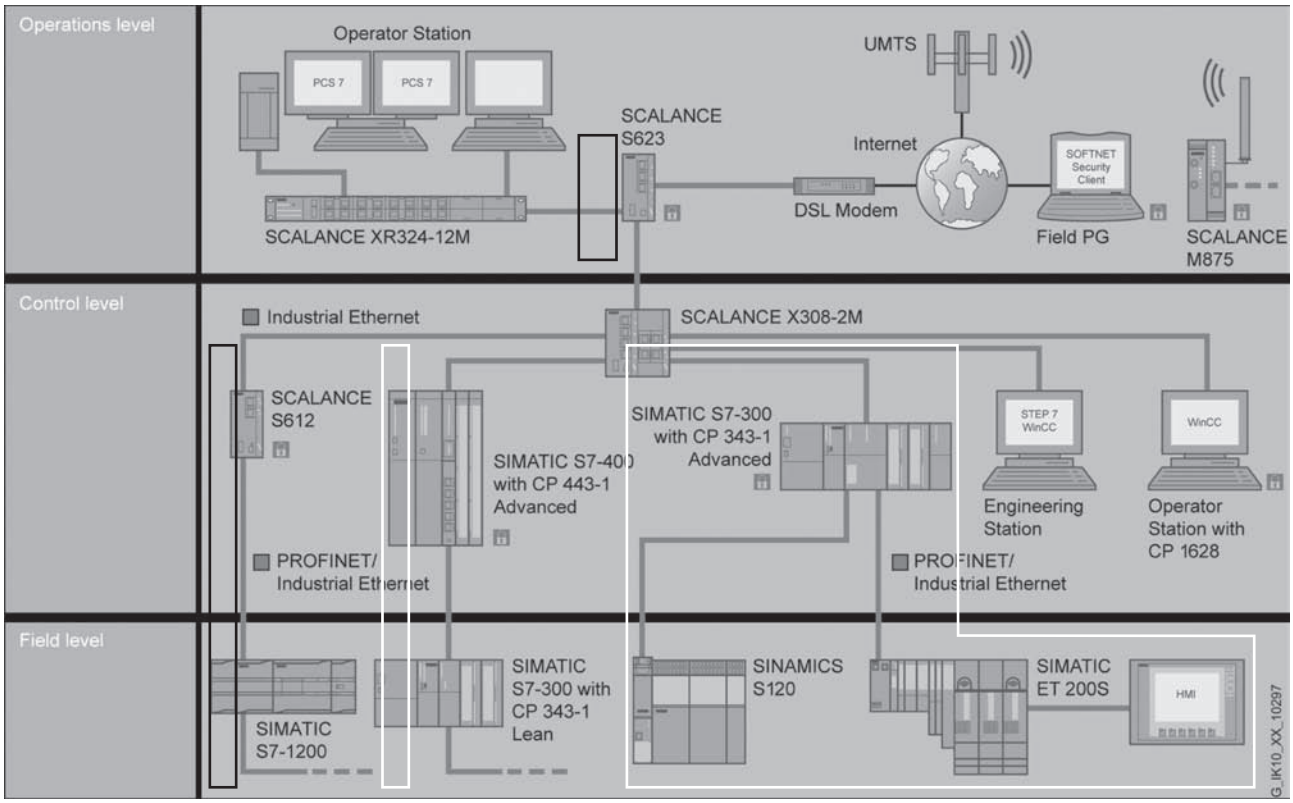
Усиленные системы безопасности и постоянное обновление

Так как каждый интерфейс, хотя бы теоретически, имеет точку доступа, позволяющую осуществлять атаку, разработчики системы должны всегда уточнять, какие порты и накопители действительно необходимы. Система укрепления безопасности удаляет все ненужные программные компоненты, деактивирует все неиспользуемые порты, накопители и интерфейсы, чтобы устранить возможные точки атаки и закрыть потенциально опасные каналы связи. Строгое управление учетными записями дополнительно гарантирует, что каждый пользователь системы получит только те права, которые необходимы непосредственно для выполнения его работы. И, разумеется, пароли должны быть надежными, а пользовательские данные постоянно обновляться и проходить проверки. Файлы патчей для устранения ошибок защиты и обновления системы должны регулярно копироваться. Строгие меры безопасности являются основой системы обнаружения сетевых атак и позволяют выявлять вредоносные программы или устанавливать связь только с надежными программами (вайтлистинг).

Концепция промышленной безопасности от Siemens

Концепция промышленной безопасности от Siemens базируется на пяти ключевых пунктах, которые покрывают главные аспекты защиты:

– Внедрение практического и комплексного **управления безопасностью** в понятиях используемой технологии, также как и процессов инжиниринга и производства.



Защита ячейки с сетевым устройством (SCALANCE S) **Защита ячейки с Security Integrated PC/PLC-CPs**

– **Интерфейсы** к офисной IT и Интернет/Интранет подчиняются четко определенным предписаниям — и контролируются соответственно.

– **ПК-базированные системы** (HMI, инжиниринг и ПК-контроллеры) должны быть защищены антивирусным ПО, вайтлистингом (позитивные списки) и интегрированными механизмами безопасности.

– **Уровень управления** защищается:

• автоматически активированными функциями защиты, интегрированными в компоненты автоматизации и приводов;

• функциями, которые активируются программистом — например, установка паролей доступа.

– **Коммуникации** должны контролироваться в целях обнаружения вторжений и быть разумно сегментированы с помощью шлюзов.

Новые продукты Siemens для сетевых коммуникаций

Защита промышленных коммуникаций и снижение риска атак является одним из ключевых факторов обеспечения безопасности. Для этого компанией Siemens предлагается ряд модулей безопасности и программное обеспечение, а также компоненты с элементами Security Integrated (встроенной безопасности) для реализации концепции защищенных ячеек.

– Сетевые модули SCALANCE S, например, S623 с дополнительным портом DMZ, который открывает отдельную и, при необходимости, ограниченную точку доступа для сервисных целей, например — удаленное обслуживание через Интернет.

– Программное обеспечение SOFTNET Security Client, обеспечивающее доступ через Интернет или Интранет компании к ячейкам автоматизации или ПК, защищенным модулями SCALANCE S или компонентами с Security Integrated.

Security Integrated

– Защита контроллеров серий SIMATIC S7-300 и S7-400 с помощью коммуникационных процессоров CP 343-1 Advanced и CP 443-1 Advanced, последние версии которых имеют функциональность firewall и VPN.

– С помощью коммуникационного процессора CP 1628 промышленные ПК защищаются firewall и VPN — для безопасных коммуникаций без специальных настроек операционной системы. Компьютеры, оборудованные данным модулем, могут подключаться к защищенным ячейкам.

– SCALANCE M875 3G роутер для безопасного доступа к производственным участкам через мобильную беспроводную сеть 3G.

Заключение

• Промышленная безопасность является не только вопросом технической реализации; она начинается с осознания важности безопасности на всех уровнях менеджмента и работниками.

• Безопасность — это постоянный процесс, который должен учитываться во всех фазах жизненного цикла производства.

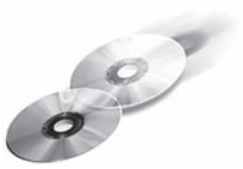
• В зависимости от определенных рисков, присущих системе автоматизации, должны быть приняты и регулярно контролироваться соответствующие организационно-технические меры.

• Siemens Industry Automation предоставляет продукты и системы, а также сервис для обеспечения полноценных решений по промышленной безопасности для наших заказчиков.

SCALANCE S 602

SCALANCE S 612

SCALANCE S 613



SOFTNET Security Client VPN

Firewall VPN	**Фильтрация IP-, MAC адресов и портов аутентификация, целостность данных**

Представительство ООО «Сименс» в Республике Беларусь
220004 Минск ул. Немига, 40, офис 604
Тел.: (017) 217-34-84
Факс:(017) 210-03-95
E-mail: minsk-office.cd@siemens.com
www.siemens.by

Новая функциональность межсетевого экрана ASA 5500-X Next-Generation Mid-Range Security Appliances

Продолжая развивать свою широко известную стратегию информационной безопасности Cisco SecureX, компания Cisco оснастила самый популярный в мире межсетевой экран Cisco Adaptive Security Appliance новой функциональностью Cisco® ASA CX (решение для информационной безопасности, учитывающее контекст). Это решение выводит платформу Cisco ASA далеко за пределы возможностей, доступных для современных межсетевых экранов "нового поколения", позволяя гораздо лучше распознавать угрозы и очень гибко настраивать правила доступа для различных приложений. Cisco ASA CX дает возможность сетевым администраторам определять, какие именно устройства и пользователи имеют право получить тот или иной тип доступа к сетевым ресурсам, а также к тысяче с лишним приложений и 75 тысячам микроприложений.

Кроме того, Cisco обновила средние модели своих межсетевых экранов, сделав их в 4 раза более производительными и в корне поменяв их архитектуру, которая теперь может быть расширена новой функциональностью без особых усилий и без необходимости установки аппаратных модулей. Если прибавить к этому решение Cisco TrustSec® и платформу управления политиками Cisco Identity Services Engine (ISE), то вполне уместно сказать, что компания Cisco в очередной раз подняла отраслевую планку информационной безопасности на качественно новый уровень.

Потребности современного бизнеса изменили облик сетевой безопасности. Предприятиям приходится поддерживать все больше типов пользователей: обычных сотрудников, субподрядчиков, а иногда и партнеров из числа конкурентов, — предоставляя им все более широкий доступ к приложениям, устройствам и другим ресурсам. В этих обстоятельствах предприятие должно гарантировать, что доступ к приложениям, данным и сервисной функциональности будут получать только пользователи с соответствующими полномочиями, для остальных же эти ресурсы должны быть закрыты. Таким образом, традиционные модели информационной безопасности устарели, и ИТ-отделам приходится искать золотую середину между производительностью и безопасностью.

Предложения Cisco в области информационной безопасности устраняют противоречие между безопасностью и производительностью, позволяя совершенствовать и то, и другое. В результате компании получают возможность повысить мобильность своих сотрудников и снизить риски, свойственные "предприятиям без границ". Cisco предлагает рынку уникальное мощное сочетание средств управления, позволяющих учитывать малейшие детали контекста, идентификации, политик и интеллектуальных функций. Это решение поможет предприятиям ускорить развитие бизнеса и поддержать нужный уровень информационной безопасности для всех устройств во всех сегментах корпоративной сети.

Cisco ASA CX — решение нового поколения для информационной безопасности с учетом контекста

Это решение расширяет платформу ASA, еще выше поднимая отраслевую планку прозрачности и глубины детализации систем управления. Cisco ASA CX распознает более тысячи приложений, таких как Facebook, Google+, LinkedIn, Twitter и iTunes, и подразделяет их на 75 тысяч с лишним микроприложений. Затем все микроприложения сводятся в простые для понимания категории, что позволяет администраторам межсетевых экранов легко разрешать или запрещать доступ к тем или иным частям "большого" приложения (к примеру, микроприложения Facebook распределяются по категориям "бизнес", "сообщество", "образование", "развлечения", "игры" и т.д.). В результате ИТ-отделы получают возможность предоставлять пользователям доступ к большему количеству приложений, сводя к минимуму число абсолютных запретов.

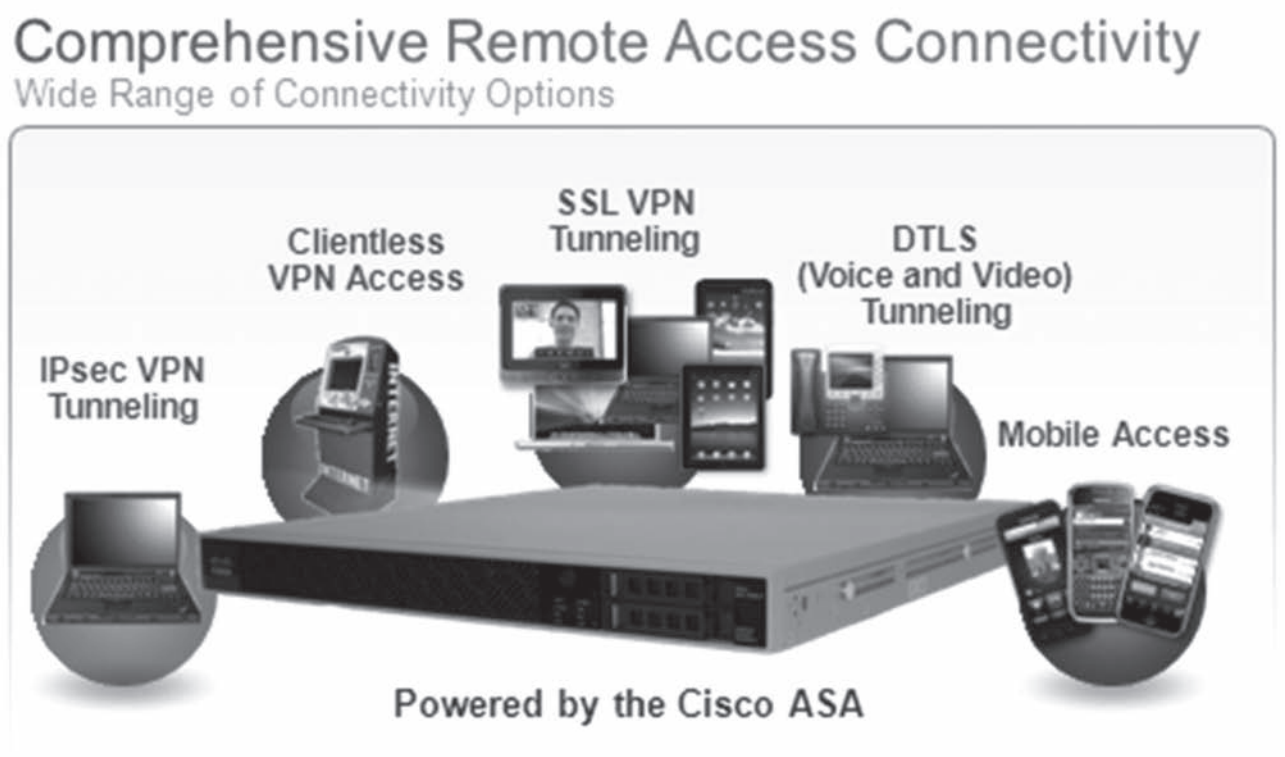
Cisco ASA CX использует широкие возможности сетевой архитектуры безопасности Cisco SecureX Framework, учитывающей контекст и работающей в унифицированных сетях доступа, граничных сетях, сетях корпоративных подразделений и центров обработки данных, а также в облачных сетевых сегментах. Эта архитектура полностью поддерживается продуктами и услугами Cisco для информационной безопасности.

Cisco ASA CX отличается от всех других межсетевых экранов. Только это решение использует систему SecureX для получения полного доступа к интеллектуальным сетевым функциям и агрегации данных, поступающих из локальной сети, с помощью системы Cisco AnyConnect Secure Mobility, а также для получения информации о хакерских угрозах в режиме, близком к реальному времени, из глобального центра Cisco Security Intelligence Operation (Cisco SIO), непрерывно предоставляющего заказчикам Cisco самый высокий уровень защиты.

Это решение дает сетевым администраторам возможность устанавливать устройства и приложения с высоким уровнем защиты и управляемости. Администраторы получают четкие данные о типе устройства, установленной на нем операционной системе, местоположении устройства и текущем уровне безопасности.

Решения Cisco TrustSec и Cisco ISE

Решения Cisco TrustSec 2.1 и ISE 1.1 дают пользователю полное представление о сети с помощью новых датчиков, интегрированных в сетевую инфраструктуру для автоматического распознавания и классификации всех подключенных к сети устройств. Кроме того, решение ISE 1.1 предоставляет в реальном времени результаты целенаправленного сканирования оконечных устройств в соответствии с принятыми политиками, что позволяет еще лучше и точнее классифицировать сетевые устройства. Вместе взятые эти решения выдают самое точное и полное представление обо всей корпоративной инфраструктуре, независимо от ее размеров. Помимо этого, TrustSec 2.1 расширяет поддержку новаторской технологии Cisco Security Group Access (SGA), предоставляющей пользователю возможность детального управления политиками в проводных и беспроводных сетевых инфраструктурах.



Средние модели устройств безопасности Cisco ASA 5500-X

В состав семейства новых высокопроизводительных устройств нового поколения для информационной безопасности Cisco ASA входят модели ASA 5512-X, 5515-X, 5525-X, 5545-X и 5555-X, оптимизированные для установки в граничных сегментах сетей, предоставляющих доступ в Интернет как малым, так и большим предприятиям. Учитывая контекст с помощью архитектуры Cisco SecureX Framework, эти устройства поддерживают множество услуг информационной безопасности без установки дополнительных аппаратных модулей, работают на мультигигабитных скоростях, предоставляют широкий выбор интерфейсов и обладают резервными блоками питания — и все это заключено в компактный корпус 1RU. В качестве опции предлагается более широкая и глубокая защита сети с помощью интегрированных облачных и виртуализированных программных сервисов информационной безопасности, поддерживаемых центром анализа сетевых угроз Cisco SIO.

Сертификация в области информационной безопасности

Cisco обновила программы сертификации в сфере информационной безопасности — Cisco CCNA® Security, Cisco CCNP® Security и Cisco Security Specialist. Теперь эти программы включают изучение систем ASA и предоставляют обучаемым знания и практические навыки, учитывающие передовой опыт лучших специалистов по сетевой безопасности, инженеров и экспертов, использующих новейшее оборудование, устройства и решения Cisco.

Вместо того, чтобы сосредотачиваться исключительно на межсетевом экране, компания Cisco учитывает широкий контекст, в котором межсетевой экран выступает как живая, активная и динамичная часть отлично защищенной сети, — говорит Кристофер Янг (Christopher Young), старший вице-президент компании Cisco возглавляющий подразделение информационной безопасности и взаимодействия с государственными органами. — Cisco встраивает функции информационной безопасности в саму сеть, используя ее уникальные возможности в области учета контекста, интеллектуальных сервисов и управления. Никакая другая часть вашей инфраструктуры не имеет таких широких знаний о происходящем, как сеть. Мы приступаем к активному использованию этих знаний и начинаем с межсетевого экрана.

Cisco ISE предоставляет нашей компании лучшее в своем классе решение для информационной безопасности с удивительно тонкой настройкой, дающей нам полное представление о пользователях без установки дополнительного оборудования, — отметил Дэвид Кеннеди (David Kennedy), вице-президент компании Diebold, Inc. и главный директор по безопасности. — Cisco — давний доверенный поставщик компании Diebold, где безопасность считается неотъемлемой частью корпоративной культуры. Мы правильно сделали, поручив Cisco решение своих задач в области глобальной сетевой безопасности. Решение Cisco ISE позволило нам упростить управление корпоративной безопасностью и помогло надежно идентифицировать и защитить каждого пользователя и каждое устройство, подключаемое к нашей сети.

Решения Cisco AnyConnect, ASA, ASA CX и IronPort позволили нам реализовать давнюю мечту — создать систему информационной безопасности, в которой все компоненты взаимодействуют друг с другом и работают как единое целое, — заявил Ник Янг (Nick Young), менеджер по поддержке сетей из компании Four Seasons Healthcare (FSHC). — Использование продуктов Cisco для информационной безопасности помогло нам упростить управление, повысить прозрачность

Продолжение читайте на 46 стр.

ВирусБлокАда

Построение эффективных систем информационной безопасности АСУ ТП на базе комплексного подхода.

Резников Юрий Геннадьевич, руководитель группы технической поддержки компании ОДО «ВирусБлокАда»

В современном мире системы автоматизированного управления технологическими процессами (далее АСУ ТП) приобретают все большее значение. Каждый аспект жизни человека претерпевает автоматизацию, глобализацию, что вызвано постоянным ростом скорости и удобства жизни и работы человека. Количество информации в таких условиях увеличивается в геометрической прогрессии. Развитие технологий и методов управления способствовало превращению АСУ ТП из изолированных устройств управления в промышленные сети на базе стандартных сетевых протоколов. АСУ ТП все больше стали напоминать корпоративные сети с их хорошо известными угрозами и уязвимостями. Компьютерные вирусы, хакерские атаки, сбои программного обеспечения, DoS и другие распространенные типы атак уже реально влияют на производственные процессы, и количество инцидентов с каждым годом неуклонно растет.

Суть комплексного подхода к обеспечению Информационной безопасности

В настоящее время в Республике Беларусь действует закон "Об информации, информатизации и защите информации", который ставит следующие цели защиты информации (статья 27):

- обеспечение национальной безопасности, суверенитета Республики Беларусь;
- сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;
- обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Данные цели позволяют говорить о том, что одной из основных задач защиты информации, наряду с обеспечением собственно целостности, доступности, конфиденциальности и сохранности информации, является обеспече-

Начало читайте на 45 стр.

и лучше реагировать на требования бизнеса. Мы перестали думать о том, что можно или нельзя разрешать, и сосредоточились исключительно на пресечении несанкционированных действий. С нетерпением ждем новых решений, способных управлять всеми перечисленными устройствами через единую глобальную консоль.

Решение Cisco ASA 5500-X отлично подходит для межсетевого экранирования с высокой производительностью и поддержкой множества услуг информационной безопасности, одновременно работающих на межсетевом экране, — утверждает президент корпорации Little eArth Corporation Co., Ltd. (LAC) Осаму Саито (Osamu Saito). — Устройства Cisco ASA превосходят наши требования к межсетевым экранам и системам предотвращения вторжений (IPS), работающим на одном устройстве. Мы с удовольствием используем устройства ASA в своем японском центре информационной безопасности и с их помощью предоставляем самый высокий уровень защищенности организациям, работающим на территории Японии.

Медицинский центр Sentara стремится предоставлять своим пациентам услуги самого высокого качества, — говорит Чад Спирс (Chad Spiers), директор компании Sentara Healthcare, отвечающий за инфраструктуру для передачи голоса и данных. — Cisco ISE полностью соответствует нашим высоким стандартам информационной безопасности, повышения эффективности операций и удовлетворения нормативных и законодательных требований. Использование стандарта 802.1x позволяет поддерживать динамический авторизованный пользовательский доступ, распознавать клинические данные, не допускать их смешивания с обычными пользовательскими данными и блокировать передачу медицинских данных на сотни устройств, многие из которых подчиняются требованиям FDA и регулируются поставщиками.

Cisco и Xerox развивают решение TrustSec, чтобы правильно отреагировать на взрывообразный рост количества персональных устройств, используемых на рабочем месте, — заявил Рик Дастин (Rick Dastin), президент подразделения корпорации Xerox по разработке продукции для корпоративного сектора. — Чтобы защитить конфиденциальную информацию, компаниям нужно в первую очередь защитить сетевые оконечные устройства: принтеры, планшетные компьютеры, веб-камеры и так далее, — и незамедлительно внедрить политики информационной безопасности. TrustSec дает ИТ-менеджерам возможность автоматически идентифицировать, отслеживать и контролировать все устройства из центральной точки. TrustSec обеспечивает надежную защиту входящих и исходящих каналов на этих устройствах.

Cisco Systems Holding BV,
Представительство в Республике Беларусь
220034, г.Минск, ул. Платонова, 1Б,
Бизнес-центр «Виктория Плаза»
E-mail: pburba@cisco.com
Сайт: www.cisco.com

ние БЕСПЕРЕБОЙНОЙ работы организации, в том числе и АСУ ТП.

В связи с этим комплексным подходом к обеспечению информационной безопасности (далее ИБ) в АСУ ТП можно назвать подход, который рассматривает работу АСУ ТП на уровне работы компьютерной сети и строится на обеспечении в первую очередь БЕСПЕРЕБОЙНОСТИ работы такой системы.

Этапы комплексного подхода обеспечения ИБ АСУ ТП

Средства управления, считающиеся важными для любой организации с точки зрения

стандарта ISO/IEC 27002, следующее:

- защита данных и секретность личной информации
- защита организационных записей
- права на интеллектуальную собственность

С точки зрения безопасности АСУ ТП можно сказать, что защита прав на интеллектуальную собственность не является приоритетной.

Средства управления, считающиеся общей практикой в области защиты информации, включают в себя (согласно стандарту ISO/IEC 27002):

- программный документ в области защиты информации;
- распределение обязанностей по защите информации;
- осведомленность, образование и подготовка по защите информации;
- правильная обработка в приложениях;
- управление технической уязвимостью;
- менеджмент непрерывности бизнеса;
- управление инцидентами и улучшениями в системе защиты информации.

Данные положения полностью соответствуют постановлению №675 Совета Министров Республики Беларусь "О некоторых вопросах защиты информации". В данном документе политика информационной безопасности — это совокупность документированных правил, процедур и требований в области защиты информации, действующих в организации и содержащих:

- цели построения системы защиты информации;
- перечень защищаемых сведений;
- определение ответственности субъектов информационных отношений за обеспечение защиты информации;
- определение прав и порядка доступа к защищаемой информации (субъектам информационных отношений предоставляется объективно необходимый для них уровень доступа к защищаемым сведениям);
- правила доступа к сетям общего пользования, в том числе глобальной сети Интернет;
- порядок работы с электронной почтой и другими системами обмена, передачи сообщений;
- порядок применения технических средств защиты и обработки информации;
- организационные мероприятия по разграничению доступа к техническим средствам защиты и обработки информации;
- порядок действий при возникновении угроз обеспечению целостности и конфиденциальности информационных ресурсов, в том числе чрезвычайных и непредотвратимых обстоятельств (непреодолимой силы), и ликвидации их последствий;
- инструкции для субъектов информационных отношений, регламентирующие порядок доступа к ресурсам информационной системы, установления подлинности субъектов, аудита безопасности, резервирования и уничтожения информации, контроля за целостностью защищаемых сведений, защиты от вредоносного программного обеспечения и вторжений.

Все положения, описанные в данных определениях справедливы и для АСУ ТП, что влечет за собой вывод об унификации методов обеспечения ИБ в офисных и производственных сетях организаций.

Рассмотрим основные этапы комплексного подхода к обеспечению ИБ АСУ ТП:

1. Построение эффективной политики информационной безопасности, согласно определению;
2. Реализация положений политики информационной безопасности в соответствии с «лучшими практиками» описанными в ISO IEC 27000;
3. Непрерывный аудит выполнения политики безопасности с целью её улучшения.

Реализация положений политики информационной безопасности

Реализацию положений политики информационной безопасности можно разбить на следующие этапы:

- реализация физическими средствами обеспечения информационной безопасности (охранные системы, системы видеонаблюдения и т.д);
- реализация организационными мерами обеспечения информационной безопасности (инструкции и директивы);
- реализация программно-техническими средствами обеспечения информационной безопасности (антивирусы, брандмауэры, и т.д);

При реализации положений политики безопасности необходимо учитывать следующие факторы:

- Модели нарушителей для конкретной информационной системы.
- Возможные методы нарушения безопасности информационной системы.

Модели нарушителей для АСУ ТП

Компьютерная группа экстренной готовности США (US-CERT) выделяет следующие типы нарушителей для систем АСУ ТП:

- Враждебные государства;
- Террористы;
- Промышленные шпионы и организованная преступность;
- Хактивисты;
- Хакеры.

Помимо этих групп можно выделить внутренних нарушителей, которые имеют физический доступ к оборудованию, что облегчает процесс нарушения информационной безопасности объекта.

Среди внутренних нарушителей можно выделить следующие типы:

- Халатный
- Манипулируемый
- Обиженный
- Нелояльный
- Подрабатывающий
- Внедренный

Группы внешних нарушителей.

Враждебные государства.

Программы кибер-оружия враждебных государств могут наносить ущерб в широком спектре областей, от практически безобидной пропаганды и дефейса вебстраниц до атак, целями которых являются максимальные людские жертвы и нарушение инфраструктуры. Кибер- войны являются самой опасной угрозой, поскольку их цель состоит в ослаблении или полном уничтожении инфраструктуры государства. По прогнозам US-CERT, в ближайшие 5-10 лет данный тип нарушителей станет преобладающим.

Террористы.

Основной целью террористов является зарождение паники среди населения, однако ввиду того что традиционные терракты (взрывы, захваты и т.д) производят больший эффект, чем кибер-атаки, террористы в ближайшем будущем представляют ограниченную угрозу информационной составляющей АСУ ТП.

Промышленные шпионы и организованная преступность.

Монетизация нарушений — основная задача данной группы. Нарушения могут включать подрыв инфраструктуры для преимущества конкурентов, нарушения доступности, конфиденциальности и целостности информации.

Хактивисты.

Хактивисты — маленькая группа настроенных против государства людей, основной целью которых является поддержка своего политического кредо. О серьезных атаках на инфраструктуру речь в большинстве случаев не идет.

Хакеры.

Хакеры, как ни странно, несут наибольший ущерб, вызванный их многочисленностью. Цели данной модели нарушителя варьируются от легальных (интерес, улучшение защищенности атакуемого объекта) до нелегальных (компрометация АСУ ТП, кража информации, предоставление нелегального доступа к АСУ ТП).

Хакеры могут быть разделены на следующие группы:

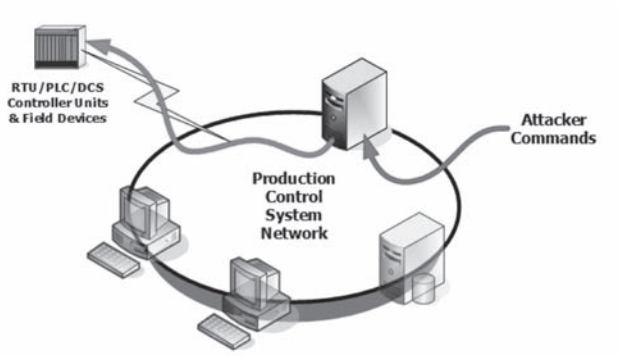
- Сообщества хакеров
- Неопытные хакеры (или script kiddies), которые не ищут уязвимости, а пытаются использовать найденные до них, зачастую уже закрытые.
- Вирусописатели и разработчики вредоносного программного обеспечения, целью которых является приобретение известности за счет вывода из строя компьютеров и сетей атакуемого предприятия.
- Исследователи безопасности, желающие получить вознаграждение после предоставления информации о взломе службе безопасности атакуемой организации.
- Профессиональные хакеры-злоумышленники, разработчики программного обеспечения для проникновения в сети атакуемой организации.

Методы атак на АСУ ТП

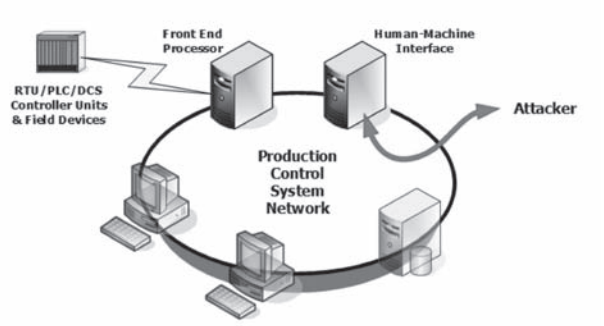
Рассмотрим некоторые из возможных способов атак на АСУ ТП.

Прямая отправка команд оборудованию.

Самый простой способ управления промышленным оборудованием, поскольку большинство ПЛК, преобразователей протоколов или серверов сбора данных не подразумевают аутентификации пользователей, и злоумышленнику достаточно просто установить связь с системой для того, чтобы её скомпрометировать.

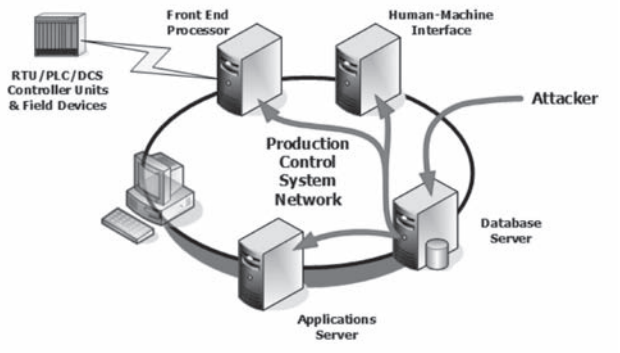


Перехват экрана управления АСУ ТП



Такая атака заключается в том, что атакующий способен с помощью специализированных утилит (не обязательно вредоносных) перехватить экран управления АСУ ТП. В этом случае оператор будет видеть движение мыши на экране, вызванное злоумышленником, а злоумышленник будет ограничен правами текущего пользователя-оператора АСУ ТП.

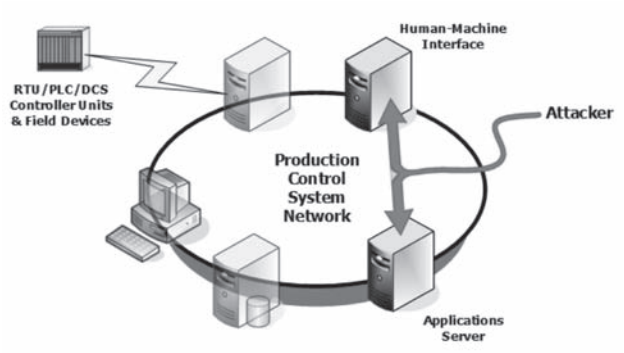
Внесение изменений в базу данных (БД)



Некоторые АСУ ТП позволяют изменить работу подконтрольной системы изменением базы данных.

Атаки типа "Man-in-the-middle"

Атаки подобного рода могут быть осуществлены в случае, если атакующему известны технические детали функционирования АСУ ТП. В этом случае он может одновременно подменять информацию на экране управления и получить полный контроль над атакуемой системой.



Идея эшелонированной защиты АСУ ТП

При реализации положений политики безопасности очень важно соблюдение комплексного подхода к обеспечению информационной безопасности, поскольку ни один отдельный аспект сам по себе не способен обеспечить полной защиты АСУ ТП. При построении защиты необходимо принять решение по следующим вопросам:

1. Приоритеты информационной безопасности (например, целостность, конфиденциальность или доступность);
2. Четкие требования к безопасности АСУ ТП (если технологический процесс требует удаленного доступа из корпоративной сети, то следует продумать защиту такого соединения от возможных атак);
3. Ресурсы, выделяемые на защиту АСУ ТП от злоумышленников.
4. Возможные угрозы и риски (при рассмотрении конкретной АСУ ТП часть из описанных ранее угроз может стать неактуальной, например, в случае отсутствия БД в составе АСУ ТП);
5. Вид архитектуры системы безопасности (даже при наличии действующей системы в рамках АСУ ТП может быть возможность её рефакторинга с целью улучшения);
6. Описание системы безопасности в виде ПБ и прочих документов.

Идея эшелонированной защиты давно и с успехом применяющаяся при защите офисных сетей, заключается в выделении иерархических уровней, к которым применяются физические, организационные и программно-технические меры защиты.

Рассмотрим простейший пример: компьютер в составе сети, на котором установлена консоль управления АСУ ТП. К компьютеру применяем:

- Организационные меры защиты (определение сотрудников, которые могут работать на данном компьютере и их ответственность в случае нарушения безопасности по их вине);
- Физическую защиту (фактически защиту от кражи или использования не по назначению);
- Программно-техническую защиту (обновление ОС, установка оптимальных прав для пользователей, защита от вредоносных программ).

Аналогичные построения можно сделать для рабочей группы/домена, всей сети организации и объединения сетей организаций. В каждом из случаев выделение подобных мер защиты позволит упростить и одновременно повысить надежность системы информационной безопасности благодаря применению широко известного принципа декомпозиции.

Аудит информационной безопасности в АСУ ТП

Аудит информационной безопасности информационных систем можно разделить на следующие этапы:

- Инициирование процедуры аудита
- Сбор информации аудита
- Анализ данных аудита
- Выработка рекомендаций
- Подготовка аудиторского отчета

При сборе информации для аудита информационной безопасности, также как и при обеспечении положений политики безопасности, можно применять комплексный подход. Он заключается в том, что аудит ИБ в АСУ ТП можно разделить на два уровня:

1. Уровень промышленной сети. На данном уровне необходимо проверять подверженность контролирующих ОС уязвимостям, стойкость паролей, наличие привилегированных прав пользователей там, где этого не требуется, работу программно-технических средств защиты информации и т.д.
2. Уровень промышленных устройств. Из-за того, что многие из промышленных устройств управляются ОС специального назначения, но обмениваются информацией, используя стандартные протоколы связи, они уязвимы для нарушителей. Проверка и обеспечение безопасности таких устройств может в частном случае предотвратить техногенную катастрофу с большим количеством жертв.

При любом аудите (внешнем или внутреннем) целесообразно подобное разбиение, поскольку оно позволяет наиболее комплексно получить информацию о состоянии защиты аудируемой системы, в частности АСУ ТП. Результаты подобного аудита — повод для улучшения процедур и механизмов защиты информации в АСУ ТП.

При построении систем защиты информации в АСУ ТП можно заметить, что существует сходство подходов к защите информации в офисных сетях и сетях АСУ ТП. Принимая во внимание это сходство и учитывая различия в работе офисных сетей и АСУ ТП, можно использовать одинаковые методы построения систем защиты информации. Проявление различий можно устранить применением метода декомпозиции, позволяющего получить комплексную защиту системы.

ОДО «ВирусБлокАда»
220088, г. Минск, ул. Смоленская, 15, 803б
Тел.: (017) 294-84-29
E-mail: info@anti-virus.by
www.anti-virus.by

Бевалекс

Актуальные вопросы обеспечения информационной безопасности промышленных АСУ ТП

как критически важных объектов информатизации (КВОИ) с использованием ПАК «Цитадель»

Базелев Вячеслав Юрьевич,
руководитель направления
информационной
безопасности
СП «Бевалекс» ООО

1. Компьютеры ненадежны, но люди еще ненадежнее.
2. Любая система, зависящая от человеческой надежности, ненадежна.
3. Число ошибок, которые нельзя обнаружить, бесконечно в противовес числу ошибок, которые можно обнаружить, — оно конечно по определению.
4. В поиски повышения надежности будут вкладываться средства до тех пор, пока они не превысят величину убытков от неизбежных ошибок или пока кто-нибудь не потребует, чтобы была сделана хоть какая-то полезная работа.

Законы ненадежности Джилба

Производство современной конкурентоспособной высокотехнологичной продукции или предоставление ресурсов, к примеру, в топливно-энергетической сфере, невозможно представить без использования автоматизированных систем управления технологическим процессом (АСУ ТП), предназначенных для выработки и реализации управляющих воздействий на совокупность технологического оборудования и реализованных на нем по соответствующим инструкциям или регламентам технологических производственных процессов.

В настоящее время АСУ ТП характеризуются:

- унификацией и стандартизацией сетевых (общепринятых в ИТ-сфере) и индустриальных технологий (протоколов);
- созданием и внедрением АСУ ТП на базе серийно выпускаемых промышленных контроллеров, совместимых с персональными компьютерами и серверным оборудованием со специальным прикладным программным обеспечением;
- заменой аппаратных помещений на серверные или центры обработки данных (ЦОД).

На современном предприятии инженеры подразделений АСУ отслеживают работу управляемых механизмов удаленно с автоматизированных рабочих мест. При этом работа, в большинстве своём, ведется под управлением операционных систем семейства Windows, к тому же, зачастую, с возможностью одновременного доступа во внешние сети (Интернет).

Результатом этих тенденций является то, что для АСУ ТП растет вероятность осуществления угроз извне. Примером служит широко обсуждаемое появление вредоносных программ типа «flame», «duqu» и «stuxnet» («червь», созданный конкретно под Siemens SCADA-систему SIMATIC WinCC). Изнутри АСУ ТП также более уязвимы, чем прежде, — доступ к устройствам АСУ ТП могут получить всё большее количество сотрудников с использованием стандартных методов и средств сетевого доступа, растет зависимость АСУ ТП от непреднамеренных ошибок и намеренных негативных действий персонала.

Получается, что все производства с использованием АСУ ТП в степени не меньшей, чем широко распространенные компьютерные информационные системы, нуждаются в защите.

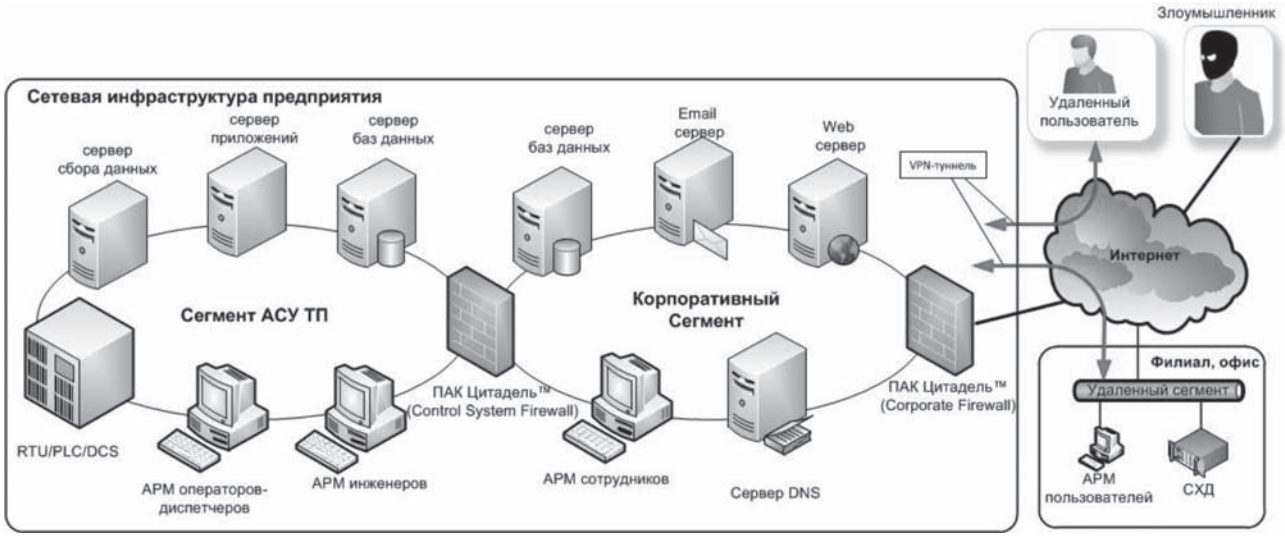


Рисунок 1. Вариант построения защищенной сетевой инфраструктуры предприятия, имеющего АСУ ТП

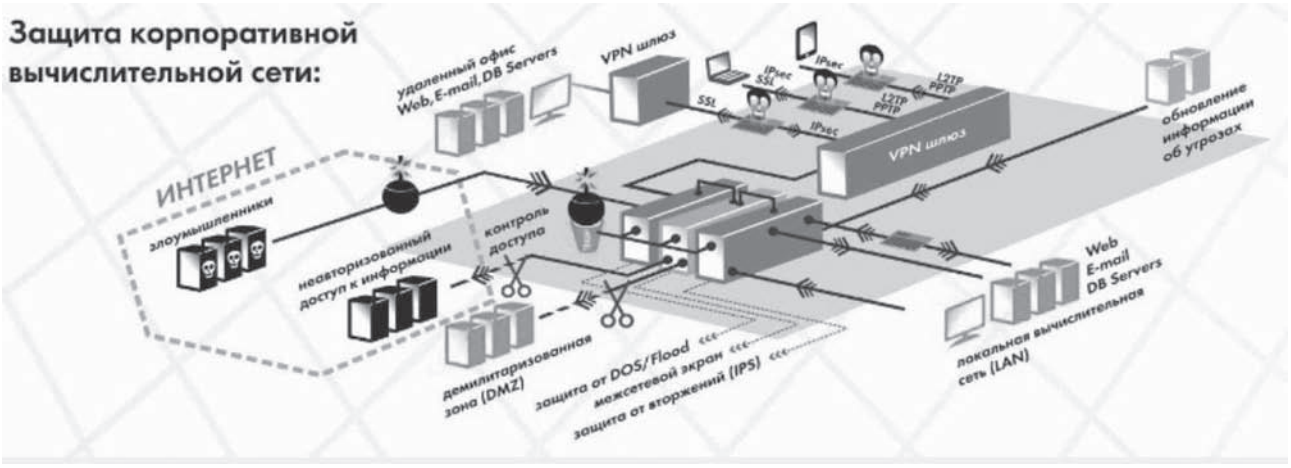


Рисунок 2. Вариант построения защищенной сетевой инфраструктуры на базе ПАК Цитадель™

Как организовать защиту АСУ ТП?

Следуя лучшим мировым практикам, при построении сетевой структуры предприятия, имеющего АСУ ТП, СП «Бевалекс» ООО предлагает пользоваться передовыми методиками в области управления ИТ и прислушаться к следующим рекомендациям:

Рекомендация 1

- *защищать корпоративную подсистему от «внешних» сетей межсетевым экраном **(Corporate Firewall)** (см. рисунок 1);*
- *отделять информационную подсистему, в которой происходит обработка данных АСУ ТП, от корпоративной подсистемы межсетевым экраном **(Control System Firewall)**.*

Указанный вариант построения защищенной системы позволит минимизировать риски, связанные с влиянием на АСУ ТП следующих видов угроз:

- подмена данных и модификация данных;
- "replay"-атаки;
- перехват информации (в том числе ключевой).

Рекомендация 2

В работе межсетевого экрана, «защищающего» сегмент АСУ ТП, акцент следует делать на обеспечение надежности, а именно: защиту от различного типа атак, направленных на выход из строя оборудования, каналов связи (DOS/DDOS, переполнение буфера, обнуление данных). А в работе межсетевого экрана, «закрывающего» корпоративный сегмент, наряду с обеспечением надежности важна защита конфиденциальных данных предприятия.

В качестве устройств, реализующих функции межсетевого экранирования, — Corporate Firewall и Control System Firewall — СП «Бевалекс» ООО предлагает использовать программно-аппаратный комплекс «Цитадель» ТУ BY 100944292.011-2011 (далее — ПАК Цитадель™) в составе:

– сервер Бевалекс™ (система менеджмента качества СТБ ISO 9001-2009);

– программное обеспечение «Astaro Security Gateway Software Network Appliance версия 8»[1], прошедшее проверку на соответствие требованиям безопасности (экспертное заключение № 281 от 19.09.2011 г. Оперативно-аналитического центра при Президенте Республики Беларусь).

При этом Intel-совместимая аппаратная платформа ПАК Цитадель™ является конфигурируемой и масштабируемой по производительности, а также количеству интерфейсов, ОЗУ, объему и RAID НЖМД, формату и типоразмеру соответственно текущим и перспективным потребностям предприятия, то есть наращиваемой согласно планируемому росту производственной нагрузки. Указанное свойство позволяет не только экономить средства предприятия при модернизации, но и относительно недорого проводить ремонт (замену) комплектующих из состава ПАК Цитадель™.

Рекомендация 3

Необходимо обеспечить высокий уровень отказоустойчивости системы и бесперебойное питание оборудования.

ПАК Цитадель™ позволяет настроить систему «горячего» резерва на случай сбоя основной системы (активно-пассивная конфигурация). А также создать кластер, распределяющий сетевой трафик между узлами в составе определенной группы (активно-активная конфигурация), с целью оптимизации использования ресурсов и ускорения вычислений (рисунок 3).

В качестве системы, обеспечивающей высокий уровень доступности, может использоваться кластер, состоящий из двух и более узлов на базе

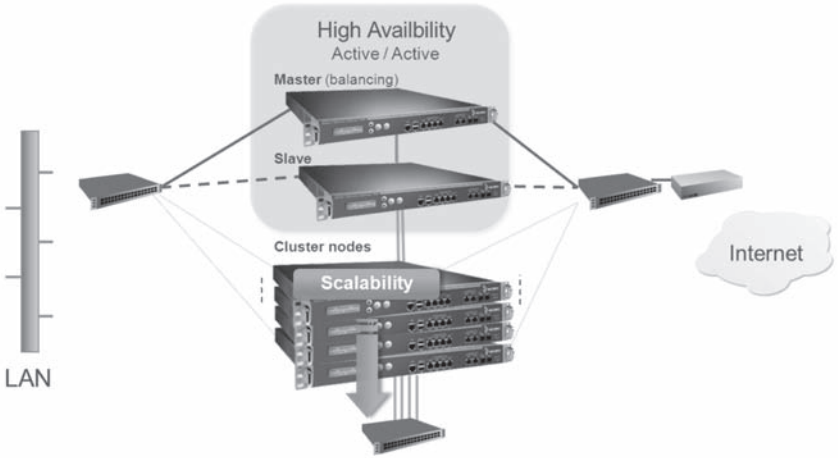


Рисунок 3. Работа ПАК Цитадель™ в режиме обеспечения отказоустойчивости

[1] Возможна поставка и установка программного обеспечения в виде виртуальной машины (сертифицировано VMware и Citrix)

ПАК Цитадель™.

Каждому узлу кластера назначается одна из следующих ролей:

– главный узел: главная система в составе кластера/конфигурации с «горячим» резервом, отвечает за синхронизацию и распределение данных.

– ведомый узел: резервная система в составе кластера/конфигурации с «горячим» резервом, принимает на себя функции главного узла в случае его сбоя.

– рабочий узел: обычный узел кластера, занимающийся только обработкой данных.

Все узлы осуществляют мониторинг состояния друг друга с помощью, так называемых, сигналов Heartbeat — периодически отправляемых многоадресных пакетов UDP, которые позволяют проверить, активен ли другой узел. Если по техническим причинам узел не отправляет этот пакет, его объявляют недоступным. В зависимости от роли, назначенной вышедшему из строя узлу, конфигурация меняется следующим образом:

– в случае сбоя главного узла его место занимает ведомый узел, а рабочий узел с самым высоким показателем готовности становится ведомым узлом;

– в случае сбоя ведомого узла его место занимает рабочий узел с самым высоким показателем готовности;

– в случае сбоя рабочего узла возможно снижение производительности по причине уменьшения количества доступных процессоров. Это событие не оказывает влияния на отказоустойчивость.

Бесперебойное питание оборудования достигается тем, что связь между устройством ИБП и ПАК Цитадель™ осуществляется через интерфейс USB. Как только устройство ИБП начинает работу с использованием батареи, администратору отправляется уведомление. Если сбой питания сохраняется в течение более длительного периода времени и напряжение устройства ИБП приближается к критическому значению, администратору отправляется другое сообщение — «ПАК Цитадель™ отключится автоматически».

Рекомендация 4

Руководителям предприятий и лицам, ответственным за информационную безопасность, стоит понимать, что построение системы информационной безопасности — это организационно-технический процесс, начинающийся с разработки соответствующих внутренних документов.

В противном случае возможно появление серьёзных инцидентов из-за, казалось бы, незначительных факторов:

– не произведённого вовремя обновления системного программного обеспечения какого-либо модуля АСУ ПК;

– доступа на территорию предприятия неуполномоченных лиц или нерегламентированного доступа сотрудников в нерабочее время;

– проведение сервисных работ с сетевыми устройствами или устройствами системы защиты информации в штатном режиме в рабочие часы.

Рекомендация 5

После выполнения всех рекомендаций вернуться к рассмотрению рекомендации №1, так как обеспечение информационной безопасности — это циклический процесс.

Подводя итог, сообщаем, что ПАК Цитадель™ включает в себя базовые функции межсетевого экранирования, NAT, удаленного доступа по протоколам PPTP/L2TP, а также опциональные дополнительные функции, активируемые исходя из потребностей пользователя.

Таким образом, для ПАК Цитадель™, в качестве Control System Firewall (см. рисунок 1), достаточно активировать функции Network Security (Сетевая безопасность). При этом будут обеспечены: защита информационной системы предприятия от различного рода сетевых атак (IPS, AntiDoS), возможность резервирования ширины канала и поддержка набора протоколов туннелирования для создания удаленных соединений (SSL Remote Access, IPSec Remote Access), интеграция с серверами Active Directory, eDirectory, RADIUS, TACACS+, LDAP). А на ПАК Цитадель™, защищающий корпоративный сегмент Corporate Firewall (см. рисунок 1), целесообразно дополнительно к Network Security возложить функции:

– Web Security (Безопасность веб-технологий) — URL-фильтрация, антивирусное сканирование при работе в веб-средах, Spyware Protection, сканирование HTTPS, IM/P2P-фильтрация.

– Mail Security (Безопасность электронной почты) — защита электронной почты, принимаемой и отправляемой из сети (Anti Spam, Antivirus, Email Encryption);

– Web Application Security (Безопасность веб-приложений) — обеспечение защиты URL-адресов от переопределения, механизмов «обратного прокси», идентификации и предотвращения использования SQL-инъекций и межсайтового скриптинга, направленных против находящихся в сети веб-серверов и их приложений;

К сожалению, это не значит, что покупка одного, двух или более устройств ПАК Цитадель™ или любого другого средства обеспечения безопасности является панацеей от инцидентов информационной безопасности. Единственный путь обеспечения комплексной и системной безопасности — отношение к информационной безопасности как к процессу.

При выборе ПАК Цитадель™ в качестве средства защиты корпоративной сети и АСУ ТП предприятие получает:

– возможность построения отказоустойчивых решений;

– возможность одновременного централизованного управления несколькими ПАК Цитадель™;

– наличие функций балансировки нагрузки;

– управление качеством сервисов (QoS, quality of service);

– гибкость в выборе функциональных модулей;

– возможность использования резервных каналов доступа во внешние сети (с поддержкой UMTS/3G-модемов);

– встроенные средства резервного копирования и восстановления;

– возможность сохранения и восстановления полной конфигурации в одном файле;

– мониторинг, анализ и полный контроль трафика, используемого отдельными пользователями, отделами, сетевыми узлами, приложениями;

– развитые средства формирования отчетов, настраиваемый уровень детализации отчетов.

При построении систем информационной безопасности СП «Бевалекс» ООО в своей работе руководствуется:

– международными стандартами и лучшими практиками (COBIT, ITIL, ISO);

– нормативно-правовыми актами Республики Беларусь;

– принципами уважения к своим клиентам.

СП «Бевалекс» ООО
220137, г.Минск, ул. Солтыса, 191
Тел.: (17) 330-16-16
Факс: (17) 330-16-30
E-mail: info@bevalex.by
www.bevalex.by

Безопасная осень 2012

Журнал «Технологии безопасности» организует ряд специализированных международных научно-практических семинаров и конференций, посвященных проблемам обеспечения комплексной (информационной и инженерно-технической) безопасности объектов различных категорий.

С участием и при поддержке ведомств: ОАЦ, НИИ ТЗИ, Национальный банк Республики Беларусь, Институт национальной безопасности Республики Беларусь, МВД Республики Беларусь, БГУИР и пр.

На сентябрь-октябрь-ноябрь 2012 г. запланировано проведение научно-практических семинаров:

1. «ЦОД: повышение технической и экономической эффективности проектирования, внедрения и эксплуатации».

2. «Современные методы и средства обеспечения комплексной безопасности нфраструктуры и процессов «облачных» технологий».

3. «PCI DSS 2.0 и PA DSS 2.0 - требования и методы обеспечения безопасного функционирования платежных систем».

4. Риски Fraud-мошенничества в деятельности операторов связи.

Приглашаем:
- профильные компании выступить в статусе соорганизатора/партнера запланированных мероприятий;
- специалистов принять активное участие в экспертном формировании программ и докладов с учетом специфики решения практических задач заинтересованных подразделений компаний и ведомств.

Подробнее на сайте **aercom.by**

Курсы повышения квалификации специалистов по проектированию, монтажу и наладке технических средств и систем охраны

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ
журнал для руководителей предприятий и специалистов отрасли безопасности

Журнал «Технологии безопасности» и «Межотраслевой институт повышения квалификации и переподготовки кадров» БНТУ реализуют совместный проект – курсы повышения квалификации специалистов по проектированию, монтажу и наладке технических средств и систем охраны.

Лекторы: Практикующие специалисты, представители производителей и поставщиков средств и систем охраны, представители ДО МВД РБ

Учебные программы соответствуют всем требованиям Совета министров и Минобразования РБ;
Максимально направлены под требования Департамента охраны МВД РБ в области лицензируемых видов деятельности.

СОДЕРЖАНИЕ КУРСА

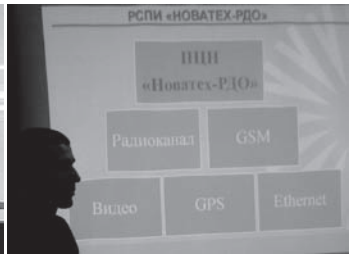
Нормативное правовое обеспечение в области проектно-монтажных работ технических средств и систем охраны
- Порядок разработки технического задания на проектирование технических средств и систем охраны;
- Состав, порядок разработки, согласования и утверждения проектной документации на технические средства и системы охраны;
- Технический надзор за выполнением проектных и монтажных работ по оборудованию объектов техническими средствами и системами охраны;
- Организация проведения монтажа и пусконаладочных работ технических средств и систем охраны.

Технические средства и системы охраны
- Технические средства и системы охраны периметра;
- Технические средства и системы охраны зданий и помещений, защищаемых объектов;
- Системы цифровой регистрации видеосигнала (системы видеонаблюдения);
- Интегрированные системы технических средств охраны;
- Современные системы передачи извещений.

Охрана труда
- Правовое обеспечение деятельности по охране труда на предприятии;
- Электробезопасность. Пожарная безопасность. Правила оказания первой помощи пострадавшим от поражения электрическим током;
- Требования безопасности при производстве работ по монтажу, наладке технических средств и систем охраны.

Контактная информация:
ООО «АэркомБел»,
Тел./факс: 017-290-84-05,
e-mail: podpiska@aercom.by
Регистрация заявок, информация
Тел.: 017-256-10-35 (47)



Сравнительный анализ систем безопасности централизованных и распределенных банковских систем обработки информации

Тепляков Анатолий Адамович, директор ЗАО «НТЦ Контакт»

Справка ТБ

Тепляков Анатолий Адамович. Образование высшее, инженер электронной техники. В 1975 году окончил Минский радиотехнический институт, в 1982 — Белорусский институт народного хозяйства по специальности инженер-экономист. Начинал работу в Минском управлении ЦНПО «КАСКАД» инженером. С 1992 по 2003 — директор НТЦ «КОНТАКТ», 2003-2007 — заместитель директора по науке Научно-исследовательского республиканского института технической защиты информации. 2007-2008 — начальник отдела безопасности УП «ИВЦ Минфина», с 2009 — заместитель директора, с 2011 — директор ЗАО «НТЦ КОНТАКТ». С 2000 года — преподаватель Академии управления при Президенте Республики Беларусь. Опыт работы по созданию систем и элементов защиты информации с 1994 года по настоящее время. Руководил разработкой более чем 20 средств и систем защиты информации, которые применяются по сей день. Автор 11 книг и пособий по защите информации.

Системы обработки информации в своем историческом развитии пережили несколько этапов. Сначала для обработки больших информационных массивов применялись майнфреймы — большие универсальные вычислительные машины. Они стоили больших денег, имели большую вычислительную мощность и обслуживали большое число пользователей. Операционная система майнфреймов была одна на всех, приложения и другие программы — тоже. И все это стоило неимоверно дорого.

С течением времени на смену майнфреймам пришли маленькие, мощные (конечно, не настолько мощные, как майнфреймы, но зато дешевые) персональные ЭВМ. Они позволили решать задачи для каждого отдельного пользователя, имели удобные интерфейсы, дешевые операционные системы, системы управления базами данных, коммуникационные пакеты и емкие накопители, объем которых постоянно возрастал. Быстро росли и вычислительные мощности процессоров. Постепенно они становились все больше и больше — причем настолько, что их мощность уже становилась избыточной для персональных вычислений. В это же время появились скоростные каналы связи. ПЭВМ начали объединять в локальные вычислительные сети, которые со временем разрослись до размеров страны. Высокая пропускная способность сетей стала позволять объединять процессоры в мощные локальные комплексы, загрузить которые одиночные пользователи уже не могли — и на сцену опять пришли централизованные вычисления, правда, на другой технологической основе. Как видим, круг замкнулся — но уже на принципиально ином, более высоком технологическом витке.

Достоинства и недостатки централизованных и распределенных вычислений в ограниченных рамках данной статьи мы рассмотрим лишь в одном аспекте, а именно — с точки зрения их влияния на создание системы защиты информации, опираясь на практический опыт одного из старейших разработчиков и производителей средств защиты информации в Республике Беларусь — закрытого акционерного общества «НТЦ Контакт».

Состав защищаемых информационных ценностей в распределенных и централизованных системах обработки информации примерно одинаков. Информационные ценности и в одной и в другой системе одни и те же: для банка — это персональные данные клиентов, классификаторы, справочники, архивы, данные систем защиты и т.п. А вот модели нарушителей в этих системах немного различаются, хотя бы из-за того, что в централизованных системах количество администраторов намного меньше, чем в распределенных.

Сравнение рисков и угроз. В централизованных системах существенными являются угрозы для центра обработки и типового пользователя. Для распределенных систем угрозы будут теми же, плюс угрозы, связанные с межузловыми обменами. При этом следует иметь в виду, что компоненты распределенной системы в узлах частично дублируются, но в ней есть и уникальные данные в узлах, которые могут быть выведены из строя, так что стоимость резервирования из-за большого количества для них высока. Централизованные системы резервировать проще — создается резервный центр, соединяемый с основными скоростными каналами связи. Конечно, затраты на это решение достаточно высоки, но в пересчете на одно рабочее место они значительно ниже, чем в распределенной системе.

Риски для сравнимых угроз в централизованных и распределенных системах приблизительно одинаковы — это риски утечки, искажения, навязывания, подмены информации и т.п. Но в распределенных системах эти риски действуют для множества различных классов пользователей, использующих различные ресурсы, в связи с чем суммарные риски возрастают. Для централизованных систем эти риски стабилизируются и являются фиксированной величиной, их гораздо проще контролировать. Например, в распределенной системе достаточно распространены случаи, когда произошел инцидент, его ликвидировали и никому об этом не сообщили. В централизованных системах это невозможно, поскольку все сведения об инцидентах накапливаются в централизованных журналах.

Кроме того, в распределенных системах чрезвычайно усложнено управление версиями. Часто поддерживается множество версий одного и того же продукта, да и продуктов обычно несколько. Поддержание одних и тех же форматов становится для распределенных систем очень большой проблемой. К примеру, всегда найдется какой-то узел, заявляющий об отсутствии средств для перехода на новую версию. Всегда может возникнуть причина, по которой версионность будет разной, а это значит, что будут неодинаковые форматы, что потребует дополнительных средств на поддержание старых форматов. Учитывая, что уровень безопасности системы определяется самым слабым звеном, синхронизация версий становится одной из важнейших и трудно разрешимых задач распределенных систем. В централизованной системе данная проблема решается просто — каждая новая версия программы инсталлируется автоматически, не требуя дополнитель-

ных организационных и человеческих ресурсов (как пример — реализованная ЗАО «НТЦ КОНТАКТ» автоматическая инсталляция новых версий криптозащиты для одного из белорусских банков).

Сравнение средств и методов защиты. В связи с тем, что риски и угрозы централизованных и распределенных систем различаются, то, безусловно, будут различаться средства и методы защиты. Поскольку, как мы уже говорили, угроз в распределенной системе больше и вероятность их реализации выше, то для нее потребуются средства защиты более высокого уровня, которые должны будут дублироваться. С другой стороны, нужно понимать, что если в распределенной системе отказал весь узел, система все равно работает — она только деградирует. То есть выживаемость распределенных систем при прочих равных условиях всегда выше. Для централизованных же систем нужно использовать дополнительные методы повышения надежности и выживаемости, например, такие, как дублирование, которое позволяет сохранить основные функции в случае отказов. Если взять живой пример из практики ЗАО НТЦ «КОНТАКТ», для решений на основе продуктов SAP AG управление открытыми ключами использует разнесенные серверы для удостоверяющих центров, работающих в режиме горячего резерва, а для исключения разрушения самих хранилищ центров хранения сертификатов их синхронные копии — репозитории — выносятся за пределы защищенной зоны, что приводит к большей устойчивости системы.

Защита от утечки информации по техническим каналам. В настоящее время значение этих каналов для любых систем чаще всего недооценивается. Однако следует иметь в виду, что в последнее время стоимость систем технической разведки сильно снизилась, а их эффективность возросла. Разведывательная аппаратура, которая десять лет назад стоила миллионы и сотни тысяч долларов, сейчас стоит на два-три порядка дешевле, т.е. становится более доступной. А это значит, что к возможности ее использования надо относиться серьезно.

Конечно, здесь основной проблемой является стоимость средств защиты. Чаще всего, в связи с необходимостью больших затрат, технической защитой пренебрегают, выполняя мероприятия по защите только госсекретов.

Если сравнивать централизованную и распределенную системы с точки зрения утечки информации по техническим каналам, то разница между ними очень велика. В распределенной системе средства защиты от утечки нужно ставить в каждой точке обработки, а в централизованной можно поставить сверхнадежную, мощную защиту в одном месте, и расходы для обеспечения одного и того же уровня защищенности одного рабочего места будут на порядок меньше. Например, при разработке ЗАО «НТЦ КОНТАКТ» системы безопасности для централизованной системы обработки данных одного из банков нам было достаточно установить всего 2 устройства защиты ПЭВМ от НСД — ПАК «Барьера» — для защиты корневых сертификатов с учетом наличия основного и резервного центров. Для распределенной системы таких устройств понадобилось бы в разы больше, соответственно, затраты увеличились бы на порядок.

Физическая защита. В централизованных системах физическая защита всегда лучше, поскольку средства затрачиваются на мероприятия, касающиеся небольшого количества пользователей, имеющих физический доступ к системе. Несмотря на то, что затраты на защиту центра больше, экономический эффект при защите централизованной системы выше, что позволяет создавать за те же деньги более качественную защиту. В ЦОДе можно ввести многофакторный контроль (например, веса входящих и видеоконтроль перемещения в защищаемых помещениях) и т.п.

Организационные решения. Конечное количество пользователей будет одинаковым в обеих системах, но в распределенной системе количество администраторов, которые поддерживают управление, естественно, будет больше (на каждом узле по администратору). И, конечно же, обеспечить качество персонала в централизованной системе будет проще, чем в распределенной.

Криптографическая защита. Одна из угроз связана с нарушением конфиденциальности информации. Решением является применение криптографических средств. Они относительно дешевы — при больших партиях составляют порядка 20-30 долларов за рабочее место. При этом основные затраты приходятся на систему управления ключевой информацией. А это значит, логично было бы вывести из отдельно взятого предприятия систему управления открытыми ключами, сделать ее общей для группы организаций. Но каждый здесь должен сам для себя решить, нужен ли ему собственный удостоверяющий центр. На сегодняшний день вся республика разбита на маленькие островки, которые управляют своими ключами сами. Необходимо было бы собрать их в единую систему. Но для создания и существования такой системы основное значение будет иметь стоимость ее сертификатов. Если цена сертификата будет низкой, будет преобладать тенденция к укрупнению систем

управления ключами. При высокой цене сертификата будет преобладать тенденция к созданию собственных систем управления. Надеяться на то, что в республике может успешно работать монопольная структура, которая будет выпускать сертификаты открытых ключей по 100 долларов США за штуку, сейчас не приходится, поскольку организация, которой нужно 1000 сертификатов в год, конечно же, скорее всего за 100 000 долларов купит собственную систему управления сертификатами и будет тратить один раз в десять лет 1000 долларов на то, чтобы купить один корневой сертификат. Экономя, таким образом, 99900 долларов США в год.

Подводя итог, можно сказать, что и централизованные, и распределенные системы обработки данных имеют свои преимущества и недостатки. Однако можно с уверенностью сказать — постепенно мы идем к централизованным вычислениям, как в малых офисных решениях, так и в больших, масштаба республики, системах. Опыт ЗАО «НТЦ Контакт» показывает преимущества централизованных систем, в том числе и в области защиты информации.

P.S. Надо понимать, что система безопасности — это всего лишь вспомогательный компонент, который помогает экономить средства за счет уменьшения количества инцидентов. Но поскольку финансирование мероприятий по безопасности осуществляется из чистой прибыли, это значит, на каждый рубль, который мы вкладываем в безопасность, мы уже заплатили как минимум два рубля налогов и иных отчислений. Поэтому как только Ваши затраты на систему безопасности начинают «съедать» более 10 процентов от стоимости того, что она защищает, по нашему мнению, ее нужно срочно оптимизировать. ■

DLP в Беларуси: пять вопросов, требующих ответов

На сегодняшний день одним из самых надежных способов защиты информации компании является установка DLP-системы. О том, каковы особенности белорусского DLP-рынка, а также о тенденциях развития систем для защиты данных, любезно согласился побеседовать Александр Акимов, генеральный директор компании **Falcongaze**, занимающейся разработками в сфере информационной безопасности.

Александр, здравствуйте, судя по всему DLP-системы пока не нашли широкого распространения в Беларуси, что же сдерживает активное применение DLP в белорусских компаниях?

Добрый день. Говорить о том, что есть какие-то особые препятствия, которые мешают распространению DLP в Беларуси, будет неверным. Но при этом стоит отметить значительно меньшую в сравнении, например, с Россией осведомленность компаний в вопросах способов защиты информации от утечек. Удивляться этому особо не приходится, учитывая, что потенциал белорусского рынка в разы, а то и в десятки раз меньше потенциала того же российского рынка. По этой причине многие вендоры не проявляют сильного интереса к данному региону. Также широкому распространению DLP систем мешают своего рода устоявшиеся и устаревшие мифы. Например, некоторые думают, что DLP — это хорошо и такие системы эффективны, но что называется не для всех, так как стоят слишком дорого, сложны в понимании, очень затратны и ресурсоемки при внедрении. Но времена меняются. Благодаря новым подходам к разработке современные системы DLP перестают быть неуклюжим и громоздким инструментом, рассчитанным на эксплуатацию исключительно в крупных сетях. Соответственно, постепенно меняется и отношение рынка к системам для защиты информации от утечек. К собственникам бизнеса и руководителям компаний разного уровня приходит понимание того, что защита данных отнюдь не является прерогативой крупных корпораций.

Если уж мы заговорили о мифах, многие считают, что DLP «из коробки» не работают и де факто не могут быть эффективными. Так все же, коробочное решение DLP — миф или реальность?

Большинство DLP вендоров, говоря о коробочных решениях в инфобезопасности, в сам термин «коробка» вкладывают уничижительный смысл. Укрепляя тем самым мнение о том, что система для защиты информации по определению должна быть громоздкой. Делают они это сознательно, не имея возможности реализовать простой и понятный инструмент для контроля утечек.

Однако если говорить именно об эффективном инструменте, то DLP из коробки — это реальность. Хотя и с некоторыми оговорками. Задумываясь о покупке системы для защиты корпоративной информации, заказчик должен четко понимать задачи, которые он собирается решать, используя такого рода программный продукт. Также заказчик должен осознавать, что грамотное внедрение DLP сопровождается целым комплексом организационных мер, которые, как вы понимаете, в коробку не положишь. Иными словами, заказчику нужен определенный консалтинг.

Если говорить о консалтинге, аудите и анализе, насколько важными оказываются эти услуги при внедрении DLP?

Прежде чем приступать к внедрению, заказчик должен самостоятельно или, что и происходит чаще всего, с помощью поставщика, определить те задачи, которые он будет решать при помощи продукта. В противном случае, велика вероятность того, что после покупки DLP-система будет использоваться как банальный инструмент для просмотра переписок.

А вот для того чтобы продукт работал именно как DLP, чтобы он реально упрощал работу офицера безопасности и помогал ему выжимать из предоставленного инструмента по максимуму — тут без аудита, анализа и консалтинга не обойтись. Но, следует понимать, что все эти процедуры не могут существовать в отрыве от самого DLP решения. Иными словами, если не использовать DLP для

Акимов Александр Игоревич, генеральный директор компании Falcongaze

Справка ТБ

Акимов Александр Иванович, образование высшее, в 1992 году окончил БГУИР. Опыт работы в сфере информационной безопасности и систем защиты от утечки информации с 2007 года.

аудита и анализа, после его покупки может последовать разочарование ввиду несоответствия DLP ожиданиям заказчика. И тут уже никакой консалтинг не поможет. Поэтому покупатель должен понимать всю важность пилотных внедрений и не лениться сравнивать предлагаемые ему DLP решения на практике, а не по описаниям.

Скажите, что происходит после внедрения? Нужно ли какое-то сопровождение уже после того, как система была установлена в компании?

Надо разделять техническое сопровождение и консультативное. Мы уже говорили о консалтинге, и он настоятельно рекомендуется. Какой бы подробной ни была документация по продукту, каким бы простым в использовании ни был сам продукт, человеку, ранее не сталкивавшимся с подобным инструментом, будет сложно в нем быстро разобраться и понять сходу все тонкости, позволяющие использовать DLP-систему по максимуму. Поэтому мы еще на стадии пилотных внедрений проводим обучение заказчика, с удовольствием отвечаем на возникающие вопросы, и если заказчик четко формализуют стоящие перед ними задачи, это позволяет нам оказывать помощь в составлении новых и оптимизации уже созданных политик безопасности.

Говоря о техническом сопровождении, думаю, когда решение реализовано качественно и работает корректно, то, в принципе, после внедрения, о каком-то особенном сопровождении речи идти не должно. Разумеется, возможно возникновение каких-то вопросов, но все решается в обычном рабочем порядке.

Александр, ну и в заключение такой вопрос: как вы оцениваете размер и объем рынка DLP-систем в Беларуси?

В случае, если речь идет об абсолютных цифрах, я не возьмусь отвечать на этот вопрос. Скажу так: мы видим перспективу DLP рынка, как в Беларуси, так и в других странах. Прежде всего, я говорю о нашей компании, поскольку мы одинаково уверенно чувствуем себя как на рынке малого и среднего бизнеса, так и в корпоративном сегменте. Остается добавить, что на размер рынка DLP в Беларуси позитивно могут повлиять законодательные органы и регуляторы. Пока вопросы стандартов защиты информации не отражены в должной мере в белорусском законодательстве, но если такие законы появятся в ближайшее время, то, конечно же, это автоматически подстегнет рынок. ■

Проблематика внедрения DLP систем в Республике Беларусь

Никифоров Сергей Никанорович, главный инженер ООО «Нейрон-М»

Перспективы и особенности развития DLP-систем в Республике Беларусь

DLP-системы в Республике Беларусь появились сравнительно недавно. Широкое распространение этих систем на Западе мало повлияло на белорусский рынок, на наш взгляд, в основном из-за отсутствия русифицированных систем, документации, отсутствия классификации этих систем и, как следствие, непонимание правомерности их использования в системах безопасности предприятия. С появлением на рынке ряда Российских систем мониторинга компьютеров в локальной сети, которые можно было бы классифицировать как системы контроля информации, несколько изменили отношение к DLP системам и их перестали «бояться», так как они не относились к лицензируемой сфере деятельности — они не защищали активно информационные потоки, а просто позволяли их контролировать. С этого момента и началось внедрение систем DLP в службы безопасности банков и других крупных предприятий. В настоящее время на рынке Беларуси находят применение ряд различных систем, в основном Российского производства, отличающихся функциональными возможностями и ценой.

Нормативное регулирование применения DLP- систем в Республике Беларусь отсутствует. Наше, в частности, обращение в лицензирующие органы (ОАЦ при Президенте РБ) вызвало недоумение, зачем нужно сертифицировать подобные программные комплексы, так как они не являются системами активной информационной защиты. В России подобного рода системы также не подлежат сертификации.

Коробочное решение при поставке систем DLP, на наш взгляд, реально и позволило бы шире охватить заинтересованные предприятия, особенно это касается небольших, имеющих в своем арсенале 10-30 компьютеров и не имеющих в штате системного администратора. Наш опыт внедрения DLP-систем подтверждает данное утверждение. Целый ряд систем нами был поставлен с условием простой поставки без установки, инсталляции и технического сопровождения. Опыт превзошел наши ожидания. Системы не только были установлены, запущены в эксплуатацию, но и не потребовали вмешательства наших специалистов в процессе эксплуатации. Это объясняется тем, что для внедрения «коробочного» варианта были выбраны достаточно простые в установке, имеющие подробное техническое описание на русском языке, системы. Это основное требование, необходимое при поставке «коробочных» решений.

Исходя из сказанного выше и используя наш опыт установки DLP-систем, можно сказать, что для небольших предприятий (10-30 компьютеров) вопросы консультаций, сопровождения занимают очень мало времени и ограничиваются редкими консультациями по телефону или другим средствам связи. В случае же внедрения сложных распределенных систем, контролирующих сотни компьютеров, вопросы сопровождения, обучения специалистов служб безопасности становятся более актуальными, так как в процессе эксплуатации возникают вопросы «тонкого» характера, которые сложно описать в руководстве по эксплуатации.

На сегодняшний день рынок DLP-систем нами оценивается как достаточно перспективный. К нему можно отнести службы безопасности банков; предприятия оборонного комплекса; предприятия, имеющих коммерческие секреты. Ну и конечно, развитию этого рынка способствует ценовой фактор. Сегодня известен ряд систем, отличающихся по цене в десятки, а то и сотни раз, при этом функциональные возможности очень мало отличаются. ■

SearchInform

Обзор систем противодействия утечкам информации. DLP системы в Беларуси

Барановский Александр Валерьевич, директор ООО "НПТ"

Справка ТБ

Барановский Александр Валерьевич, окончил БГУИР, ФИТУ в 2000 г. После службы в пограничных войсках РБ занимал руководящие должности в ряде коммерческих организаций. С 2009 г. — директор компании «НПТ», эксперт по информационной безопасности. Автор ряда публикаций и исследований.

За первую половину 2012 года белорусский рынок DLP-систем поменялся не слишком существенно. Как и раньше, доминирующим на нем остается лидирующее по техническим характеристикам решение — «Контур информационной безопасности SearchInform», еще более укрепивший свои позиции благодаря новым функциям, реализованным в нем компанией-производителем.

Белорусский рынок DLP

Текущий год, как и прошлый, сложно назвать благоприятным для белорусского рынка DLP-систем. Из-за экономических трудностей предприятия, несмотря на необходимость качественной защиты от утечек информации, сокращают бюджеты на внедрение DLP-систем, но с удовольствием их тестируют, что позволяет показать существующую проблематику руководству.

Наиболее актуальной проблемой по-прежнему остается использование организациями «заплаточных» решений, т.е. покупка средств защиты от утечек информации, закрывающие только отдельные каналы передачи данных. Подобные «заплаточные» решения показали свою полную несостоятельность и неэффективность, однако предприятия продолжают их приобретать по причине отсутствия средств для покрытия всех каналов возможной утечки информации. В то же время качественные современные DLP-системы, включая флагмана рынка СНГ «Контур информационной безопасности SearchInform», предлагают гораздо более удобное решение благодаря своей модульной архитектуре. То есть организация может приобрести в первую очередь наиболее значимые для неё модули (защиту почты, HTTP и внешних устройств), а остальное уже приобрести позже, когда появятся деньги (Skype, IM, FTP и т.д.).

В то же время риски утечек информации для белорусских предприятий существенно возросли, как из-за миграции персонала в Россию, где более высокие зарплаты, так и из-за поиска персоналом дополнительных источников дохода. Сегодня белорусы как никогда готовы «сливать» конфиденциальную информацию тому, кто готов её купить. Но, к сожалению, белорусские организации по-прежнему недооценивают значимость этой угрозы. Открываются новые компании, которые на старте испытывают «кадровый голод» в профессионалах, поэтому логично предположить переманивание специалистов из других компаний.

DLP в белорусской банковской сфере

Банковская сфера традиционно активно прибегает к услугам поставщиков и интеграторов DLP-систем из-за необходимости обеспечения банковской тайны. На сегодня можно говорить о том, что банки являются наиболее защищенными от утечек информации среди всех белорусских компаний. Тем не менее, и здесь есть к чему стремиться, потому что в подавляющем большинстве банков также работают различные средства защиты, зачастую не интегрированные в единую систему.

Наиболее популярным решением среди белорусских банков по-прежнему остается «Контур информационной безопасности SearchInform», разработанный российской компанией SearchInform и внедряемый ООО «НПТ». Популярность данного продукта обусловлена его возможностями: на сегодня это единственный продукт, который обеспечивает контроль всех возможных каналов утечек информации, поддерживает работу на терминальных серверах, позволяет контролировать корпоративные ноутбуки даже за пределами сети компании. Более подробную информацию о характеристиках различных DLP-продуктов на белорусском рынке можно найти в сопровождающей статью таблице.

Несмотря на негативные тенденции в плане защищенности данных в других отраслях, банки сегодня продолжают обеспечивать защиту данных на должном уровне. Тем не менее, вести речь об усилении этой защиты как о тенденции пока преждевременно, поскольку сегодня банки сконцентрированы в большей степени на защите от других информационных угроз (проникновения в корпоративную сеть, кардинга и т.п.).

Кроме того хочется отметить, что в коммерческих банках, к сожалению, встречаются фиктивные конкурсы, которые проводятся «для галочки» и результаты оказываются иными, нежели должны быть исходя из ценовых и функциональных предложений. Но это отдельная тема, которую возможно мы осветим в одном из номеров журнала, с конкретными примерами.

Кроме того, в DLP решениях есть такая интересная функция, как остановка по срабатыванию, т.е система может остановить документ или сообщение, которое содержит информацию, которой запрещено покидать пределы организации. На самом деле, этот функционал очень мало востребован из-за ложных срабатываний и угрозы остановки работы предприятия в плане отправки писем, записи документов на флэшки и т.д. Многие клиенты

даже просят не ставить им данный функционал, т.к. нужна почти 100% гарантия отсутствия сработки по ложным запросам. Иначе тысячи заблокированных писем и сообщений вам гарантированы. А один из банков делает на этом акцент, не понимая всех последствий, которые может повлечь использования этой функции и я более, чем уверен, что никогда не будет ею пользоваться, разве что при блокировании почтового трафика при контроле цифровыми отпечатками.

Технологии и требования

Применение DLP в Беларуси пока ограничивается, зачастую, контролем внешних USB-носителей (закрытие доступа) и http (контроль посещаемых ресурсов). Только сравнительно немногие организации строят полноценный «защитный контур», перекрывающий все потенциальные каналы утечки конфиденциальной информации. Интеграторы DLP-систем отмечают, что спрос на модули, защищающие от утечек через электронную почту, веб-сервисы, интернет-пейджеры, торренты и другие сетевые каналы утечки пока существенно меньше, хотя он и демонстрирует уверенные тенденции роста. В первую очередь это связано с существенно меньшей стоимостью «контроля устройств» по сравнению с контролем сетевого трафика, причем стоимость здесь складывается не только из лицензионных отчислений за программное обеспечение, но и из цен на перенастройку существующего и покупку нового сетевого оборудования, внедрение, настройку, поддержку технически более сложного ПО.

Среди предъявляемых в последнее время требований стоит выделить возможность применения нескольких технологий обнаружения утечек данных. По-прежнему вне конкуренции здесь такая функция как «поиск похожих», позволяющая обнаруживать в перехваченном трафике конфиденциальные документы, даже специально измененные инсайдерами перед отправкой, на сегодняшний день это самый эффективный поиск, который минимизирует количество ложных срабатываний и в десятки раз превосходит примитивные поиски по словам или словосочетаниям.

Также одним из важных требований белорусских заказчиков является простота внедрения продукта, поскольку зачастую внедрение DLP-систем специалистами вендора оказывается даже дороже, чем стоимость самих лицензий, не говоря уже о том, что некоторые из «представителей» российских вендоров не могут сами произвести установку тестовой версии предлагаемого решения или же оказать техническое сопровождение. Это мы вполне тоже сможем обсудить в одном из номеров с указанием конкретных компаний-интеграторов и с обязательным привлечением специалистов различных предприятий и банков, которые с этим сталкивались. В этом плане «Контур информационной безопасности SearchInform», который можно внедрить за несколько часов, остаётся вне какой-либо конкуренции.

Перспективы и тенденции

Наиболее важной тенденцией на сегодня является усиление угрозы утечек информации для всех организаций. Из-за недостаточной защищенности пострадать могут даже те компании, деятельность которых не связана напрямую с информацией, включая предприятия реального сектора экономики. Но, конечно, под самой большой угрозой остаются банки, страховые компании, ИТ-компании, операторы сотовой связи и другие подобные организации.

Из-за того что утечки информации по причине большого ущерба и негативного влияния на репутацию допустившей их организации зачастую замалчиваются, возникает иллюзия, будто в Беларуси утечек информации нет. Это очень опасная иллюзия, поскольку она лишает компанию защиты, а давно известно, что утечку легче предупредить, чем «расхлебывать» её последствия.

Таким образом, в будущем мы увидим увеличение числа утечек информации и, как следствие, усиление внимания организаций к этой проблеме, что должно, в свою очередь, повлечь за собой рост рынка DLP-систем в Беларуси.

Новые функции «Контура информационной безопасности SearchInform»

В течение года компания SearchInform реализовала ряд существенных улучшений своего продукта, еще более укрепляющие его лидирующие позиции на белорусском рынке:

- Перехват исходящей и входящей HTTP-почты, перехват HTTP_IM и перехват сообщений, передаваемых через протокол IMAP при использовании популярного почтового клиента Thunderbird.
- Возможность автоматического удаления индексов по условиям, позволяющим администраторам перестать беспокоиться о том, что на новые индексы не хватит места на диске.
- Плановый перезапуск серверных служб продуктов в целях профилактики программных сбоев.
- Возможность настраивать исключения для мониторинга трафика по хостам, что полезно, например, в тех случаях, когда Web-приложения, работающие из браузера, не допускают мониторинга HTTPS.
- Фильтрация HTTP-трафика по типу его содержимого. Так, к примеру, можно настроить его таким образом, чтобы исключить перехват мультимедиа-контента и снизить таким образом нагрузку на сервер.
- Поддержка VLAN для компаний, имеющих распределенную корпоративную локальную сеть и множество филиалов.
- Одновременный поиск по нескольким атрибутам, например, можно найти все письма, которые один пользователь отправил другому.
- Функция подсчета количества сообщений при построении графа позволяет визуально идентифицировать самых общительных сотрудников.
- Возможность работы продукта без использования сторонних модулей для перехвата данных, передаваемых на внешние устройства.
- Поддержка полноценного контроля устройств для тех пользователей, которые работают через терминальные серверы.
- Помещение почтовых отправлений, содержащих подозрительный текст или вложения, в «карантин».
- Поддержка перехвата протоколов мгновенного обмена сообщениями (IM) на рабочих станциях пользователей. Это дает возможность осуществлять перехват данных, передаваемых по защищенному с помощью SSL-шифрования каналу.

ООО «НПТ»
г. Минск, ул. К. Чорного, 5А, пом. 5а
Тел./факс: (029) 649-77-79
E-mail: ab@searchinform.ru
Год основания: 2009

УНП: 191117428

Модернизация и новые решения в продукте Falcongaze SecureTower

Для того чтобы соответствовать возрастающим требованиям рынка, разработчики программных решений должны находиться в состоянии постоянной эволюции, не только подстраиваясь под уже существующие потребности, но и предугадывая их заранее. Именно такой подход является своеобразным девизом компании **Falcongaze**, занимающейся разработками программного обеспечения в сфере информационной безопасности.

Флагманский продукт **Falcongaze** — система **SecureTower**, предназначенная для обеспечения информационной и экономической безопасности предприятий, постоянно изменяется и дополняется инструментами, которые делают решение основных задач продукта все более эффективными.

Несмотря на собственное видение того, каким функционалом должна обладать система, разработчики **SecureTower** постоянно прислушиваются к мнению заказчиков уже купивших или использующих пилотную версию продукта, поскольку именно его практическое применение во всей полноте раскрывает те потребности, которые стоят перед заказчиком.

С самого начала **SecureTower** представляла собой решение, коренным образом отличающееся от громоздких, тяжелых во внедрении и эксплуатации DLP-систем. Рынку нужен был высокотехнологичный, но в то же время простой в понимании и использовании универсальный продукт, который способен обеспечить качественную защиту корпоративной информации и повысить эффективность работы предприятия в целом. Именно такой подход к реализации и лег в основу разработки **SecureTower**.

В развитии **SecureTower** определены следующие приоритеты:

- Эффективный контроль преднамеренного хищения или случайной утечки данных по различным каналам
- Развитие функционала для создания гибких и разнообразных политик безопасности
- Формирование неограниченного по времени хранения архива перехваченных данных и удобный инструмент для расследования инцидентов в ретроспективе
- Управление операционными, репутационными и правовыми рисками
- Совершенствование функционала по работе системы в распределенных офисах и контроль мобильных рабочих мест
- Обеспечение простоты внедрения и использования в сочетании с высокой производительностью и отказоустойчивостью

SecureTower обеспечивает контроль максимального количества каналов коммуникации, перехватывая весь трафик, поступающий и передаваемый по электронной почте, через мессенджеры, включая текстовые, sms- и голосовые сообщения Skype. Решение контролирует информацию, публикуемую на форумах, в блогах, чатах или социальных сетях. Под контролем также находятся файлы, передаваемые по протоколам FTP/FTPS, HTTP/HTTPS и др., а также отправляемые на сетевые и локальные принтеры. Количество контролируемых каналов постоянно растет и в настоящий момент завершается реализация функционала, позволяющего контролировать внешние устройства.

Весь перехваченный трафик проходит проверку на соответствие установленным политикам безопасности. В случае обнаружения инцидента сотрудник, ответственный за информационную безопасность в компании, незамедлительно получит об этом уведомление.

Сохраняя весь перехваченный трафик в базу данных, **SecureTower** накапливает своеобразный архив, позволяющий просматривать «историю» внутрикорпоративных бизнес-процессов и событий. Такой архив может храниться сколь угодно долго без ущерба для производительности, что позволяет расследовать любой инцидент в ретроспективе. Возможность создания интерактивных отчетов облегчает работу сотрудников службы безопасности и делает ее более эффективной.

Большое внимание в развитии **SecureTower** уделяется функционалу, обеспечивающему не только информационную, но и экономическую безопасность компаний. Система **SecureTower** позволяет отслеживать все действия персонала за компьютером, выявляя случаи нецелевого использования сотрудниками корпоративных ресурсов и рабочего времени.

SecureTower одинаково успешно функционирует как в обычных локальных, так и в сетях компаний, имеющих территориально распределенную структуру офисов: крупных холдингах или филиальных сетях. **SecureTower** обеспечивает полный контроль мобильных рабочих мест (ноутбуки, нетбуки и т.д.), покидающих пределы компании. Все информационные потоки на таких устройствах будут зафиксированы и в полном объеме переданы службе безопасности при ближайшем подключении к сети компании.

Система **SecureTower** качественно отличается от других DLP-решений удобством внедрения и использования. Установка системы не требует изменения инфраструктуры сети или покупки дорогостоящего оборудования. Для того чтобы развернуть и настроить **SecureTower** даже в сети со сложной структурой, как правило, достаточно нескольких часов. При этом система обладает высокой производительностью и отказоустойчивостью.

Таким образом, благодаря эффективным инструментам для защиты информации и расширенному функционалу по контролю за активностью сотрудников на рабочих местах **SecureTower** можно по праву считать изящным, универсальным и простым для понимания решением, которое не только защищает данные, но и оптимизирует работу всей компании.

ООО «Фалконгейз»
Эксклюзивный дистрибьютор
в Беларуси — компания ДПА Бел
220116, г.Минск,
пр-т Дзержинского, 104, оф.503
Тел.: (017) 277-26-37, (029) 195-11-15
E-mail: info@dpa.by

УНП: 191125825

Новый продукт на белорусском рынке OTP-решений от ЗАО "БЕЛТИМ СБ"

ЗАО "БЕЛТИМ СБ" — официальный представитель и партнёр компании "Датавэй секьюрити", согласно договорам о дистрибьюции и неразглашении конфиденциальной информации представляет решение компании GTB Technologies по защите от утечек конфиденциальной информации и продукт GTB Inspector.

Уникальность данного решения заключается в том, что применяются различные механизмы обработки документов, что, во-первых, позволяет автоматически производить категоризацию и классификацию документов, во-вторых, обеспечивает контроль над перемещением данных. Обнаружение конфиденциальной информации основывается на применении ключевых слов и регулярных выражений цифровых отпечатков словарей. GTB DLP состоит из следующих основных компонентов:

1. GTB Inspector;
2. GTB Endpoint protector;
3. GTB eDiscovery.

Система обладает следующими функциональными возможностями:

- Мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов вычислительных сетей Заказчика конфиденциальной информации по HTTP-HTTPS и SMTP-каналам.

- Сбор и хранение всех POST-запросов, потенциально содержащих защищаемую информацию, передаваемых за пределы сегментов вычислительных сетей Заказчика с использованием HTTP-каналов (внешний сервис электронной почты, форумы и т.п.).

- Автоматический поиск КИ в сегментах сети Заказчика.

- Запись, протоколирование и уведомление ответственных лиц о нарушении политики ИБ (инцидентов ИБ) в части обработки КИ.

GTB Inspector сканирует и анализирует весь исходящий трафик в реальном времени. При прохождении заданного порога чувствительности вся подозрительная активность останавливается, при этом администратор безопасности получает уведомление о происшедшем инциденте.

Результат: Преднамеренная или случайная передача конфиденциальной информации оперативно идентифицируется и блокируется, данные остаются внутри безопасного периметра в полном соответствии с действующей политикой Информационной Безопасности.

Поддержка протоколов: SMTP + TLS, Microsoft Messenger, HTTP, ICQ, HTTPS, AIM, Web Mail, Google Talk, HTTP Server, Jabber, POP3, Peer-to-Peer приложения, FTP, SSL, Instant Messengers.

GTB Endpoint Protector — это программно-аппаратный комплекс, позволяющий решить проблему утечек конфиденциальной информации посредством использования съемных накопителей информации, таких как смартфоны, iPad, USB карты, съемные жесткие диски, CD и DVD записывающие устройства и т.д.

GTB Endpoint Protector контролирует доступ к съемным носителям информации, предоставляет детальные отчеты активности, защищает важные данные посредством их шифрования и может быть прекрасно интегрирован с GTB Inspector для полной защиты информации.

Результат: GTB Endpoint Protector отслеживает любую активность устройств на портах Ввода/Вывода на системном блоке и обеспечивает контроль централизованной политики доступа к конфиденциальной информации.

Действия по обеспечению политики ИБ: блокирует, заносит в лог, проверяет, шифрует по типу устройства, по типу данных.

GTB eDiscovery — это программный продукт для поиска, аудита и классификации хранящейся в корпоративной сети конфиденциальной информации. GTB eDiscovery сканирует корпоративную сеть, включая сервера, рабочие станции и ноутбуки. Поиск конфиденциальной информации проводится с той же тщательностью, что и у комплекса GTB Inspector, с той разницей, что GTB eDiscovery проводит аудит данных в состоянии покоя.

GTB eDiscovery прекрасно интегрируется с GTB Inspector и GTB Endpoint Protector для получения полноценного DLP решения.

Результат: Возможность идентифицировать потенциальные утечки информации до их возникновения. GTB eDiscovery позволяет предусмотреть возможность потери данных, например, в связи с потерей или кражей ноутбука или заражением системы вредоносным ПО.

Преимущества: возможность одновременного сканирования тысяч компьютеров; высокая скорость сканирования; не перегружает сеть; защищает файлы всех форматов, включая исходный код, аудио, видео, текст и т.д., файлы БД, почти полное отсутствие ложных срабатываний, высокая точность работы срабатываний, автоматический или ручной режим, бесперебойная обработка данных поиска, широкий спектр возможных настроек, возможность работы без оператора.

ЗАО «БЕЛТИМ СБ»
220002, РБ, Минск, пр-т Машерова, 25
Тел.: (017) 334-95-12, 334-99-11
E-mail: info@beltim.by
Сайт: www.beltim.by

УНП: 190527159

Средства защиты от утечек информации

Компания поставщик	ЗАО «БЕЛТИМ СБ»	ООО «НПТ»	ООО «Нейрон-М»			
Продукт/разработчик	GTB DLP Suite/GTB Technologies	«Контур информационной безопасности SearchInform»	LanAgent Bel (Нетворк профи РФ-Нейрон-М РБ)	Security CuratorBel (АтомПаркРФ-Нейрон-М РБ)	StaffCopBel АтомПаркРФ-Нейрон-М РБ)	LanMonitor-Bel (название условное) Нейрон-М РБ
Тип решения (аппаратно, программное, программно-аппаратное)	программное, программно-аппаратное	программное	программное	программное	программное	программное
Сертификат	нет данных	идёт процесс получения экспертизы ОАЦ	не требуется	не требуется	не требуется	не требуется
Русификация	будет в 14,8 для основной консоли (Central Console)	+	+	+	+	+
Технологии						
Анализ по словарю и регулярные выражения	+	+	+	+	+	+
Лингвистический анализ	–	+	–	–	–	+
Онтологический анализ	–	+	–	–	–	-
Поддержка анализа транслита	–	+	+	+	+	+
Поддержка замаскированного текста	–	+				+
Поддержка особенностей русского языка при анализе содержимого	–	+	+	+	+	+
Анализ с использованием цифровых отпечатков	+	+	+	–	–	+
Количество поддерживаемых форматов файлов	все в сетевом исполнении и 65 для Endpoint	116	нет данных	нет данных	нет данных	нет данных
Типы каналов связи, мониторинг которых возможен. Почта						
Входящая SMTP	–	+	+	+	+	+
Исходящая SMTP	+	+	+	+	+	+
SMTPS	+	+	–	+	+	+
Внутренняя Microsoft Exchange	только при использовании Mail Transfer Agent предоставленого нами	+	–	–	+	+
Внутренняя IBM Lotus Domino	только при использовании Mail Transfer Agent предоставленого нами	+	–	–	+	+
ESMTP	+	+	–	–	+	+
POP3	+	+	+	+	+	+
POP3S	–	+	–	+	+	–
IMAP4	+	+	+	+	+	+
IMAP4S	–	+	+	+	+	+
Интернет-пейджеры						
ICQ, Miranda (OSCAR)	+	+	+	+		+
Mail.ru Агент	–					
(не работает через прокси)	+	+	+	+	+	
Windows Live Messenger	+	+	+	+	+	+
AOL AIM	+	+	+	+	+	+
Yahoo! Messenger	+		+	+	+	+
Google Talk	только в связке с прокси	+	+	+	+	+
Skype (текст)	–	+	+	+	+	+
Microsoft Office Communicator	+	+	+	+	+	+
Jabber	+	+	+	+	+	+
MySpace IM	только для англ. языка	нет данных	+	+	+	+
Перехват файлов IM	+	+	+	+	+	+
Сетевые принтеры	+	+	+	+	+	+
Контроль внешних устройств						
HDD	+	+	+	+	+	+
USB	+	+	–	+	–	+
COM/LPT	+	+	–	–	–	+
Wi-Fi, Bluetooth и др.	только блокирование	+	+	+	+	+
Локальные принтеры	только блокирование	+	+	+	+	+
Запрет доступа к конфиденциальным файлам на рабочей станции для заданных приложений	–	–	+	+	+	+
Очистка диска рабочей станции от конфиденциальных данных (перемещение в карантин)	только для Win 2008 R2	–	+	+	+	+

Компания поставщик	ЗАО «БЕЛТИМ СБ»	ООО «НПТ»	ООО «Нейрон-М»			
Продукт/разработчик	GTB DLP Suite/GTB Technologies	«Контур информационной безопасности SearchInform»	LanAgent Bel (Нетворк профи РФ-Нейрон-М РБ)	Security CuratorBel (АтомПаркРФ-Нейрон-М РБ)	StaffCopBel АтомПаркРФ-Нейрон-М РБ)	LanMonitor-Bel (название условное) Нейрон-М РБ
Ограничение доступа в зависимости от типа съемного носителя	+	+	+	+	+	+
Возможность разрешать копирование только на доверенные носители	+	+	+	+	+	+
Автоматическое определение реального владельца данных на основе заданных критериев	+	+	+	+	+	+
Контроль буфера обмена	–	+	+	+	+	+
Контроль копирования из общих папок	–	+	+	+	+	+
Контроль копирования в общие папки	+	+	+	+	+	+
Контроль источников хранимых данных	+	+	+	+	+	+
Мониторинг в режиме онлайн	+	+	+	+	+	+
Контентная фильтрация копирования	+	+	+	+	+	+
Контроль использования устройств в зависимости от типа файла	+	+	+	+	+	+
Шифрование данных при копировании на устройства (криптопериметр)	+	–	+	+	+	–
Контроль хранения данных						
Поиск конфиденциальной информации на рабочих станциях	+	+	+	+	+	+
Поиск конфиденциальной информации на серверах и в сетевых хранилищах	+	+	+	+	+	+
Настройка действий: копирование, перемещение, удаление	только навешивание политик с разными правами доступа	+	+	+	+	+
Уведомление администратора о нарушениях политие хранения КИ	+	+	+	+	+	+
Защита хранимых данных с помощью шифрования для защиты от утечек при хищении носителей	+	–	+	+	+	+
Управление системой и обработка инцидентов						
Собственная консоль	+	+	+	+	+	+
MMC-консоль	+	–	+	+	+	+
Web-консоль	+	–	+	+	+	+
Сохранение истории инцидентов для последующего анализа	+	+	+	+	+	+
Отчеты						
Возможность построения отчетов о нарушениях	+	+	+	+	+	+
Экспорт отчетов	+	+	+	+	+	+
Логирование действий администраторов	+	+	+	+	+	+
Мониторинг агентов и их защита						
Возможность в онлайн-режиме контролировать клиентские компьютеры	+	+	+	+	+	+
Контроль работы агента	+	+	+	+	+	+
Контроль политик агента	+	+	+	+	+	+
Возможность настройки реагирования на события	+	+	+	+	+	+
Защита агента от удаления или выключения	только средствами AD	+	+	+	+	+
Контроль целостности	+	+	+	+	+	+
Контроль сетевой активности пользователей						
Фотография рабочего дня пользователя (подробные отчеты)	–	+	+	+	+	+
График сетевой активности пользователя (детализация)	только для нарушений	+	+	+	+	+
Граф взаимосвязей любого пользователя с внутренними и внешними абонентами	только для нарушений с внешними абонентами	+	–	–	–	+
Снимки экрана рабочих столов пользователей	–	+	+	+	+	+
Динамическая система отчетности с возможностью интерактивного изучения данных	+	+	+	+	+	+
Мониторинг активности рабочей станции						
Контроль активности приложений на компьютерах пользователей	– только запрещение запуска приложений со съемных носителей	+	+	+	+	+
Контроль запущенных процессов	–	+	+	+	+	+
Графическая отчетность	+	+	+	+	+	+
Интеграция со стороны ПО						
Интеграция с любыми сторонними утилитами посредством встроенных API	посредством SDK	+	нет данных	нет данных	нет данных	нет данных
Интеграция со сторонними решениями	посредством SDK	+	+	+	+	+
Интеграция с прокси-серверами	всеми, кто поддерживает ICAP, предоставляем так же свой прокси	+	+	+	+	+
Интеграция с почтовыми серверами	+	+	+	+	+	+

Новинки рынка

Видеокамера HD-SDI AMC-B920HD

Производитель: TM Axiom
Поставщик: Группа компаний «Сфера»
Назначение:
Профессиональная цветная корпусная видеокамера разрешения HD и высокой чувствительности благодаря своим техническим характеристикам и удобству в использовании успешно применяется как в простых системах видеонаблюдения, так и в сложных конфигурациях в интегрированных охранных комплексах.
Особенности:
Применение новой 1.3 CMOS матрицы 1.3 Megapixel Sony Progressive формирует сверхвысокое разрешение и наиболее четкое изображение с разрешением 720ТВЛ при минимальной освещенности на объекте 0,06лк.
Благодаря широким возможностям настройки, а также большому количеству режимов автоматической регулировки уровня видеосигнала (выкл./низкий/средний/высокий), баланса белого (авто/отслеживание/пользователь), а также различным эффектам изображения (антиблик, зеркальное отображение, негатив/позитив, "заморозка") камера прекрасно работает в самых сложных условиях. Отображаемые на экране сообщения позволяют оперативно отслеживать состояние камеры.
Видеокамеры предназначены как для внутренней установки, так и для монтажа в термокожухах вне помещений.
Технические характеристики:
Видеокамера HD-SDI корпусная без объектива, 1/3" 1.3 Megapixel Sony Progressive, день/ночь (механический ИК-фильтр), 720твл, 0.1лк/F1.2 (цветной режим), C/CS, DD, S/N>52дБ, HSBLC, 3D-DNR, OSD, 126(Д)x67(Ш)x60(В)мм, 12В/2Вт
Время появления на рынке: 1 квартал 2012 г.

Видеокамера AMC-IRD203VDN-24

Производитель: TM Axiom
Поставщик: Группа компаний «Сфера»
Назначение:
Профессиональная цветная купольная камера день/ночь предназначена для использования в составе охранных систем видеонаблюдения в наиболее сложных световых условиях.
Особенности:
Высокое разрешение 700 ТВЛ. Блок ИК подсветки вынесен за пределы видеомодуля для обеспечения лучшего теплового режима. Имеет форму полусферы, что способствует простому монтажу к потолку и стене в помещениях. Джойстик для настройки экранного меню.
Технические характеристики:
Видеокамера купольная, 1/3" SONY 960H CCD, 700твл, день-ночь (механический ИК фильтр), электронно-оптический затвор: авто, 1/50 ~ 1/120 сек., объектив: 4-9 мм авто Manual zoom lens, 0.1 лк/F2.0, ИК-подсветка 20м (43 диода), 0.1 Lux/F2.0, S/N>50дБ, BNC 1.0Vp-p/75Ом, 12VDC / 24VAC, 106x106 мм, -10°...+50°C
Время появления на рынке: 3 квартал 2012 г.

Видеокамера HD-SDI KPC-HD38M

Производитель: KT&C, Южная Корея
Поставщик: Группа компаний «Сфера»
Назначение:
Профессиональная цветная видеокамера сверхвысокого разрешения благодаря своим техническим характеристикам и удобству в использовании, успешно применяется как в простых системах видеонаблюдения, так и в сложных конфигурациях в интегрированных охранных комплексах.
Особенности:
Миниатюрная квадратная видеокамера без диафрагмы, с объективом с фиксированным фокусом. Применение новой CMOS-матрицы 2.1 Mega Pixel, 1/3" Exmor SONY CMOS формирует сверхвысокое разрешение (1080x1920p) и наиболее четкое изображение. Благодаря широким возможностям настройки, а также большому количеству режимов автоматической регулировки уровня видеосигнала (выкл./низкий/средний/высокий), баланса белого (авто/отслеживание/пользователь), цифровому подавлению шумов (3-DNR), а также различным эффектам изображения (антиблик, зеркальное отображение, негатив/позитив, "заморозка", цифровой «зум») камера прекрасно работает в самых сложных условиях.
Технические характеристики:
Видеокамера HD-SDI в квадратном миникорпусе, 2.1 Mega Pixel, 1/3" Exmor SONY CMOS, разрешение 1080px30fps/720px60fps, электронная функция день-ночь, 0.1 лк/F2.0, f 3.6мм, Board Lens, WDR, 3DNR, AWB, BLC, OSD, 12V DC, 38x38x36мм, -10°...+50°C
Время появления на рынке: 2 квартал 2012 г.

Видеокамера HD-SDI KPC-HDB450

Производитель: KT&C, Южная Корея
Поставщик: Группа компаний «Сфера»
Назначение:
Профессиональная цветная видеокамера сверхвысокого разрешения благодаря своим техническим характеристикам и удобству в использовании, успешно применяется как в простых системах видеонаблюдения, так и в сложных конфигурациях в интегрированных охранных комплексах.
Особенности:
Миниатюрная цилиндрическая видеокамера без диафрагмы, с объективом с фиксированным фокусом. Применение новой CMOS-матрицы 2.1 Mega Pixel, 1/3" PANASONIC CMOS формирует сверхвысокое разрешение (1080x1920p) и наиболее четкое изображение. Благодаря широким возможностям настройки, а также большому количеству режимов автоматической регулировки уровня видеосигнала (выкл./низкий/средний/высокий), баланса белого (авто/отслеживание/пользователь), цифровому подавлению шумов (3-DNR), а также различным эффектам изображения (антиблик, зеркальное отображение, негатив/позитив, "заморозка", цифровой «зум») камера прекрасно работает в самых сложных условиях.
Технические характеристики:
Видеокамера HD-SDI в цилиндрическом корпусе, 2.1 Mega Pixel, 1/3'' PANASONIC CMOS, разрешение 1080px30fps/720px60fps, электронная функция день-ночь, 0.1 лк/F2.0, f 3.6мм, Board Lens, WDR, 3DNR, AWB, BLC, OSD, 12V DC, 45(D)x75(L), -10°...+50°C
Время появления на рынке: 2 квартал 2012 г.

IP видеокамера EDN2210

Производитель: EverFocus Electronics Corp. (Тайвань)
Поставщик: СООО «Сатурн-Инфо»
Сертификат: не подлежит обязательной сертификации
Особенности:
- 1/2.7" Progressive Scan CMOS
- 2 мегапикселя (1080p)
- Чувствительность 0.1 Люкс @ F1.5
- Объектив f=4мм/F=1.5
- Формат сжатия H.264 / M-JPEG
- Поддержка Micro SD карты
- Широкий Динамический Диапазон (WDR)
- Power over Ethernet (PoE)

Характеристики: Питание PoE (IEEE 802.3af), размеры 117 x 50 мм, вес 170г, рабочая температура -10˚C~50˚C.
Время появления на рынке: июнь 2012

IP видеокамера ETN2110

Производитель: EverFocus Electronics Corp. (Тайвань)
Поставщик: СООО «Сатурн-Инфо»
Сертификат: не подлежит обязательной сертификации
Особенности:
- 1/2.5" CMOS
- Чувствительность 0.5 Люкс /0 Люкс (с подсветкой)
- Формат сжатия MPEG-4, M-JPEG и H.264
- ИК подсветка
- Панорамирование: 355°(-177.5°~177.5°), 51°/с макс.
- Наклон: 135°(-45°~90°), 48°/с макс
- Поддержка Micro SD карты
- Power over Ethernet (PoE)

Характеристики: Питание DC12B/PoE, вес 415г, рабочая температура 0˚C~50˚C.
Время появления на рынке: июнь 2012

IP видеокамера EQN2110

Производитель: EverFocus Electronics Corp. (Тайвань)
Поставщик: СООО «Сатурн-Инфо»
Сертификат: не подлежит обязательной сертификации
Особенности:
- 1/4" CMOS
- 1 Мегапиксель (1280x800)
- Чувствительность 0 Люкс (с подсветкой), 1.5 Люкс (без подсветки)
- Объектив f = 3.6 мм, F 2.3

- Формат сжатия H.264 / MPEG4 / M-JPEG
- Встроенный PIR датчик
- Встроенный Динамик/Микрофон
- Поддержка Micro SD карты
- Power over Ethernet (PoE)

Характеристики: Питание DC12B/PoE, размеры 33 x 69 x 103 мм, вес 110 г, рабочая температура 0˚C~50˚C.
Время появления на рынке: июнь 2012

IP видеокамера EQN2171

Производитель: EverFocus Electronics Corp. (Тайвань)
Поставщик: СООО «Сатурн-Инфо»
Сертификат: не подлежит обязательной сертификации
Особенности:

- 1/4" CMOS
- 1 Мегапиксель (1280x800)
- Чувствительность 0 Люкс (с подсветкой), 1 Люкс (без подсветки)
- Объектив f = 3.6 мм, F 2.3
- Формат сжатия H.264 / MPEG4 / M-JPEG
- WiFi 802.11b/g/n
- Встроенный Динамик/Микрофон

Характеристики: Питание DC12B, размеры 33 x 69 x 103 мм, вес 105 г, рабочая температура 0˚C~50˚C.
Время появления на рынке: июнь 2012

SafeNet

Поставщик: ООО «Измет»
Производитель: Германия
Назначение: SafeNet- это электронная система контроля, которая способна повысить уровень сервиса, управлять депозитарием, что в значительной степени расширяет возможности депозитария.

Особенности: SafeNet — это тщательно продуманное решение в программном обеспечении, которое доказало свою эффективность во многих существующих проектах и показало полный контроль и оперативное управление депозитарием.
Возможности: SafeNet предлагает комплексный пакет интересных и рациональных возможностей и решений.
Характеристики:

- сетевая поддержка
- легкое управление
- центральная клиентская база
- общий протокол отчетов
- легкое внедрение в уже существующие процессы
- документация и статистика
- импорт и экспорт данных в существующие базы
- анализ событий
- безлимитное количество пользователей и отделов
- доступность видеосъемки событий
- способность к использованию внешнего хостинга
- не нужно доп.инсталяции программ на ПК
- интегрированная система подключения депозитариев любых производителей
- адаптированные договора аренды и условий

USB-СЕЙФ «Меркурий» СЮИК 466216.001

идеальный носитель для защищенного хранения личного ключа, участвующего в формировании ЭЦП

Персональное устройство для защиты информации при ее обработке и хранении под управлением ОС MS Windows 2000/XP/2003/Vista/7.
Сертификат: ОАЦ при Президенте РБ № BY/112 03.03/ 036 00159
Принцип работы: встроенное программное обеспечение защищает секретность и целостность информации путем шифрования национальными криптографическими методами
по ГОСТ 28147-89
Производитель:
ЗАО НТЦ «КОНТАКТ» — одно из ведущих белорусских предприятий в сфере технических, аппаратно-программных и криптографических средств защиты информации
220007 г. Минск, пер. Студенческий, 7. Тел./факс: 222-73-18

Cisco Systems Holding BV, Представительство в Республике Беларусь

220034, г. Минск, ул. Платонова, 1Б, Бизнес-центр «Виктория Плаза»
E-mail: pburba@cisco.com
Сайт: www.cisco.com
Год основания: 2008
УНП: 102341971
Контактные лица: Глава Представительства Павел Бурба.
Сертификат: ОАО «Гипросвязь».

А

АВАНТ-ТЕХНО, ОДО

220004, г. Минск, ул. Короля , 45- 16в
Тел./факс: (017) 200-01-09, 226-43-52
E-mail: contact@avant.by
Сайт: www.avant.by
Год основания: 2003
УНП: 190423783
Контактные лица:
директор Козодаев Руслан Валерьевич,
начальник отдела продаж Новик Владимир Павлович,
начальник отдела систем видеонаблюдения Красногоров Александр Михайлович.
Лицензии:
№ 02300/0343681 на право осуществления деятельности по обеспечению пожарной безопасности выдана МЧС РБ, действительна до 02.06.2013.
Производство: охранные, пожарные извещатели и оповещатели.
Сертификаты: производство (перечень товаров с номером сертификата и датой выдачи):

Наименование	Дата выдачи	Действителен до:	Сертификат №
Извещатель «АВАНТ-DG55»	07.05 2010	03.05.2015	BY/112 03.03.023 00243
Извещатель «АВАНТ-Glasstrek»	07.05 2010	03.05.2015	BY/112 03.03.023 00244
Извещатель «АВАНТ-Pro»	07.05 2010	03.05.2015	BY/112 03.03.023 00239
Извещатель «АВАНТ-Digigard»	07.05 2010	03.05.2015	BY/112 03.03.023 00242
Извещатель «АВАНТ-211»	07.05 2010	03.05.2015	BY/112 03.03.023 00245
Извещатель «АВАНТ-Pro PET»	07.05 2010	03.05.2015	BY/112 03.03.023 00238
Извещатель «АВАНТ-Pro CU1»	07.05 2010	03.05.2015	BY/112 03.03.023 00241

Услуги:
консультации по подбору и применению охранно-пожарного оборудования и систем видео-наблюдения. Гарантийное и послегарантийное сервисное обслуживание на базе собственного авторизованного сервисного центра.
Поставка:
- технические средства охранно-пожарной сигнализации;
- системы видеонаблюдения и контроля доступа;
- IP видеосистемы;
- сопутствующие материалы для монтажа систем.

Дистрибьютор компаний:
PARADOX (Канада) — ведущий мировой производитель охранной техники, выпускающий обширный спектр охранного оборудования и продающий свою продукцию более чем в 60 стран мира.
HIKVISION — международная компания с производством в Китае, разработка и производство IP видеосистем, видеокамер, видеорегистраторов и плат видеоввода. Первое место в мире по производству видеорегистраторов. Hikvision представляет самые передовые решения со сжатием в формате H.264 для индустрии цифрового видеонаблюдения на основе своих собственных запатентованных алгоритмов. Продукция Hikvision обеспечивает безопасность различных сфер деятельности во всем мире, включая розничную торговлю, аэродромы, железные дороги, банки, промышленные предприятия, стадионы и т.д.
Бастион — широкий ассортимент источников питания.
НВП Болид — производитель интегрированных охранных систем.
Avicam Electronics — видеокамеры, видеорегистраторы, объективы и сопутствующее оборудование.

АкссонСофт, ООО

220100, г. Минск, ул. Куйбышева, 40, офис 3.
Тел.: (017) 292-66-11, 292-66-99
E-mail: minsk@axxonsoft.com
Сайт: www.axxonsoft.by
УНП: 191217449
Контактное лицо: директор Лисовский Дмитрий Васильевич.
Производство: программное обеспечение.
Поставка:
- интегрируемая платформа безопасности с распределенной архитектурой «Интеллект».
- цифровые системы видеонаблюдения:
  - Интеллект Лайт;
  - SmartВидео;
  - Axxon Smart IP.

Дистрибьютор компаний: официальное представительство компании ITV | AxxonSoft.

Б

СП «Бевалекс» ООО

220137, г. Минск, ул. Солтыса, 191
Тел.: (17) 330-16-16
Факс: (17) 330-16-30
E-mail: info@bevalex.by
Сайт: www.bevalex.by
Год основания: 1992
УНП: 100944292
Основной профиль деятельности: создание комплексных автоматизированных систем управления
Продукция:
- компьютер и сервер БЕВАЛЕКС™;
- оборудование терминальное Экспресс -3-Р™;
- система серверов высокой плотности БЕВАЛЕКС™;
- система хранения данных БЕВАЛЕКС™;
- центр обработки данных Поток™;
- комплекс обеспечения сетевой безопасности Цитадель™;
- система электронного документооборота «РЕКОРД»™.

ЗАО «БЕЛТИМ СБ»

220002, РБ, Минск, проспект Машерова, 25
Тел.: (017) 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 досмотровое 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 компаний «Банковский информационный центр»

220123 Минск,ул. В.Хоружей, 29-903
Тел.: (017) 289-50-14, 334-36-38, (44) 777-97-01
E-mail: office@bic.by
Сайт: bic.by
Год основания: 1996
Продукция: банковское оборудование, кассовое оборудование, электронные табло, система контроля мерных слитков, комплексные решения, рециркуляционные темпокассы Roller Cash, оптико-электронные тренажеры, депозитные ячейки, ночные сейфы
Дилеры:
г. Гродно — (филиал ООО «СтатСервис»), тел. 0152-44-25-86,
г. Брест — ЧП Толстопятов А.Н., тел. 0162-43-05-35,
г. Барановичи — РЦ ВТИ, тел. 01634-2-53-96,
г. Гомель — ЧП Рудый Н.М.., НПК «Элмис и К», тел. 0232-50-47-62,
г. Орша, Витебск — предприятие "Дельта-ТВ",
г. Витебск — Предприятие «ТЕЗАН», тел. 0212-36-52-54,
г. Могилев — ОуСиЭсЛайн, тел. 0222-22-94-84
Компания представляет на рынке РБ продукцию известных производителей оборудования для обработки наличности Talaris (De La Rue) (Англия), Laurel (Япония), Magner (США), Multivac (Германия), EBA (Германия), Вилдис (Россия)

В

ВирусБлокАда, ОДО

ВирусБлокАда

220088, г. Минск, ул. Смоленская, 15 — 803б
Тел./факс: (017) 294-84-29
E-mail: info@anti-virus.by
Год основания: 1997
УНП: 101294617
Контактное лицо: коммерческий директор Резников Геннадий Константинович
Лицензии:
№01019/50 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выдана ОАЦ при Президенте РБ, действительна до 14.12.2014.
Сертификаты:
21 декабря 2006 г. компании получила сертификат соответствия системы менеджмента качества проектирования, производства и технической поддержки программного продукта требованиям белорусского стандарта СТБ ИСО 9001-2001 и немецкого DIN EN ISO 9001: 2000 (ежегодно компания проходит подтверждение соответствия).
Услуги:
в Республике Беларусь — разработка, внедрение и эксплуатация программного обеспечения, предназначенного для защиты от воздействия вредоносных программ в промышленных и иных организациях республики для замещения аналогичных импортных продуктов;
в мире — экспорт разработанного ОДО «ВирусБлокАда» национального программного обеспечения, предназначенного для защиты от воздействия вредоносных программ, способного конкурировать с лучшими мировыми аналогами.
Проекты и разработки:
- комплекс антивирусных программ Vba32;
- автоматизированное рабочее место администратора «Комплекса VBA32»;
- система фильтрации нежелательной электронной почтовой корреспонденции в Национальном банке Республики Беларусь, функционирующей совместно с компонентами комплекса Vba32 программных средств защиты от воздействия вредоносных программ и др.

И

ООО «Измет»

220026, РБ, г. Минск, проезд Подшипниковый, 9-21
Тел.: (017) 284-64-00 (многоканальный); (29) 33-33-018; (29) 260-40-60
E-mail: izmet@izmet.by
Сайт: www.izmet.by
Год основания: 2005
УНП: 690325966
Производство: шкафы металлический, сейфы, стеллажи, верстаки, почтовые ящики, ключницы. Медицинская и лабораторная мебель. Банковское оборудование. Оборудование для склада и СТО
Услуги: предлагает комплексное решение задач по оборудованию помещений, осуществляет замер, проектирование, подбор, доставку и монтаж оборудования с наиболее эффективным использованием имеющейся площади, а также оказывает послегарантийное обслуживание

ЗАО НИП «ИНФОРМЗАЩИТА»

Информзащита
Системный интегратор

127018 Москва, ул. Образцова, д. 38
Тел.: +7-495-980-2345 (многоканальный)
E-mail: market@infosec.ru
Сайт: www.infosec.ru
Год основания: 1995
ИНН: 7702148410
Услуги: оценка и обеспечение соответствия требованиям регуляторов и стандартов по инфор-мационной безопасности, системы управления идентификацией и аутентификацией, системы мониторинга событий информационной безопасности, обеспечение сетевой безопасности с применением сертифицированных криптографических средств защиты информации, системы контроля целостности программных сред, системы контроля доступа к периферийным устройствам, внедрение инфраструк-

туры открытых ключей, системы антивирусной защиты и защиты от спама.
Лицензии: МО России № 799, ФСБ России № 431Т, ФСБ России № 8780М, ФСБ России № 8779С, ФСБ России № 12230 К, ФСБ России № 12231 Н, СВР РФ № 514, ФСТЭК Аттестат аккредитации, ФСТЭК № 119, ФСТЭК № 1651, ФСТЭК № 0179, ФСТЭК № 0283, ФСБ России № 12301
Сертификаты: ФСБ России № 124-1473 на АПКШ «Континент», ФСБ России № 525-1463 на СКЗИ «Континент-АП», ФСБ России № 525-1462 на АПКШ «Континент», ФСТЭК № 2659 на Cisco IPS 4260 Sensor, ФСТЭК № 2063 на SAP NetWeaver 7.01 Application Server, ФСТЭК № 1981 на «Спецкомплекс-ФК», ФСТЭК № 1968 на «Континент-АП», ФСТЭК № 1967 на ПАК «Соболь», ФСТЭК № 1900 на систему «КУБ», Газпроектинжиниринг №ГО00.RU.1233.Р000048 на оказание услуг (работ), Независимый центр сертификации «Альянс» № СМК.RU/05.12-0367 на соответствие требованиям ГОСТ Р ИСО 9001-2008, ФСТЭК № 2595 на Cisco FWSM, ФСТЭК № 1617 на Cisco Catalyst 3750, ФСТЭК № 1428 на Proventia Management SiteProtector, ФСТЭК № 1426 на Internet Scanner, ФСТЭК № 1318 на Proventia Desktop Endpoint Security, ФСТЭК № 1317 на Proventia Server Intrusion Prevention System, ФСТЭК № 1316 на Proventia Network Intrusion Prevention System, ФСТЭК № 1238 на Secret Net 5.0 — С (сетевой вариант), ФСТЭК № 1237 на Secret Net 5.0 — С (автономный вариант), ФСТЭК № 1119/1 на Secret Net 5.0 (мобильный вариант), ФСТЭК № 907 на Соболь, ФСТЭК № 860 на RealSecure Server Sensor 7, ФСБ России № СФ/027-1795 на ПАК "Соболь". Версия 2.0, ФСБ России № СФ/027-1450 на ПАК "Соболь". Версия 3.0, ФСБ России № СФ/124-1781 на СКЗИ М-506А-ХР, ФСБ № СФ/027–1449 на СЗИ «Соболь», МО РФ № 1012 на Программно-аппаратный комплекс «Росомаха» (Версия 1.0)

К

КОМТИД, ООО

ООО «КОМТИД»

220141, г.Минск, ул. Купревича 1-3-241
Тел.: (017) 211-83-24
E-mail: comtid@tut.by
Сайт: http://www.comtid.com
Год основания: 1996
УНП: 101166264
Контактные лица:
директор Балахничёв Игорь Николаевич
Сертификаты:
- сертификат соответствия по ТР №С-BY.ПБ16.В.00121 на оповещатели ПКИ Иволга, Колибри, Бекас, Шмель, Цикада, ПКИ-2, ПКИ-3, действителен до 14.06.2015 года;
- сертификат соответствия по ТР №С-BY.ПБ16.В.00122 на оповещатели ПКИ-СП12, СП24 Феникс, Филин до 14.06.2015;
- сертификат соответствия по ТР №С-BY.ПБ16.В.00123 на оповещатели речевые Говорун РС1, РС2, РО до 14.06.2015;
- сертификат соответствия №BY/112 03.03.023 00017, на ПКИ-1, действителен до 17.11.2011;
- сертификат пожарной безопасности №ССПБ.BY.ОП066.В00955 на 212-88М, действителен до 14.01.2012;
- сертификат соответствия на ИП 212-88М, действителен до 14.01.2012;
- сертификат соответствия №BY/112 03.03. 033 01310 на ПКИ-СМ12, действителен до 05.03.2014;
- сертификат соответствия №С-RU.ПБ16.В.00003 на ИП 212-88А-р, действителен до 10.08.2014.

Производство:
оборудование для охранной и пожарной сигнализации:
- оповещатели звуковые;
- оповещатели звукоречевые;
- оповещатели светозвуковые;
- оповещатели световые;
- устройства подсветки светодиодные (стробоскопические);
- извещатели пожарные дымовые;
- извещатели дымовые автономные;
- разные аксессуары.

НТЦ КОНТАКТ, ЗАО

220034, г.Минск,
ул. Первомайская, 17, оф.1к
Тел./факс: (017) 294-76-76
E-mail: atep52@mail.ru
Год основания: 1990
УНП: 100037461
Контактное лицо: Тепляков Анатолий Адамович
Лицензии:
№ 01019/52 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выдана 29.04.2004 ОАЦ при Президенте РБ, действительна до 29.04.2014.
Сертификаты:
на средства ЭЦП и шифрования, на комплекс защиты от НСД «Барьер», на средство защищенного хранения информации «Меркурий», на генератор линейного зашумления.
Услуги: разработка, сопровождение устройств и систем безопасности, аттестация систем безопасности
Поставка:
систем криптографической защиты и шифрования, средств защищенной обработки и хранения информации, средств защиты от утечки по техническим каналам.
Проекты и разработки:
подсистема криптографической защиты АСБ «Беларусбанк», подсистема криптографической защиты Национального кадастрового агентства Республики Беларусь, подсистема криптографической защиты Министерства финансов Республики Беларусь, комплекс защиты от НСД «Барьер», средство защищенного хранения информации «Меркурий», генератор линейного зашумления.

Н

Нейрон-М, ООО

220119, г. Минск, ул. Тикоцкого, 16, оф 75в
Тел./факс: (017) 261-49-63, (029) 661-49-63, (029) 142-45-18
E-mail: info@neuron-m.by, kv_home@mail.ru
Год основания: 2010
УНП: 191338429
Поставка:
DLP-системы, системы записи телефонных переговоров, системы оповещения по каналам связи, система идентификации по голосу
Проекты и разработки:
системы идентификации по голосу, системы поиска по ключевым словам, распознавание речи, многоканальная запись аудиоинформации
Дистрибьютор компаний: Атом Парк (РФ), Нетворк Профи (РФ), Вентор (РФ)

ООО «Нордман»

220112, г.Минск, ул. Сырокомли-38, пом. 10Н, офис 1
Тел.: (29) 559 62 10
E-mail: info@nordman.by
Сайт: nordman.by
Год основания: 2011
УНП: 191440943
Основная специализация: проектирование, разработка дизайна, строительство банковских помещений и операционно-кассовых залов «под ключ», оснащение помещений широким спектром самого современно-

го банковского оборудования и техники, а также специализированной мебелью
Партнер и эксклюзивный представитель в Республике Беларусь Группы компаний «Europeum»

НПТ, ООО

г. Минск, ул. К.Чорного, 5А, пом.5а
Тел./факс: (029) 649-77-79
E-mail: ab@searchinform.ru
Год основания: 2009
УНП: 191117428
Контактное лицо: директор Барановский Александр Валерьевич
Поставка: КИБ SearchInform (DLP решение, позволяющее контролировать Skype, почту, внешние устройства, интренет-мессенжеры, устройства печати, HTTP трафик, шифрованные каналы, учет рабочего времени)

О

ОРИОНПРОЕКТ, ЧСУП

220131, г. Минск, 1-й Измайловский пер., д. 51, оф. 4
Тел.: (017) 290-04-58, 290-04-59
Сайт: www.orionproject.by
E-mail: info@orionproject.by
Skype: orionproject_support
Год основания: 2009
УНП: 191107028
Контактные лица:
заместитель директора ЧернякЕвгений Евгеньевич,
заместитель директора по техническим вопросам Лубневский Евгений Георгиевич
Услуги:
• продвижение, разработка, техническое сопровождение, обучение, реализация, гарантийное, послегарантийное обслуживание и ремонт продукции «НВП Болид» (РФ) на рынке РБ.
• проведение сертификационных и плановых испытаний оборудования на соответствие существующим нормам безопасности.
• проведение конференций, семинаров и обзорных лекций с проектно-монтажными и другими заинтересованными организациями на предмет популяризации применения оборудования «НВП Болид», ознакомление с новыми технологиями и тенденциями развития в области систем обеспечения безопасности, автоматизации и диспетчеризации объектов.
• оказание содействия, консультаций и помощи в решении организационных и технических вопросов поставки, применения и наладки оборудования.
Поставка: весь спектр оборудования ЗАО НВП «Болид».
Дополнительная информация: авторизованный представитель компании ЗАО НВП «Болид» на территории РБ.

П

ООО «ПРАКТИКСЕРВИС»

231000, г.Сморгонь,
ул.Железнодорожная, д.36, ком.1
Тел.: (01592) 2-10-72
E-mail: PRAKTIK-SERVICE@mail.ru
Год основания: 2005
УНП: 590339502
Производство: спец.бронеавтомобили для инкассации
Услуги: обслуживание бронезащиты спец.бронеавтомобилей, установка пулестойких стекол до 5 кл.стойкости к воздействию стрелкового оружия включительно
Проекты и разработки: освоение новых моделей на базе а/м Peugeot

Р

ЗАО «РИЭЛТА»

197101, Санкт-Петербург, ул. Чапаева, д.17
Тел.: (812) 498-19-71, 603-28-91
Сайт: www.npf.rielta.ru
E-mail: npf@rielta.ru
Год основания: 1993
Продукция: широкий спектр охранных извещателей, приемно-контрольных приборов, устройств для видеонаблюдения, источников питания, автоматических выключателей освещения, приемников ИК-излучения
Услуги: сборка печатных плат, инструментальное производство, литьевое производство, оптические покрытия
Сертификаты: Сертификат соответствия ИСО 9001-2008
Certificate ISO 9001-2008
Сертификат IQNet
Сертификат Sincert

РОВАЛЭНТСПЕЦСЕРВИС, ООО

Адрес: 220007, г. Минск, ул. Вододько, 22
Тел.: (017) 228-17-73, (017) 228-16-80
Отдел продаж: (017) 228-17-75, (017) 228-17-72, (017) 228-16-95
Факс: (017) 228-16-96
E-mail: Sales@rovalant.com
Сайт: www.rovalant.com
Год основания: 1994
УНП: 190285495
Контактные лица:
директор Карпович Владимир Викторович,
заместитель директора Куприянов Александр Семенович.
Лицензия:
№ 02300 /0344206 (на право осуществления деятельности по обеспечению пожарной безопасности), выдана МЧС РБ, действительна до 21 февраля 2012 г.
Производство:
- адресно-аналоговая система пожарной сигнализации АСПС БИРЮЗА;
- пожарный прибор управления ОБЕРЕГ;
- импульсные источники бесперебойного питания ББП;
- система мониторинга НЕМАН;
- интегрированная система безопасности ИСБ 777;
- извещатели пожарные дымовые оптико-электронные: ИПДО-212-1, ИПДО-212-С, ИПДО-212-А;
- приемно-контрольные охранно-пожарные приборы серии «А»;
- автоматизированные системы контроля и учета энергоресурсов (АСКУЭ).
Продажа: системы видеонаблюдения компании Samsung Techwin.
Услуги:
- разработка, производство и торговля оборудованием систем

безопасности и мониторинга; системы контроля доступа; аксессуары;
- проектирование, монтаж и техническая поддержка;
- весь спектр продукции для организации технического противодействия угрозам — от систем объектовой защиты и каналов передачи информации до систем мониторинга.

С

САТУРН-ИНФО, СООО

Республика Беларусь, 220015, г. Минск,
ул. Пономаренко, 35а, офис 616
Тел./факс: (017) 251-62-06; 256-25-23
(029) 656-17-50, (029) 756-17-18
E-mail: saturn@saturn-info.com, www.saturn-info.com
Год основания: 1993
УНП: 100063951
Контактные лица:
директор Сергей Романович Худалеев, зам. директора Михаил Ярославович Гилеп
Лицензии:
№ 02300/728 (на право осуществления деятельности по обеспечению пожарной безопасности) — действительна по 21 апреля 2016 г.;
№ 02010/848 (на право осуществления охранной деятельности) — действительна по 20 мая 2014 г.
Производство: аналоговый акустический извещатель «ШКЛО-730»; цифровой акустический извещатель «ШКЛО-У»; источник бесперебойного питания «ИБП Сатурн».
Услуги: проектирование, монтаж, наладка и сервисное обслуживание систем безопасности.
Дистрибьютор компаний:
Bosch Security Systems (Нидерланды), Honeywell Security (Нидерланды), Everfocus Electronics (Тайвань), SC&T (Тайвань), Anvox (Китай), Tokina (Япония).
Выполненные проекты:
Белорусская железная дорога (станция «Минск-Пассажирский»); бизнес-центр «Инфо»; ОАО «Беларуськалий»; сеть магазинов «Соседи»; сеть магазинов «Связной»; фабрика «Ареола»; ОАО «Белгазпромбанк»; ЗАО «Трастбанк»; ЗАО «Минский транзитный банк»; ОАО «Технобанк»; ЗАО «РРБ-Банк»; ОАО «Банковский Процессинговый Центр»; ОАО «Белтрансгаз»; РУП «Белавиа»; сеть АЗС «Юнайтед Компани»; ООО «Софтклуб», ОАО «Горизонт»; Минский электромеханический завод имени Козлова; ООО «Франдеса»; Минское областное управление Департамента охраны МВД РБ.

ООО "Сименс" представительство в Республике Беларусь

220004, Беларусь, Минск, ул. Немига, 40, офис 604
Тел.: (17) 217-34-84
Факс: (17) 210-03-95
E-mail: minsk-office.cd@siemens.com
Сайт: www.siemens.by
УНП: 102295743
Оборудование для автоматизации процессов, контрольно-измерительное оборудование.
Проекты по модернизации производства (совместно с партнерскими компаниями).

СТАЛВИСКОМ, ООО

220007, г .Минск, ул.Володько, 12-102
Тел./факс: (017) 205-48-24
E-mail: sale@stalviscom.by
Сайт: www.stalviscom.by
УНП: 191194104
Контактное лицо: специалист по продажам Стабровский Александр Леонидович
Поставка:
- цифровые системы безопасности;
- системы видеонаблюдения;
- системы контроля и управления доступом;
- домофоны;
- переговорные устройства;
- замки, доводчики;
- шлагбаумы, приводы для ворот;
- турникеты, ограждения, металлодетекторы;
- системы оповещения.

Дистрибьютор компаний: официальный представитель «Skyros», VideoNet.

Группа компаний «Сфера»

220118 г. Минск ул. Машиностроителей 29-117 (5этаж)
Тел/факс: (17) 341 50 50
Velcom: (29) 641 50 50
МТС: (29) 541 50 50
E-mail: info@secur.by
Сайт: www.secur.by
Год основания: 1995
УНП: 100972915
Контактное лицо: директор Малаховский Денис Святославович
История группы компаний «Сфера» началась в 1995 году. Это, без преувеличений, было время становления современного рынка систем безопасности в Беларуси. Начав с дистрибуции систем охранно-пожарной безопасности, ГК «Сфера» в последующие годы значительно расширила спектр предложений, накопив внушительный опыт, наладив долговременные партнерские связи с производителями оборудования и клиентами. Не стремясь быть первыми, мы по-прежнему стремимся быть лучшими — предоставляя нашим заказчикам наиболее полный комплекс решений, соответствующих динамике времени.
Следуя этому принципу, который является базовым для компании, мы пошли по пути узкой специализации. На сегодняшний день «Сфера» — это группа компаний, каждая из которых занимается решением определенного круга задач. Такой подход позволяет нашим клиентам получать оптимальный, полностью завершенный результат с максимальной степенью проработки индивидуального проекта.
Группа компаний «Сфера» включает:
• управляющую компанию ОДО «Сфератрэйд», представляющую широкую линейку наиболее востребованных рынком решений безопасности;
• компанию ООО «Легион безопасности», специализацией которой является дистрибуция высокотехнологичных, инновационных систем класса hi-end;
• производственную компанию ООО «Инженеркомплекс», обеспечивающую профессиональное инженерное сопровождение на каждом этапе разработки и внедрения охранной системы: проектирование, монтаж, пуско-наладочные работы и обслуживание систем безопасности.
В своей деятельности мы руководствуемся прежде всего ожиданиями клиента, который заинтересован в надежном положительном результате. А полный цикл процессов, которые необходимо реализовать для достижения заданных целей, становится задачей специалистов ГК «Сфера».
ОТВЕЧАЯ ОЖИДАНИЯМ РЫНКА
Под эгидой группы компаний «Сфера» разработана собственная марка охранного оборудования AXIOM™. Главной целью ее создания было предоставить рынку возможность выбора из линейки изначально сба-

лансированных, экономичных и обладающих адекватным качеством моделей. Благодаря этому решения AXIOM™ подходят к любому профилю проекта и компании-заказчика — от учреждений здравоохранения, образования и производственных комплексов до банковских и финансовых организаций, объектов розничной торговли и частной собственности.

При этом каждый проект ГК «Сфера» остается уникальным. В мире интеллектуальных решений невозможно с точностью до последней запятой скопировать однажды созданные проекты — ведь каждый объект, требующий внедрения системы безопасности, обладает индивидуальными характеристиками, даже если дизайн проекта следует некоторым стандартам.

СОВРЕМЕННЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ

Успешное развитие невозможно без постоянного отслеживания последних тенденций и стремления максимально им соответствовать. Будучи более 15 лет на рынке, группа компаний «Сфера» большое внимание уделяет регулярному поиску и анализу наиболее перспективных новинок, налаживанию эффективных партнерских взаимоотношений с лучшими производителями Европы и мира, обновлению спектра своих предложений и своевременному включению в него решений последнего поколения. Каждый год мы включаем в свой каталог 2-3 новых бренда, делая современные разработки доступными, а Ваш выбор — разнообразным.

Группа компаний «Сфера» является постоянным участником профильных мероприятий — выставок, семинаров и конференций, в т.ч. международного уровня, где решения от ГК «Сфера» неоднократно удостаивались наград и дипломов различных степеней.

Система менеджмента качества в ГК «Сфера» сертифицирована по стандарту ISO 9001, что гарантирует соответствие внутренних процессов в компании современным представлениям о надежности, гибкости и эффективному взаимодействию.

Сегодня в группе компаний «Сфера» занято более 50 высококвалифицированных штатных специалистов, чья компетентность регулярно подтверждается сертификацией непосредственно компаний-производителей. На базе ГК «Сфера» создан сервисный центр по гарантийному и послегарантийному обслуживанию оборудования и организован собственный учебный центр, где проводится обучение и практические семинары для специалистов различного уровня, а также организуются встречи с клиентами, круглые столы и обсуждения современных тенденций в области безопасности.

МИССИЯ: БЕЗОПАСНОСТЬ

Наша миссия — быть проводниками инновационных решений на рынке систем безопасности Беларуси, делая их массово доступными для организаций любого уровня и профиля. И мы реализуем ее путем достижения конкретных целевых ориентиров:

- Поставка надежного оборудования, независимо от ценовых сегментов;
- Выполнение полного цикла работ по проектированию, монтажу, наладке и системной интеграции;
- Всесторонняя сервисная поддержка и сопровождение выполненных проектов силами собственного сервисного центра.

Дистрибутор производителей и торговых марок

AXIOM, 3S (Тайвань), KT&C (Южная Корея), MOBOTIX AG (Германия), ZAVIO (Тайвань), NUUO (Тайвань), Fujinon (Япония), Pinetron (Южная Корея), LG Security Electronics (Корея), Truen (Корея), SALTO (Испания), GSN Electronic (Израиль), Rielta (Россия), LOB (Польша), Elmes (Польша), Roger (Польша), QUIKO (Италия), JIS (Испания), Kenwei (Китай), Seoul Commtech Co. (Южная Корея), PERCo (Россия), ITV (Россия), JSB Systems (Россия), AccordTec (Россия), Elesta (Россия), Bolid (Россия) и др.

Проекты

Хозяйственный суд (г. Минск), Представительство ООН в РБ, КГБ РБ, «Тойота-Центр» (г. Минск), автоцентр «Пежо», летний амфитеатр (г. Витебск), РУП "БМЗ», СП «Санта Бремор», РУП «Белтелеком», ИООО «БелЕвросеть», Минский метрополитен, сеть АЗС ОАО «Беларуснефть», РУП «Белпочта», ГП «Белаэронавигация», аэропорт «Минск-1», ЗСАО «Бролли», ВЦ ЗАО «Аквабел», ИООО «Атлант-М Холпи», ТС «Квартал Зеленый бор», ОАО «БПЦ», Казино ZEUS, паркинг бизнес-центра «ТИТАН», ЗАО «ВТБ-банк», ЗАО «БТА-банк», РУП «Могилевлифтмаш», ОАО «Банковский процессинговый центр», сеть универсамов «Рублевский», ОАО «Минский часовой завод», ООО «Олиси», ЗАО «Оксна», РУП «Минскэнерго» филиал «Энергонадзор», ИООО «ТНК БиПи-Запад», РУП «Белсоюзпечать», РУП «Белреставрация», ООО «Хенкель Баутехник», ЗАО "ТК Банк", ЗАО «БелСвиссБанк», СЗАО «Асбис», ЗСАО «Белингосстрах» и др.

Лицензии

- N 02010/209 на право осуществления охранной деятельности, в том числе проектирование, монтаж, наладка и техническое обслуживание средств и систем охраны. Выдана Министерством внутренних дел Республики Беларусь, действительна до 15.08.2021 г.
- N 02300/50 на право осуществления деятельности по обеспечению пожарной безопасности. Выдана Министерством по чрезвычайным ситуациям Республики Беларусь, действительна до 10.02.2016 г.

У

УНИБЕЛУС, СП ООО

UNIBELUS

220033, г. Минск, ул. Нахимова, 10
Тел./факс: (017) 291-15-05, 230-72-40
E-mail: info@unibelus.com
Сайт: www.unibelus.by
Год основания: 1994
УНП: 100834637
Контактное лицо: генеральный директор Забабуха Юлия Аркадьевна
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, мультимедийной, локально-вычислительные сети, охранной сигнализации, периметральной системы охраны, противокражной диспетчеризации; телефония; часофикация; радиофикация; система автоматизации.
Дистрибьютор:
Aiphone (Япония), OPTEX (Япония), «Риэлта» (Россия), «Артон» (Украина), «Технос-М» (Россия), «ТПД Паритет» (Россия), CEM Systems (Великобритания), LG Iris (США), Openers&Closers (Испания), Amtel Security (США), Green (Чехия), FEIG Electronic (Германия), Kocom (Корея), Samsung Techwin (Корея), JVC Professional Europe (Германия), CBC (Ganz, Computar), AVerMedia Information (Тайвань), Win4net (Корея), Daiwon optical (Корея), «Тахион» (Россия), Panasonic (Япония), TOA (Япония), Tasker (Италия), JTS (Тайвань), DNH (Норвегия).

Ф

ООО «Фалконгейз»

Системы информационной безопасности falcongaze™

119991, г. Москва, ул. Большая Полянка, 44/2, офис 525
Сайт: www.falcongaze.ru
Год основания: 2007
Услуги: внедрение системы комплексной защиты конфиденциальной информации на предприятии
Разработки: системы информационной безопасности — программные средства для защиты корпоративных сетей от утечки информации для мониторинга активности персонала
Программный продукт: система SecureTower
Лицензии и сертификаты:
Лицензия ФСТЭК КИ 0072 № 003596 от 16.03.2011
Сертификат ФСТЭК № 2556 от 03.02.2012
Эксклюзивный дистрибьютор продукции Фалконгейз на территории Республики Беларусь: компания ДПА Бел
Адрес: 220116, г.Минск, пр-т Дзержинского, 104,оф.503
Тел.: (017) 277-26-37, (029) 195-11-15
E-mail: info@dpa.by
УНП: 191125825