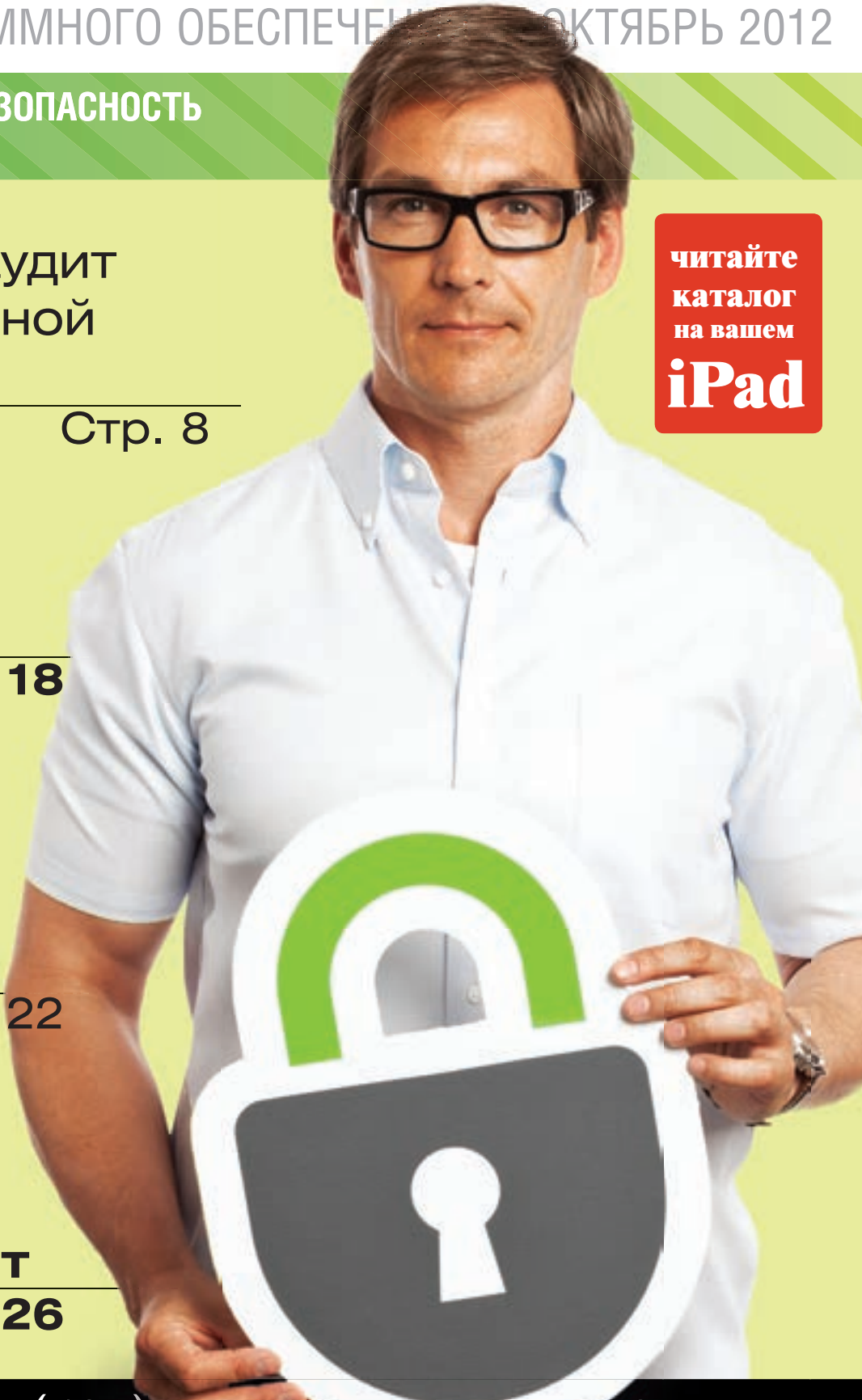
softline direct

КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОКТЯБРЬ 2012

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
спецвыпуск



Экспертный аудит информационной безопасности
Стр. 8

DLP спешит на помощь!
Стр. 18

Compliance management
Стр. 22

BYOD значит любит
Стр. 26

читайте каталог на вашем iPad

САПРяжение / 2012

Встречи с Сообществом пользователей Autodesk

Приглашаем вас присоединиться, встретиться в неофициальной обстановке и поделиться опытом внедрения и использования САПР.

Что такое САПРяжение?

САПРяжение — это встречи Сообщества Пользователей Autodesk, это возможность послушать выступления экспертов, познакомиться, обменяться опытом использования отраслевых САПР, обсудить возможности и особенности решений Autodesk. На САПРяжении можно найти новых друзей, подрядчиков или заказчиков и, конечно, увидеть в лицо активистов и модераторов популярных форумов и САПР блогеров. В качестве гостей на мероприятиях присутствуют и представители Autodesk, которым вы можете задать самые сложные вопросы.

Екатеринбург 30.10.2012
Омск 01.11.2012
Уфа 20.11.2012
Челябинск 22.11.2012

Самара 27.03.2012
Казань 29.03.2012
Волгоград 17.04.2012
Ростов-на-Дону 19.04.2012
Новосибирск 22.05.2012
Хабаровск 25.05.2012

Предварительная регистрация на САПРяжения обязательна!
http://community.autodesk.ru

Зарегистрироваться вы можете уже сейчас на сайте Сообщества Пользователей Autodesk:
http://community.autodesk.ru

Обращаем ваше внимание на то, что формат мероприятий не предполагает большого количества участников, поэтому регистрация может быть закрыта досрочно.

ВНИМАНИЕ! Даты мероприятий могут немного меняться. Актуальную информацию вы всегда сможете найти на сайте Сообщества Пользователей Autodesk.

Каталог Softline-direct – на вашем iPad

Хотите получить каталог по почте?

Заполните анкету на сайте http://subscribe.softline.ru

Если вы руководитель организации или IT-специалист

Если вас интересует эффективность применения информационных технологий

Если вам предстоит выбирать решение ваших бизнес-задач

Мы предлагаем вам бесплатную подписку на каталог программного обеспечения Softline-direct. Право на получение каталога дает только полностью заполненная анкета, оформленная на адрес организации.

softlinecompany

softlinegroup

SOFTLINE

softline

DIRECT ОКТЯБРЬ 2012

КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Специальный выпуск

Информационная безопасность

Безопасность

КАК ЗАКАЗАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

По телефону
С 9:00 до 18:00
в будние дни

По e-mail
info@softline.ru

В интернет-магазине
store.softline.ru

КАК ПОЛУЧИТЬ ЗАКАЗ

Воспользоваться нашей курьерской доставкой (в пределах Москвы бесплатно)

В нашем офисе
с 9:00 до 18:00 в будние дни

Скачать продукт самостоятельно, оплатить лицензию и получить по электронной почте код активации

Приведенные в каталоге цены действительны на дату сдачи каталога в печать.
Актуальные цены вы можете узнать у наших менеджеров по телефону или по электронной почте.

Каталог программного обеспечения Softline direct

Октябрь 201210. (129)**RU.**
Учредитель: ЗАО «СофтЛайн Трейд»
Издатель: **Игорь Боровиков**
Главный редактор: **Максим Туйкин**
Выпускающий редактор: **Лидия Добрачева**
Редакторы: **Александра Почечун, Владимир Цветков, Яна Ламзина**
Дизайнеры: **Константин Косачев, Юрий Гуляк**
Верстка: **Юлия Константинова**
Тираж: 60 000 экз.
Зарегистрировано в Государственном комитете РФ по печати, рег. № ПИ ФС7723773.
Отпечатано в типографии «ScanWeb», Финляндия

SoftlineCompany Softlinegroup

Россия 8 800 100-00-23
Москва 8 495 232-00-23

softline®

Services Software Cloud

ОПОРА РОССИИ

ОБЩЕРОССИЙСКАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА

Присоединяйтесь – это в ваших интересах!

www.opora.ru

Общероссийская общественная организация малого и среднего предпринимательства «ОПОРА РОССИИ» создана предпринимателями 18 сентября 2002 года.

(Свидетельство о регистрации общественного объединения Министерством юстиции РФ № 1027746001909 от 10 ноября 2002 года).

Основная цель деятельности ОПОРЫ РОССИИ – содействие консолидации предпринимателей и иных граждан для участия в формировании благоприятных политических, экономических, правовых и иных условий развития предпринимательской деятельности в Российской Федерации, обеспечивающих эффективное развитие экономики.

Сегодня отделения ОПОРЫ РОССИИ действуют в 81 регионе РФ – от Калининграда до Чукотки.

125 отраслевых союзов, ассоциаций и гильдий формируют Некоммерческое партнерство «ОПОРА».

Вместе ОПОРА РОССИИ и НП «ОПОРА» объединяют около 370 тысяч человек, которые создают более 5 млн. рабочих мест.

Административная реформа антимонопольная деятельность аренда барьеры Борисов Боровиков ВАС вузы ГОСЗАКАЗ ЕСН Жуков земля инновационная сфера исследование кадастр конкуренция контроль Корочкин кредитование кризис критерии крупный бизнес малая приватизация МВД Медведев международная деятельность местное самоуправление методичка Минпромторг Минфин Минэкономразвития муниципалитеты налоги наука НДС недвижимость образование ОРВ оценка персональные данные поддержка МСП правительственная комиссия МСП Правление Президиум приватизация проверки Программа действий ОПОРЫ РОССИИ прокуратура Путин пятилетие работодатели РЖД сертификация соглашение старт-ап техприсоединение техрегулирование торговля ФАС ФНС форум церковь Шаров Шувалов энергетика этика

Членом организации может стать любой гражданин, достигший 18 лет, а также юридические лица – общественные объединения.

Отстаивая свои права, предприниматели России демонстрируют государственный подход к решению стоящих перед бизнесом проблем. В настоящей рыночной экономике «все то, что хорошо для предпринимателя, – хорошо и для общества». Вот почему ОПОРА РОССИИ активно выступает за сокращение избыточных административных барьеров, упорядочение проверок государственными контролирующими органами, выход предпринимательского сообщества и представителей органов власти всех уровней и ветвей «из тени», снижение налогового бремени, упрощение процедур отчетности.

Для решения этих задач в ОПОРЕ РОССИИ сформированы комитеты – по профильным для малого и среднего предпринимательства темам, а также комиссии, отражающие «отраслевой» разрез деятельности бизнеса. Они призваны согласовать интересы бизнеса и власти в реализации ключевых направлений современной экономической политики и предложить конкретные рекомендации по решению проблем предпринимателей.

Присоединяйтесь – это в ваших интересах!

МАЛЫЙ БИЗНЕС – ОПОРА РОССИИ!

Безопасной дороги вашему бизнесу

Вячеслав Железняков,
руководитель Департамента
информационной безопасности
компании Softline

Предположим, некто (пусть этого человека зовут, к примеру, Николай) решил приобрести автомобиль. И естественно, кроме мощности двигателя, расхода топлива и количества ящиков с рассадой, которые можно увезти в багажнике на дачу, его беспокоит также и проблема безопасности: модель автомобиля, которую планируется купить, находится на верхних строчках в рейтинге угонов.

В автосалоне менеджер посоветовал Николаю приобрести хорошую сигнализацию с автономной сиреной, двусторонней связью с системой спутникового слежения. Специалист сервисного отдела рассказал, что у них большой опыт по установке дополнительного оборудования, и имеется соответствующая авторизация от производителя, а представитель страховой компании предложил дополнительную скидку на страховку КАСКО... После этого новоиспеченный владелец машины спокойно подписал заказ-наряд на установку дорогой системы защиты в полной уверенности, что ничто теперь не омрачит «медовый месяц» с его «ласточкой».

Но проходит совсем немного времени, и однажды вечером Николай не находит своего автомобиля на стоянке — он исчез навсегда. Попробуем разобраться подробнее, как же все это могло случиться? Итак, эта машина — достаточно распространенной на рынке модели; автосалон продает их десятками, а то и сотнями в месяц, непрерывно осуществляет одинаковые «внедрения» одних и тех же охранных систем и может с полным правом утверждать, что в этом у него БОГАТЫЙ ОПЫТ.

Однако здесь мы и замечаем небольшое лукавство: в случае выполнения большого количества однотипных заказов руководство автосалона стремится максимально сократить время ожидания клиента и сэкономить свои ресурсы. Поэтому сигнализации, как правило, устанавливаются в некоей простой типовой конфигурации. Вот и на машине Николая сирена, блок управления, модуль спутникового наблюдения — одним словом, все средства защиты были установлены «как всегда». Неудивительно, что, пользуясь типовой схемой установки, угонщики легко обнаружили и вывели из строя блок управления сигнализацией. Возможно, наша история была бы совсем другой, если бы установщики сигнализации разбирались в методах работы преступников и проявили немного фантазии.

Вы спросите меня, причем тут информационная безопасность? Здесь есть прямая аналогия с нашей с вами областью знаний.

Если система информационной безопасности дорогая, суперфункциональная и внедряется сертифицированными инженерами в соответствии с рекомендациями вендора — это еще не дает никаких гарантий. Важно, кто и как именно внедряет и настраивает систему в конкретном случае. Конфигурация не должна быть типовой и упрощенной — необходимо делать индивидуальную настройку системы, выполнять которую должны не инженеры общего профиля, а эксперты-аналитики, которые разбираются в угрозах и знают, как действуют злоумышленники.

Нестандартная «тонкая» настройка системы защиты может серьезно усложнить задачу киберпреступнику, повысив для него риски быть обнаруженным. А в случае ненаправленной атаки или невысокой квалификации нарушителя это может заставить его отказаться от попыток проникновения на ваш ресурс и выбрать более доступную жертву.

Департамент информационной безопасности Softline

Первый ряд, слева направо: Андрей Ивушкин, руководитель направления экспертного аудита; Кирилл Коноплев, менеджер по маркетингу Отдела маркетингового планирования; Дарья Кретова, координатор отдела маркетинга Управления сервисами; Михаил Карпов, руководитель инженерно-аналитической группы; Мария Нефедова, ведущий технический консультант; Виталия Лепехина, руководитель направления аудита и консалтинга; Мария Чуева, менеджер по продажам услуг; Лада Сафарова, ведущий маркетолог Управления сервисами.

Средний ряд, слева направо: Антон Афанасьев, руководитель прикладных решений информационной безопасности; Максим Вологжанин, менеджер по продуктам; Анастасия Лахтина, руководитель группы продвижения; Евгений Марков, ведущий консультант; Николай Антипов, ведущий консультант; Алексей Бакин, ведущий консультант; Юля Кизимова, менеджер по продажам услуг.

Верхний ряд, слева направо: Сергей Александров, руководитель инженерной группы; Антон Чернов, руководитель проектов; Виктор Гулевич, заместитель директора Управления сервисами; Евгений Подмарев, менеджер по продуктам; Дмитрий Щербинин, менеджер по продуктам; Станислав Любушкин, ведущий консультант; Александр Ветколь, менеджер по продуктам; Максим Пуха, менеджер по продуктам; Дмитрий Васильев, руководитель отдела поддержки продаж решений.

Специальные предложения по безопасности

Avira Small Business Security 2012 по цене версии Professional

При покупке 5, 10 ,15 ,20 или 25 лицензий версию Business Security можно приобрести по цене Professional Security.

Пример: Avira Small Business Security 2012 – 10ПК/2года = 9707 руб., Avira Endpoint Security 10ПК/2 года = 21320 руб.

Спецпредложения ESET

1. «АНТИВИРУСНАЯ ПЕРЕМЕНА» для школ, лицеев и других учебных заведений среднего общего образования.

   Срок действия: до 31 декабря 2012 года.

   ESET NOD32 Antivirus Business Edition по цене 160 р. — защита 1 узла / 1 год действия лицензии.
2. Скидки для медицинских учреждений.

   Скидка 30% на все решения ESET NOD32, как при покупке, так и при продлении лицензий.
3. Миграция с антивирусного продукта другого производителя. Скидка 40% при переходе с антивирусного решения другого производителя.

Сэкономьте от 40% при переходе на Symantec Endpoint Protection

Скидка от 40% при миграции с решений конкурентов на Symantec Endpoint Protection. Скидка предоставляется компаниям малого и среднего бизнеса, имеющим лицензии на эквивалентные продукты.

С Dr.Web все мечты сбываются!

Период проведения: до 14 октября.

При покупке любого акционного продукта Dr.Web вы гарантированно получаете подарок. Главный приз акции — 500 тыс. руб.

В акции участвуют коробочные продукты Dr. Web Security Space Pro в комплектации 2 ПК / 2 года и Антивирус Dr.Web Pro в комплектации 2 ПК / 1 год в акционной упаковке.

Программы «Лаборатории Касперского»

- Программа «Наука»: поставка Kaspersky Open Space Security и Kaspersky Mail & Gateway Security и продление подписки со скидкой 30% для государственных учреждений, занимающихся научно-исследовательской деятельностью.
- Программа «Медицина»: поставка Kaspersky Open Space Security и Kaspersky Mail & Gateway Security и продление подписки со скидкой 30% для медицинских учреждений.
- Программа поддержки образовательных учреждений дает возможность образовательным организациям приобрести программное обеспечение со скидкой до 80%.
- Программа «Мигрируй» предоставляет официальным пользователям антивирусного ПО третьих производителей скидку 50% на продукты «Лаборатории Касперского».

Комплексные решения Dr. Web для средних общеобразовательных учреждений

Компания «Доктор Веб» предлагает учебным заведениям специальные условия приобретения антивирусных продуктов.

Спецпредложения eScan

- Специальные условия для пользователей, которые приняли решение о переходе на антивирус нового поколения eScan с любого другого антивируса. В акции участвуют продукты eScan Antivirus (2 ПК / 1 год) и eScan Internet Security Suite (2 ПК / 1 год).
- Безопасный компьютерный класс для учеников и преподавателей: 10+1. Образовательные учреждения за каждые 10 лицензий eScan получат 1 лицензию eScan Antivirus для домашних пользователей в подарок!

Безопасная почта с GateWall Mail Security

Период проведения: до 31 декабря. Пользователи, которые приобретают (или приобрели ранее) любой почтовый сервер, могут купить GateWall Mail Security со скидкой 50%.

Подробности на http://softline.ru/specials

Услуги и решения по информационной безопасности

softline®

Экспертные услуги

Экспертный консалтинг

- Анализ соответствия системы лучшим практикам
- Анализ эффективности управления ИБ
- Построение моделей угроз, анализ рисков
- Помощь в выборе решений
- Расследование инцидентов ИБ

Технический анализ защищенности

- Сканирование уязвимостей
- Внешнее тестирование на проникновение
- Внутреннее тестирование на проникновение
- Тестирование на проникновение с использованием социальной инженерии
- Тестирование на проникновение беспроводных сетей
- Аудит фактического использования информационных ресурсов
- Аудит безопасности исходного кода приложений

Аудит на соответствие требованиям

- 152 ФЗ
- СТО БР ИББС
- ISO 27001
- PCI DSS
- Внутренней политике ИБ

Управление ИБ

Разработка и внедрение процессов управления ИБ

- Экспертный аудит ИБ
- Разработка стратегии ИБ
- Организация деятельности службы ИБ
- Разработка и внедрение процесса инвентаризации и категоризации активов
- Разработка и внедрение процесса управления инцидентами ИБ
- Разработка и внедрение процесса управления рисками ИБ
- Разработка и внедрение процесса внутреннего аудита ИБ
- Разработка и внедрение процесса обеспечения осведомленности пользователей в вопросах ИБ
- Проведение очного и дистанционного обучения сотрудников
- Поддержка процессов управления (аутсорсинг)

Мониторинг, корреляция событий и управление инцидентами

- Разработка правил корреляции событий
- Разработка процедур управления инцидентами
- Сбор свидетельств и расследование инцидентов ИБ
- Проектирование, внедрение и поддержка решений
- Сравнение и помощь в выборе решений

Управление уязвимостями

- Разработка процедур управления уязвимостями
- Проектирование, внедрение и поддержка решений
- Сравнение и помощь в выборе решений

Системы управления рисками

- Разработка требований, политик и стандартов ИБ
- Разработка правил проверки выполнения требований
- Разработка методик и процедур внутреннего аудита ИБ
- Разработка методик и процедур управления рисками ИБ
- Проектирование, внедрение и поддержка решений
- Сравнение и помощь в выборе решений

Обеспечение ИБ

Прикладные решения

Контроль носителей информации

- Разработка правил использования носителей информации
- Проектирование, внедрение и поддержка

Контентная фильтрация

- Разработка правил доступа в Интернет и спам-фильтров
- Проектирование, внедрение и поддержка

DLP/IRM

- Категоризация конфиденциальной информации
- Введение режима коммерческой тайны
- Разработка правил DLP/IRM
- Проектирование, внедрение и поддержка
- Сбор свидетельств и расследование случаев утечки

Безопасность специализированных систем

- Безопасность мобильных устройств
- Безопасность web-ресурсов
- Безопасность порталов
- Безопасность ЭДО
- Безопасность электронной почты
- Безопасность файловых ресурсов
- Безопасность ActiveDirectory
- Безопасность СУБД
- Безопасность доступа в Интернет
- Безопасность АСУТП
- Безопасность САПР
- Безопасность ERP
- Безопасность платежных систем и систем электронной коммерции
- Безопасность облачных сервисов
- Безопасность использования услуг аутсорсинга
- Безопасность процесса разработки приложений

Инфраструктурные решения

Безопасность серверов и рабочих станций

- Разработка процедур защиты конечных точек
- Проектирование, внедрение и поддержка

Безопасность критичных и фиксированных систем

- Разработка процедур защиты критичных и фиксированных систем
- Проектирование, внедрение и поддержка

Защита виртуальной инфраструктуры

- Разработка процедур защиты виртуальной инфраструктуры
- Проектирование, внедрение и поддержка

Контроль целостности

- Проектирование

Защита сетей

- Разработка требований в отношении узлов сетей
- Разработка процедур обеспечения безопасности сетей
- Проектирование, внедрение и поддержка

Криптографическая защита информации

- Разработка документации УЦ
- Разработка политик и процедур криптографической защиты
- Проектирование, внедрение и поддержка

Идентификация / аутентификация

- Разработка политик и процедур управления ролями и правами доступа
- Разработка и оптимизация ролевых моделей и матриц доступа
- Проектирование, внедрение и поддержка

Соответствие требованиям

ПДН

- Предпроектное обследование, оценка соответствия
- Создание системы защиты ПД в соответствии с ФЗ 152 (требования ФСТЭК/ФСБ)
- Обеспечение соответствия требованиям 152 ФЗ (требования СТО БР ИББС)

СТО БР ИББС

- Оценка соответствия требованиям СТО БР ИББС
- Внедрение СТО БР ИББС
- Поддержка соответствия СТО БР ИББС

PCI DSS

- Оценка соответствия требованиям PCI DSS
- Внедрение PCI DSS
- Поддержка соответствия требованиям PCI DSS
- Аудит на соответствие требованиям PCI DSS
- Аудит на соответствие требованиям PA DSS
- ASV сканирование
- Тестирование на проникновение

ISO 27001

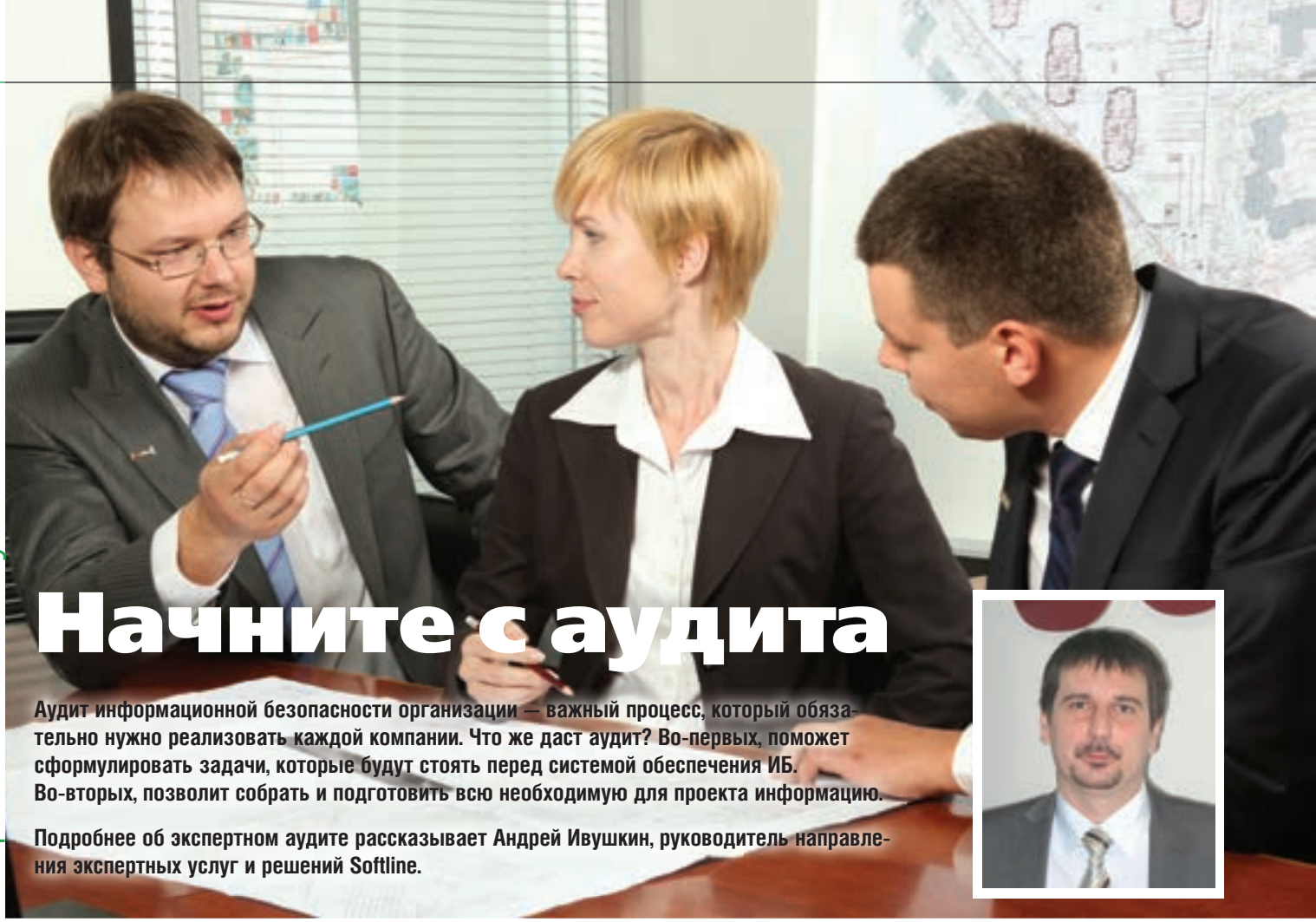
- Оценка соответствия требованиям ISO 27001
- Подготовка к сертификации ISO 27001
- Поддержка соответствия ISO 27001

Коммерческая тайна

- Категоризация конфиденциальной информации
- Подготовка в введению режима коммерческой тайны (разработка документации в соответствии с 98 ФЗ)
- Обеспечение юридической значимости электронного документооборота (в соответствии с 63 ФЗ «Об электронной подписи»)

Аттестация

- Аттестация информационных систем в защищенном исполнении



Начните с аудита

Аудит информационной безопасности организации — важный процесс, который обязательно нужно реализовать каждой компании. Что же даст аудит? Во-первых, поможет сформулировать задачи, которые будут стоять перед системой обеспечения ИБ. Во-вторых, позволит собрать и подготовить всю необходимую для проекта информацию.

Подробнее об экспертном аудите рассказывает Андрей Ивушкин, руководитель направления экспертных услуг и решений Softline.

«Типового» аудита не бывает

Среди специалистов постоянно возникают все новые и новые версии трактовки понятия «IT-аудит». Разногласия порой носят концептуальный характер. Однако для клиентов важным в этом бесконечном споре является не то, что именно отдельные представители сообщества понимают под аудитом, а те средства и наборы методов, которые при этом используют конкретные консультанты, и материальные результаты их труда.

Конечно же, «правильного» и типового аудита, подходящего для любой компании любого сектора экономики, любого масштаба и структуры, просто не существует. Типовая услуга, как правило, несостоятельна, так как каждый клиент — особенный.

Этапы работы

Любой проект по аудиту обычно состоит из нескольких условных этапов, представленных на рисунке ниже.

Каждый этап выстраивается в соответствии с задачей, адаптируется под конкретную компанию. При этом по результатам первого этапа уточняются параметры проводимого проекта и окончательно согласовывается состав работ.

На каждом этапе работ заказчик имеет возможность контролировать и согласовывать промежуточные результаты.

Компания Softline предлагает услуги по аудиту всем заинтересованным в сотрудничестве клиентам. Это аудит, который вы выбираете сами; мы лишь, опираясь на собственный опыт и компетенции, привносим свои коррективы и устоявшуюся терминологию. Желание клиента — основной закон нашей работы, и мы готовы выполнить консалтинговые работы любой сложности. В общем случае наши консультанты проводят анализ ОРД, IT-сервисов, бизнес-процессов клиента, а также анализ соответствия IT-сервисов требованиям бизнеса. Осуществляется выделение угроз и уязвимостей, оцениваются риски, выполняется построение модели угроз, разрабатываются рекомендации и готовится итоговый отчет. Мы «слышим» наших клиентов и стараемся выявить все их потребности, проводим многочисленные встречи, семинары, разрабатываем опросные формы для уточнения пожеланий, внимательно вслушиваемся в доводимую до нас информацию. Мы сотрудничаем, чтобы сделать работу качественно и удовлетворить потребности заказчика. Опираясь на опыт прошлых проектов, собственные компетенции и анализ запрошенных данных, специалисты Softline оценивают трудозатраты, стоимость работ и примерные сроки проекта. Конечно, у любого проекта есть свои риски, но профессионализм и опыт, подтвержденный многочисленными сертификатами и доверием клиентов, внушает уверенность в убедительном и качественном результате нашего труда.

Подход к проведению проекта

Аудит — один из важнейших этапов построения комплексной системы ИБ

Какой аудит?

Аудит соответствия требованиям

- ФЗ-152
- PCI \ DSS
- ISO 27001
- BS 25999
- ISO 20000
- СТО БР-ИБСС
- ФЗ «О коммерческой тайне»
- Другие требования

Аудит безопасности сервисов и систем

- **Аудит безопасности внешнего периметра корпоративной сети**
- **Аудит безопасности внутренней корпоративной сети**
- **Аудит беспроводного сегмента корпоративной сети**
- **Аудит безопасности бизнес-критичных сервисов**
  - Web-порталов
  - Систем ДБО
  - Платежных систем
  - Других систем
- **Технический аудит безопасности подсистем и сервисов**
  - Подсистемы антивирусной защиты
  - Подсистемы защиты от утечек конфиденциальной информации
  - Подсистемы межсетевого экранирования
  - Подсистемы корпоративной электронной почты
  - Другое
- **Тестирование на проникновение**
  - Внешнее
  - Внутреннее
  - Методами социальной инженерии

Комплексный аудит ИБ

- Экспертный аудит ИБ
- Анализ рисков ИБ
- ТЭО внедрения продуктов и решений по ИБ
- Разработка нормативной документации по ИБ

Комплексный аудит IT-инфраструктуры

- Аудит производительности IT-инфраструктуры
- Аудит ЛВС
- Аудит пользовательских рабочих станций
- Аудит серверного оборудования
- Аудит программного обеспечения

Softline®
Россия 8 800 100-00-23
Москва 8 495 232-00-23

Базовые стандарты безопасности давно созданы и не являются застывшей железобетонной глыбой, придавившей всех неотвратимостью своих постулатов. Стандарты — набор гибких рекомендаций. В случае ИБ любой стандарт требует как минимум аудита и оценки рисков. Защитить можно все. Было бы желание защищать! Россия относится к странам с высокими рисками в области ведения бизнеса. В странах такого типа к рискам информационной безопасности, как правило, относятся пренебрежительно. Аттестация — это малая и не самая трудная часть работы. Главное — сопровождение системы.

Вячеслав Медведев,
аналитик компании «Доктор Веб»

Для создания надежной системы ИБ необходимо провести инвентаризацию информационных ресурсов, анализ рисков, разработать концепцию защиты и политики безопасности, создать типовую модель нарушителя и проект системы защиты. На основе этого выбираются и внедряются средства защиты информации. Однако мониторинг и аудит самой системы защиты имеют не меньшее значение, т.к. компания-аудитор, как правило, обладает глубокой экспертизой и может предложить способы оптимизации и усиления надежности системы.

Владимир Чугунов,
руководитель направления по работе
с госзаказчиками компании «Аладдин Р.Д.»

Вы начинаете очередной ИБ-проект, или просто нужна оценка защищенности? А как давно вы проводили IT/ИБ-аудит? Насколько вы уверены в том, что ничего не упущено при постановке задачи? Обеспечение ИБ — чрезвычайно «тонкий» процесс. В ИБ мелочей не бывает в принципе. Так стоит ли рисковать оценкой рисков ИБ, пренебрегая отсутствием или неполноценностью информации? Ведь бизнес может и не пережить вашей ошибки.

Андрей Зеренков,
эксперт по ИБ компании Symantec

Преимущества экспертного аудита от Softline

Клиенты всегда получают набор уникальных возможностей: эксклюзивную экспертизу, профессиональный штат, огромный опыт. При разработке набора настоящих услуг мы привнесли все наши устоявшиеся базовые компетенции: клиентоориентированность, инновационность, сотрудничество, профессионализм и ответственность за конечный результат.

Иногда компании СМБ-сектора задумываются о том, как часто им стоит проводить аудит ИБ? Есть определенные практики и стандарты, предлагающие ответы на данный вопрос. Обычно рекомендованные сроки регулярного проведения аудита колеблются в периоде от 1 до 2 лет.

Возможные сложности

Основные проблемы при проведении аудита информационной безопасности, с которыми мы чаще всего сталкиваемся в своей работе, — это отсутствие документации и описания бизнес-процессов заказчика, а также нехватка какой-либо статистики по инцидентам. Часто случается, что ответственность подразделений в сфере информационной безопасности не разделена, отсутствует дисциплинарный процесс, не определено понятие защищаемой информации.

Наиболее трудозатратный этап аудита со стороны заказчика, требующий наибольшей вовлеченности его представителей, — первый, когда проводится интервьюирование представителей заказчика и заполнение анкетных форм. Этот этап мы стараемся организовать таким образом, чтобы максимально продуктивно выяснить все подробности функционирования инфраструктуры компании. После этого наша аудиторская группа агрегирует все данные и готовит подробный отчет об аудите. Это довольно длительный процесс, в котором представители организации-заказчика принимают минимальное участие.

По итогам аудита специалисты Softline могут разработать комплект нормативной документации по информационной безопасности. Это могут быть как высокоуровневые политики, стратегия или концепция ИБ, так и частные политики безопасности, вплоть до регламентов и процедур.

Кому интересны SIEM-решения?

Построение комплексной системы управления информационной безопасностью (СУИБ) — острая необходимость для любой компании. Развитая ИБ-система, в свою очередь, требует высокого уровня развития всех процессов информационной безопасности: анализа и оценки рисков, управления инцидентами, управления изменениями, управления уязвимостями, мониторинга событий ИБ и других. Высокая зрелость управляющих процессов невозможна без должного развития технического контроля, связанного со всевозможными сложными специализированными средствами автоматизации. Особое место во всей иерархии процессов СУИБ занимают так называемые SIEM-системы. Это системы класса Security Information Management / Security Event Management.

Разработка политики реагирования на инциденты ИБ

Разработка политики реагирования на инциденты информационной безопасности неэффективна без изучения всех процессов системы управления ИБ организации. Как правило, разрабатываемая политика встраивается в имеющуюся систему документации компании и имеющиеся в ней практики по обработке инцидентов ИБ. В этом случае, с учетом лучших мировых практик, существующих в компании технических средств и бизнес-процессов, мы совместно с заказчиком производим классификацию инцидентов и выстраиваем схему реакции на инциденты, создаем регламентирующие инструкции специалистам различного уровня, описываем процесс фиксации и расследования.

Способы оценки рисков в сфере ИБ

Выбор подхода к оценке рисков не определяется только лишь формальными документами и методиками, но обычно основывается на особенностях бизнеса организации, характере и глубине проникновения информационных технологий организации, уровнем зрелости компании в сфере ИБ. Опираясь на существующие стандарты и методологии, а также здравый смысл, вы сможете успешно преодолеть все сложности этого процесса. Сейчас на рынке представлены и специализированные технические средства для анализа рисков, позволяющие с успехом автоматизировать наиболее трудозатратные рутинные операции.

Необходимо с большим уважением относиться к IT-возможностям собственной компании. Развитие информационных технологий внутри организации часто воспринимается не как необходимое, поддерживающее бизнес явление, а как нечто, на что нужно выделять минимум средств. Нельзя забывать о том, что IT- и ИБ-службы дают целый ряд бизнес-преимуществ, повышая эффективность, ускоряя и упрощая защиту вашего дела.

Контакты

Мы будем рады рассказать вам больше или ответить на любые вопросы.

Пишите: security@softline.ru. Звоните: +7 (495) 232-00-23, Департамент информационной безопасности Softline.

Система менеджмента

Чем больше компания, тем сложнее обеспечить ее бесперебойное функционирование и безопасность корпоративных данных. Можно ли построить катастрофоустойчивую бизнес-систему, способную выстоять даже в случае стихийных бедствий и чрезвычайных ситуаций? Как обеспечить защиту информации и оценить ее эффективность? Как сориентироваться в многообразии стандартов и требований к организации системы информационной безопасности? Рассказывает руководитель направления систем менеджмента Департамента ИБ компании Softline Мария Акатьева.

Корпоративная система менеджмента любой компании в том или ином виде состоит из ряда подсистем управления в различных областях: финансы, маркетинг, качество, бухгалтерия и т.д. В состав корпоративной системы менеджмента также входят системы управления информационной безопасностью, информационными сервисами и непрерывностью бизнеса. Для того, чтобы система работала эффективно, все ее составляющие должны быть разработаны на базе единого принципа управления. В качестве такой основы могут быть использованы международные стандарты серии ISO.

Управление IT-сервисами

В 2005 году был выпущен международный стандарт по управлению и обслуживанию IT-сервисов — ISO 20000. Он представляет собой подробное описание требований к системе менеджмента IT-услуг и ответственность за их инициирование, выполнение и поддержку в организациях. Структура стандарта документации в области ISO 20000 следующая:

- **ISO/IEC 20000-1:2005**
  - Информационные технологии — Управление сервисами
  - Часть 1: Спецификация
- **ISO/IEC 20000-2:2005**
  - Информационные технологии — Управление сервисами
  - Часть 2: Нормы и практики
- **BIP 0005**
  - Руководство для менеджеров
- **BIP 0015**
  - Управление IT сервисами — Пособие по самопроверке
- **Для внедрения ISO/IEC 20000**
  - BIP 0030 до BIP 0039

В настоящий момент стандарт ISO 20000—1 используется для сертификации компаний на соответствие. Наличие сертификата ISO 20000 служит признанием профессионализма компании в области IT-сервисов и позволяет гарантировать клиентам отсутствие простоев и сбоев информационной системы. В основе стандарта ISO 20000 лежит ITIL — библиотека практик, содержащая рекомендации по реализации процессов управления IT-услугами. При этом ITIL описывает, как организовать работу по управлению IT-сервисами, а ISO 20000 — как проверить работу по управлению IT-сервисами.

Рис 1. Процессы ISO 20000

Для многих банков, телекоммуникационных компаний, крупных холдингов, а также предприятий, работающих с иностранными корпорациями, особенно важно наличие сертификата ISO 20000, и порой это является обязательным условием ведения бизнеса.

Полезные ссылки:

- www.iso.org — Международная организация по стандартизации
- www.bsi-russia.com/IT+Service+Management/ — BSI Management Systems CIS
- www.itsmf.com — некоммерческий международный форум по ITSM (itSMF)
- www.itsmforum.ru — Российское отделение itSMF
- www.isoiec20000certification.com — сайт itSMF по вопросам сертификации ISO/IEC 20000

Услуги Softline в области управления IT-сервисами:

- осуществление аудитов на соответствие требованиям ISO 20000 и ITIL;
- построение системы управления IT-сервисами (СУИС) в соответствии со стандартами ISO 20000 и ITIL;
- подготовка к прохождению сертификации на соответствие требованиям ISO 20000
- проектирование и внедрение отдельных процессов ISO 20000 и ITIL;
- пакет поддержки системы управления IT-сервисами (СУИС).

Управление непрерывностью бизнеса

Управление непрерывностью бизнеса является важной стратегической задачей. Любая нештатная ситуация может привести к временному прекращению деятельности компании, а, следовательно, к серьезным финансовым убыткам и потере доверия со стороны партнеров и клиентов.

Особенную нишу среди систем управления непрерывностью бизнеса занимают катастрофоустойчивые решения, позволяющие прогнозировать и предотвращать серьезные потери в случае реализации чрезвычайных ситуаций: пожаров, наводнений и др. Системы такого класса минимизируют простои и обеспечивают быстрое возобновление бизнес-процессов, достаточное для того, чтобы происшествие не привело к

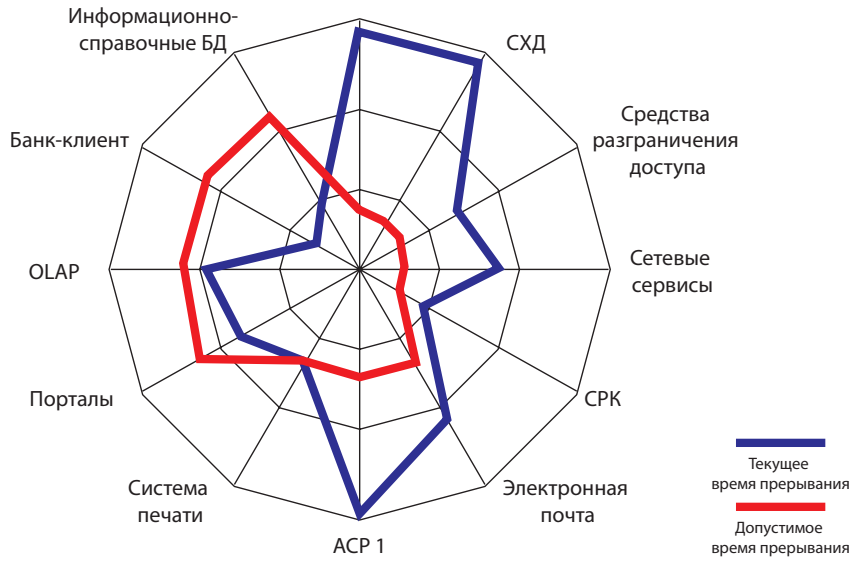


Рис. 2. Очереди восстановления

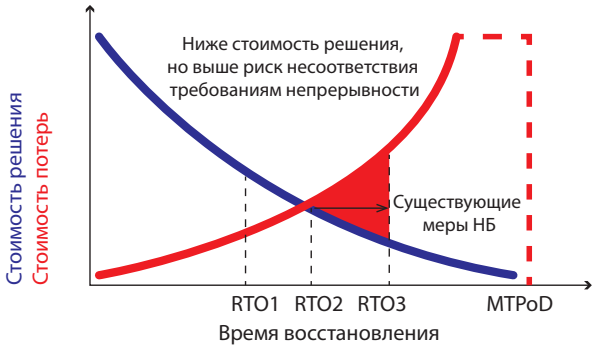


Рис. 3. Стратегия обеспечения непрерывности бизнеса

серьезным потерям или уходу компании с рынка.

Системы управления непрерывностью бизнеса (СУНБ) обеспечивают наличие у компании планов обеспечения непрерывности и восстановления критически важных услуг и сервисов, адекватных ситуации, а также обученного персонала; осуществление регулярных внутренних аудитов; проведение анализа рисков прерывания и времени простоя, допустимого по каждой услуге или сервису.

В мире существует огромное количество практик и стандартов (американских, европейских, австралийских, японских, которые применяются в этой сфере). Однако в России их современной законодательной базы в этой области практически нет. В настоящее время в РФ существует только выпущенное Центробанком Указание 2194-У от 5 марта 2009 г., содержащее рекомендации по структуре и содержанию плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности кредитной организации в случае возникновения непредвиденных обстоятельств. Многие банки проводят работу по обеспечению соответствия своих процессов требованию этого Указания.

В семействе стандартов ISO в этом году появился новый стандарт ISO 22301:2012 Societal security — Business continuity management systems — Requirements, который описывает, как можно выстроить систему непрерывности бизнеса. Компании могут сертифицироваться на соответствие требованиям этого стандарта. Данный стандарт был разработан на базе BS 25999:1/2.

Учитывая роль непрерывности бизнеса в любом секторе экономики, ISO 22301 обладает большим международным потенциалом. Так, ряд стран, в т.ч. Сингапур и Великобритания, начали утверждать ISO 22301 с целью заменить национальные стандарты. Появляется интерес внутри мирового бизнес-сообщества среди тех, кто хочет применить передовую практику и пройти сертификацию на соответствие этому стандарту. Это свидетельство широты аудитории потенциальных пользователей и существенных потенциальных выгод от применения.

ISO 22301 является частью серии стандартов, разработанных техническим комитетом ISO/TC 223 «Социальная безопасность». В настоящее время разрабатывается стандарт ISO 22313, который должен быть опубликован в начале следующего года. Этот вспомогательный стандарт будет содержать рекомендации по внедрению ISO 22301. При построении СУНБ требования по восстановлению непременно должны идти от потребностей бизнеса. Какие-то процессы важно восстановить в течение дня, какие-то — в течение недели, некоторые должны работать в режиме 24x7.

Первым этапом на пути к созданию СУНБ является анализ влияния различных чрезвычайных ситуаций на бизнес. Его результатом будет получение информации о том, в каком порядке и в какое время должны быть восстановлены различные услуги. В соответствии с этим распределяются очереди восстановления различных служб и сервисов внутри компании.

На втором этапе производится анализ рисков прерывания в условиях текущей инфраструктуры, создается план обработки рисков.

На основании анализа рисков прерывания разрабатывается стратегия обеспечения непрерывности бизнеса. Она может состоять из нескольких частей: стратегия обеспечения непрерывности IT, стратегия обеспечения непрерывности деятельности подразделений и т.д.

Затем согласно этой стратегии создаются планы восстановления бизнес-процессов и конкретных ресурсов компании. Они описывают восстановление всех услуг, подразделений и процессов. Подробно расписывается последовательность действий, необходимое оборудование и процедуры. На основании выработанной стратегии в каждой из областей формируются бюджеты на катастофоустойчивые решения.

Анализ рисков прерывания и создание плана восстановления бизнес-процессов можно автоматизировать с помощью системы LRDPS, разработанной компанией SunGard Availability Services.

Наиболее часто системы управления непрерывностью бизнеса интересуют банки и компании, работающие в сфере телекоммуникаций.

Управление информационной безопасностью

Услуги Softline в области СУНБ:

- построение системы управления непрерывностью бизнеса в соответствии с ISO 22301;
- разработка стратегии обеспечения непрерывности;
- разработка планов обеспечения непрерывности бизнеса и IT-сервисов;
- подготовка системы обеспечения непрерывности бизнеса к сертификации на соответствие ISO 22301;
- проектирование и внедрение катастофоустойчивых решений.

Существует множество различных требований и стандартов систем обеспечения информационной безопасности (СУИБ). Зачастую от СУИБ требуется соответствие не одному, а сразу нескольким из них. Обеспечить выполнение этого условия — задача весьма трудоемкая.

Одним из решений данной проблемы является построение системы на базе международного стандарта ISO 27001, содержащего требования для создания, развития и поддержания системы менеджмента информационной без-

Построение эффективной системы ИБ на крупном предприятии — это всегда долгий и непростой путь. Понимая конечные цели и опираясь на библиотеки лучших практик ITIL, можно поэтапно внедрять и интегрировать различные подсистемы ИБ, например, продукты компании «Аладдин Р.Д.» позволяют решить более сотни задач в области ИБ.

Процессу управления ИБ посвящен отдельный раздел библиотеки ITIL, который хорошо сочетается с другими методиками, такими как ISO, COBIT, PCI DSS; COBIT и ISO говорят, что нужно делать, ITIL — как.

Антон Крячков,
директор по продуктам
компании «Аладдин Р.Д.»

Крупные отечественные компании всерьез думают не только и не столько о системах/подсистемах обеспечения ИБ, которые у большинства уже успешно функционируют, а о системах управления ИБ.

Оно и понятно: уровень зрелости компаний (сиречь — высшего руководства) повышается (согласно COBIT), и на повестке дня стоят уже не чисто технические задачи, такие как выбор того или иного продукта и реализация на его базе соответствующей подсистемы ИБ, а вопросы влияния ИБ на бизнес компании в целом. Например, какое воздействие в финансовом измерении окажет на функционирование бизнес-систем внедрение/модернизация какой-либо СОИБ? Или как подобное внедрение скажется на прибыльности предприятия? Что уж говорить о расчете возврата инвестиций в ИБ при отсутствии СУИБ, или об оценке бизнес-рисков, связанных с функционированием IT- и ИБ-систем.

Серьезные организации сегодня уже трудно представить без систем управления ИБ и систем обеспечения непрерывности бизнеса. Если эта тема кажется вам неинтересной или неактуальной, задайте себе вопрос: насколько серьезно вы относитесь к бизнесу вашей компании?

Андрей Зеренков,
эксперт по информационной безопасности
Symantec

Рис. 4. Компоненты СУИБ

опасности. Стандарт можно использовать как базовую основу для реализации любых других требований.

К линейке стандарта ISO 27001 относят:

- ISO/IEC 27000:2010 — Information technology — Security techniques — Information security management systems - Fundamentals and vocabulary (глоссарий)
- ISO/IEC 27001:2005 — Information technology — Security techniques — Specification for an Information Security Management System (требования к СУИБ)
- ISO/IEC 27002:2005 — Information technology — Security techniques — Code of Practice for Information Security Management (практические правила управления СУИБ)
- ISO/IEC 27003:2010 — Information technology — Security techniques — Information security management system implementation guidance (руководство по СУИБ, помощь для пользователей)
- ISO/IEC 27004:2009 — Information technology mentation guidance — Information security management technology men (измерение эффективности СУИБ)
- ISO/IEC 27005:2011 — Information technology — Security techniques — Information security risk management (управление рисками)
- ISO/IEC 27006:2007 — Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (требования к аудиторам СУИБ)
- ISO/IEC 27011:2008 — Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (управление СУИБ для телекоммуникационных организаций)
- ISO 27799:2008 — Health informatics — Information security management

Сертификация проводится на соответствие стандарту ISO 27001. В стандарте нет конкретных технических требований, а есть описания направлений, на которые необходимо обратить особое внимание. В стандарте содержатся принципы управления, которые позволят поднять уровень ИБ компании. ISO 27001 описывает все области: IT-безопасность, HR-безопасность, физическую безопасность, область непрерывности бизнеса с точки зрения ИБ.

Системы менеджмента информационной безопасности особенно актуальны для крупных компаний, имеющих хорошее техническое оснащение. К ним относятся страховые и телекоммуникационные компании, банки, нефтяная промышленность, транспорт. Кроме того, СУИБ может заинтересовать небольшие компании, партнеры которых называют обязательным условием сотрудничества наличие сертификации в сфере ИБ, а также компании, которые хотят выйти на мировой рынок, особенно в связи с вступлением России в ВТО.

Услуги Softline в области СУИБ

- Обследование на соответствие требованиям ISO/IEC 27001:2005.
- Проведение анализа рисков ИБ.
- Построение систем управления информационной безопасностью (СУИБ) в соответствии с ISO/IEC 27001:2005.
- Построение и внедрение процессов управления ИБ.
  - Система управления рисками ИБ.
  - Система управления инцидентами ИБ.
  - Система внутреннего аудита и контроля соответствия.
  - Система управления уязвимостями.
  - Система управления активами и т.д.
- Подготовка СУИБ к сертификации на соответствие требованиям ISO/IEC 27001:2005.

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

2013 CARDEX 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

Mobility Management

Мобильные устройства — это наши бизнес-помощники, которые стали уже практически незаменимы. Не зря же говорят: без телефона — как без рук.

Нельзя умалять значимость ИБ-решений для обеспечения защиты сотовых «трубок» и других устройств: эти продукты оберегают именно от внешних угроз, коих, поверьте, немало.

Рассказывает руководитель направления инфраструктурных решений ИБ Департамента информационной безопасности компании Softline Денис Гундорин.

Сегодня существует единственный действительно эффективный механизм защиты от утечек их данных после потери или хищения мобильного устройства — это криптографические средства. Технологии «удаленного уничтожения данных» не относятся к надежным, поскольку легко обходятся посредством изъятия карты памяти для чтения на другом устройстве. Шифрование же эффективно только против случаев направленного хищения мобильных устройств, но вовсе не в ситуациях, когда утечки происходят в процессе использования устройства его владельцем (намеренно, случайно, по халатности – после утечки уже не играет значения). Это означает, что и сегодня, и в обозримом будущем исключительную важность будут иметь решения по защите от неконтролируемой передачи корпоративных данных на мобильные устройства — т.е. комплексные DLP-решения.

Сергей Вахонин,
IT-директор компании «Смарт Лайн Инк»

Следуя BYOD-тренду компания Check Point планирует к релизу решение Check Point Mobile Enterprise. Обеспечение доступа к корпоративным данным с мобильных устройств является не самой простой задачей, тут нужно найти компромисс между удобством пользователя и уровнем безопасности. В решении Check Point Mobile Enterprise мы предлагаем защищенный клиент, несущий в себе сервисы, которые могут содержать конфиденциальную информацию. В клиент полностью интегрирован клиент для корпоративный почты и календарь.
Авторизацию пользователя можно уже сделать более строгой, чем на устройстве как таковом, тем самым достигается компромисс удобства для пользователя и безопасности для конфиденциальных данных организации.

Дмитрий Воронков,
консультант по безопасности компании
Check Point Software Technologies

Вещь нужная и… уязвимая

Bring your own device — это уже не новая бизнес-тенденция, которая заключается в том, что пользователи берут с собой в офис собственные устройства, чтобы работать через них напрямую. Это удобно, добавляет мобильности, скорость реагирования на письма и решение текущих вопросов растут. Согласитесь, эта тенденция чрезвычайно полезна для бизнеса компаний.

Легко заметить еще одну коррелирующую «новую волну»: организации стали задумываться о том, как защитить информацию, хранящуюся на мобильных устройствах своих сотрудников, особенно на сотовых телефонах. Становится понятно, что такая защита просто необходима, ведь зачастую мобильный телефон — «ключ» к многим ресурсам, содержащим конфиденциальную информацию.

Наиболее актуален вопрос защиты устройств для директоров компаний и топ-менеджеров, у которых на телефонах стоят специальные приложения, связанные с рабочими ресурсами. Высший менеджмент обычно регулярно работает с конфиденциальной информацией, требующей особой охраны от рук злоумышленников.

Но представьте на минуту, что вы — директор фирмы и внезапно потеряли (или у вас украли) телефон/коммуникатор. Подавляющее большинство владельцев телефонов даже не ставят на них пароли, не говоря уже о шифровании ценных данных, и директора, к сожалению, тоже не исключения. Таким образом, попасть напрямую в корпоративные приложения через ваше устройство киберпреступнику не составит никакого труда.

Как защититься?

Специализированные решения, представленные на рынке, во многом похожи друг на друга. Среди них выделим тройку наиболее популярных: Mobile Iron, McAffee Enterprise Mobility Management и Symantec Mobile Management. По какому принципу они работают?

Это так называемые программы MDM — Mobile Device Management, также называемые Mobility Management. Сложно выделить какое-либо одно инфраструктурное решение как самое главное — для разных видов инфраструктуры, разных задач и приоритетов мы подбираем наиболее подходящие решения от разных вендоров.

Программы для защиты мобильных устройств могут зашифровать всю информацию, хранящуюся в памяти и, конечно, установить пароли. Они могут быть длинными и сложными, придуманными с учетом определенной политики. После 3–4 неудачных попыток набора пароля, вся информация будет удалена с телефона автоматически. Подключиться к телефону с целью выкачать все содержимое его памяти с помощью третьего устройства также не получится. Вся передаваемая информация дополнительно шифруется, т.е. создается дополнительный канал шифрования между пользовательским устройством и локальной сетью организации. Поэтому даже если информация будет «перехвачена» где-то по дороге, она превратится в шифр.

Уничтожить информацию на телефоне можно и удаленно. В этом случае нужно просто обратиться за помощью к системному администратору. Телефон «ловит» Интернет, автоматически подключается к корпоративной сети и моментально удаляет все данные.

Программы, защищающие мобильные устройства, очень помогают соблюдению корпоративных политик безопасности.

Контроль интернет-трафика

Организации зачастую выдают своим сотрудникам корпоративные телефонные номера, однако люди используют телефоны не только для того, чтобы звонить и заходить на внутренние локальные ресурсы компании, но и посещают различные посторонние сайты, не связанные с работой.

Разумеется, компания заинтересована в том, чтобы контролировать интернет-трафик, особенно если его оплата производится уже постфактум. Кроме того, выход в Интернет несет с собой дополнительные риски, например, заражение вирусами (которые могут начать рассылку платных sms-сообщений или напрямую воровать конфиденциальную информацию).

Развертывание системы по управлению мобильными устройствами позволяет перенаправить весь интернет-трафик через корпоративную сеть с использованием корпоративных политик, которые помогают очистить трафик от вирусов, подвергнуть web-фильтрации, контролировать траты пользователей и знать, по каким сайтам ходят пользователи. Даже если сотрудник попал в роуминг, его трафиком все равно можно управлять, установить квоту.

Подходы к обеспечению информационной безопасности при использовании пользовательских гаджетов на Android, Google Chrome OS, BlackBerry OS между собой не различаются, т.к. платформы построены по одному принципу.

Внедрение решений mobility management

О связи с другими решениями мы уже рассказали: самым важным является взаимодействие с имеющимися в организации системами, которые осуществляют фильтрацию web-траффика, предоставляют мобильный доступ к рабочим местам сотрудников, а также почтовыми агентами, системами квотирования, учета, контроля доступа. Все они взаимосвязаны и затрагивают друг друга.

В том, что касается этапов и сроков реализации проекта, все зависит от задачи. Приехать, установить и настроить — это недолго: техническая проработка занимается порядка недели. Важно понимать то, как именно нужно правильно настроить продукт, а для этого нужно хорошо подумать. Нужно понять, какие есть пользователи, какими они привилегиями обладают, куда они должны ходить, куда не должны, какой должна быть ролевая модель, какие задать политики использования устройств, как выстроить процессы и сценарии в случае потери телефона, забывания пароля. После того, как все это продумано, можно осуществить этап внедрения, настроить все необходимые правила, обучить персонал. Как и в большей части IT-вопросов, здесь нужен комплексный подход, и наша компания может помочь на всех этапах его решения. Если вам нужны проекты «под ключ» — вы попали по адресу!

Управление привилегированными учетными записями

Отсутствие контроля над привилегированными учетными записями — это непростой вопрос, и различные организации решают его по-разному.

Приведем примеры из историй успеха различных организаций. Например, одним из наших клиентов была крупная компания с большим количеством высокотехнологичного оборудования. Как и любая техника, оно со временем ломается. Необходимо предоставлять доступ для внешней техподдержки вендора, который продал это оборудование. Получается, что некая сторонняя организация получает максимальные привилегии в доступе к серверам, на которых хранится конфиденциальная информация. Для того, чтобы перестраховаться и обрести уверенность в том, что с ценными данными ничего не случится, был внедрен продукт Cyber-Ark. Он позволяет контролировать время, на которое выдается привилегированная запись, и отслеживать, что именно делает сотрудник на конкретном устройстве. Записывается видео, которое отражает абсолютно все действия человека. Благодаря этому становится намного проще расследовать инциденты.

А вот еще пример. Представьте себе дата-центр, который сдает оборудование в аренду и поддерживает работу стандартного ПО, требующегося для работы сервера. Последнюю функцию помогают реализовывать инженеры, поддерживающие сервер. Они непрерывно проводят мониторинг, обновляют ПО, администрируют. Но, опять-таки, эти инженеры являются посторонними людьми по отношению к клиентам, которые хранят на серверах свою информацию. Если клиент хочет иметь на руках самый подробный отчет о работе таких инженеров, ему стоит обратить внимание на продукт, контролирующий привилегированные учетные записи. Это не программа-шпион, она работает открыто. Если дата-центр использует такое ПО, он в открытую заявляет о честности своих сотрудников, а это большое преимущество.

Контакты

Мы будем рады рассказать вам больше или ответить на любые вопросы.

Пишите: security@softline.ru. Звоните: +7 (495) 232-00-23, Департамент информационной безопасности Softline.

По последним опросам 65% компаний разрешают сотрудникам удаленно подключаться к корпоративным сетям. Несмотря на все плюсы такого подхода, появляется серьезный риск для информационной безопасности. И тут компания может выбрать два пути: контролировать корпоративные данные и приложения на личных устройствах, либо полностью взять контроль над устройством.

Корпорация Symantec активно расширяет свой портфель мобильных решений, в том числе помогающих пользователям по всему миру работать с мобильных устройств. Решения Symantec в области поддержки подхода BYOD рассчитаны как на малый бизнес, так и на большие корпорации. Поддержка осуществляется в режиме нон-стоп, поэтому остановка работы систем практически невозможна.

Илья Леженин,
технический консультант компании Symantec

Наши разработки для BYOD являются логическим развитием решений, которые давно и успешно зарекомендовали себя на рынке ИБ, таких как устройство в виде карточки, которая вставляется в слот MicroSD и обладает функциональными возможностями привычных eToken. Для пользователей, которые уже знакомы с инфраструктурой безопасного доступа или электронной подписью, поддержка и внедрение подобных решений не будет сложной задачей.

Антон Крячков, директор по продуктам компании «Аладдин Р.Д.»

Рынок корпоративной мобильной безопасности изначально развивался по аналогии с компьютерной безопасностью. Но оказалось, что игроки, которые выпускают решения для управления мобильными устройствами внутри компаний, имеют здесь достаточно сильные позиции. В результате программы для защиты стали в основном дополнением к системам MDM.

В «Лаборатории Касперского» есть определенные планы по выпуску собственной MDM-системы. В нее будет интегрирован уже существующий корпоративный продукт Kaspersky EndPoint Security for Smartphones для защиты конечных устройств. Система будет интегрирована с другими продуктами «Лаборатории Касперского».

Александр Ерофеев,
директор по маркетингу «Лаборатории Касперского»

Устали от утечек? DLP спешит на помощь!

Data Leak Prevention (DLP, пер. с англ. «предотвращение утечек информации») — это комплекс мер по защите от утечек данных, находящихся в собственности организации. DLP-система представляет собой продукт, который на основе централизованных политик осуществляет идентификацию, мониторинг и защиту данных во время их использования, передачи и/или хранения.

Подробнее о DLP и о системах Antifraud, предназначенных для противодействия мошенничеству, рассказывает Антон Афанасьев, руководитель направления по прикладным решениям ИБ компании Softline.

DLP в ассортименте

Системы DLP широко представлены на российском рынке. Они различаются как по функционалу, так и по архитектуре, стране-производителю и стоимости. Кроме того, концептуально DLP-решения делятся на 2 группы: первая группа защищает шлюзы, вторая устанавливается на рабочие станции.

Цена решений для узкоспециализированных задач намного ниже стоимости систем Enterprise-уровня, которые, например, используются в крупных компаниях с широкой филиальной сетью и большим количеством пользователей. Стоимость может сильно варьироваться в зависимости от набора компонентов, функционала, фирмы-производителя. К примеру, если в компании около 100 рабочих станций, лицензии будут стоить от 200–300 тыс. руб, не считая серверного оборудования.

Что защищаем?

Очень важно определить, что для компании является коммерческой тайной, бизнес-критичной информацией. Это может быть некое ноу-хау, патент, разработка, база данных, любая интеллектуальная собственность. Помочь вам в этом деле смогут эксперты Softline, которые занимаются консалтингом и аудитом. Имея полный пакет документов, которые юридически описывают, что именно компания бережет и боится потерять, намного проще привлечь злоумышленника к ответственности в суде и взыскать определенные санкции.

Зачем контролировать инсайдеров?

Если ознакомиться с аналитикой российского и зарубежного рынков, становится понятно, что сотрудники чаще всего начинают воровать конфиденциальную информацию накануне увольнения. Люди делают это по злому умыслу, чтобы навредить компании, либо для того, чтобы сохранить наработки, которые помогут им трудиться в другой организации. Сотрудники часто уносят с собой различные данные, но такие утечки в большинстве случаев не наносят прямого ущерба бизнесу. Только очень небольшой процент служащих крадут информацию, чтобы таким образом навредить работодателю.

Бывает, что в процессе «грязной» конкурентной разведки компании подкупают сотрудников других организаций, чтобы те за деньги похитили нужные данные. Чаще всего подкупить пытаются не рядовых сотрудников, а тех, кто имеет доступ к закрытым хранилищам — например, системных администраторов.

Системы DLP во многом помогают оценивать и отслеживать такие ситуации, так как общение ведется не в открытую, не всегда по телефону, а зачастую по электронной почте, а копирование документов осуществляется через съемные устройства.

Стоит ли внедрять систему тайно, или лучше сделать это явно? Узнав, особенно случайно, о том, что в компании внедрена «слежка», сотрудники становятся аккуратнее, они перестают посещать сомнительные сайты в рабочее время и стараются ничего лишнего не отправлять. За счет этого срабатываний в системе DLP становится меньше. Иногда внедрение проходит в тайном режиме, если руководство уже точно знает, что информацию воруют. В этой ситуации прежде всего надо поймать вора, и только потом предавать гласности. Случается, что систему устанавливают не всем, а только некоторым «избранным» сотрудникам.

Сертификаты и аккредитации

Более 80% всех российских разработок сертифицированы, из западных систем — только около 50%. Дело в том, что процесс сертификации ФСТЭК занимает в среднем полгода с момента раскрытия исходного кода. За это время разработчик уже успевает, как правило, выпустить обновленную версию. Через год сертификация на конкретный билд уже устаревает.

Вопрос сертификации своеобразен. Многое зависит от того, какую информацию решение будет защищать. Например, если система будет защищать персональные данные, ее обязательно нужно сертифицировать по всем требованиям законодательства. С точки зрения защиты коммерческой тайны сертификационных требований к системам DLP нет, то есть для определенного рода задач сертифицированных решений не требуется.

Настраиваем DLP

Сбор информации зависит от того, какие технологии заложены в DLP-системе, какие правила в ней настроены, какие данные она защищает. Вначале система внедряется в режиме мониторинга, а затем плавно переводится в режим блокировки. На этапе мониторинга бизнес-процессы не останавливаются, но собирается информация по сработавшим политикам. Есть возможность корректировать политики, уменьшая тем самым процент ложных срабатываний. По окончании мониторинга у вас на руках будут только нужные правила.

Какие технологии здесь используются? Можно задать поиск по ключевым словам и выражениям — но в этом случае процент ложных срабатываний будет высоким. Технология цифровых отпечатков намного эффективнее. И все же ложные срабатывания произойдут и в этом случае, ведь документы иногда очень похожи друг на друга, например, если неконфиденциальный документ создан на основе конфиденциально-

го. Технология цифровых меток также высокоэффективна, так как цифровые метки ставятся на конкретные конфиденциальные документы.

В режиме мониторинга важно правильно задать все правила, обучить систему. Желательно, чтобы в компании был четко описан процесс информационного потока: как и куда данные двигаются, через кого, по каким каналам. В Softline такого рода услуги оказывает экспертная группа с международными сертификатами. Имея все сведения об особенностях инфопотока, намного проще составить грамотные правила для DLP. В среднем период мониторинга занимает 3–6 месяцев.

Идеальной DLP-системы, которая подходила бы всем, пока не изобрели. У каждого продукта свой набор технологий, поэтому не всегда одной системой можно решить весь набор задач. Многие организации уже используют несколько решений, дополняющих друг друга, от разных производителей. Чаще всего, сначала мы советуем внедрить одну систему, а по прошествии некоторого времени (год-полтора), если нужно, вторую. Важно понять, какие задачи первая система решить не может, и только после этого подбирать дополнительные решения.

На шлюзы? Или на рабочие станции?

Куда установить DLP-систему, зависит от конкретной ситуации. Не стоит забывать о том, что DLP-системы поддерживают только ПО Microsoft. Есть продукт, работающий с Linux Red Hat, а вот для Mac пока ничего не предлагается. Поэтому, если в компании используется ПО Mac, выявить утечку можно только с помощью сетевого модуля.

Нет необходимости ставить агент на рабочую станцию, если сотрудникам запрещено пользоваться мессенджерами типа ICQ и Skype, а USB-выходы заблокированы, ведь в этом случае конфиденциальную информацию можно украсть только при помощи Интернета, а его контролирует система, установленная на шлюзе. А вот если сотрудникам разрешено использовать ноутбуки или другие переносные устройства, на них обязательно стоит установить агент, который будет работать независимо от того, находится ли устройство в корпоративной сети или вне ее.

Инцидент = прямой убыток?

За рубежом DLP-системы внедряют очень активно, поскольку существуют законодательные требования о том, что в случае утечки персональных данных компания должна оповестить об этом всех, в том числе другие организации и клиентов, чьи данные «утекли». За границей уже подсчитана стоимость соответствующей рассылки в человеко-часах и стоимость расходных материалов, размер штрафов — благодаря всему этому стоимость DLP-системы уже в какой-то степени окупается, и становится возможным вычисление возврата инвестиций. Зарубежный опыт предполагает свои требования к законодательству, свой подход к бизнесу. Что касается российских реалий, у нас поддается оценке риск утраты информации определенного вида с финансовой и репутационной точек зрения. С финансовой точки зрения в любом правильно составленном контракте есть пункт о конфиденциальности. Если обнаружена утечка информации конкурентам или в общий доступ, можно применять санкции. При сотрудничестве с зарубежными компаниями также очень важна репутация — при утечке партнер может отказаться от дальнейшего взаимодействия, что означает упущенную прибыль. Также очень хорошо защищена законодательством патентная информация: нередко при сотрудничестве конструкторские бюро получают патентную информацию от партнеров, но если она попадет в общий доступ, то обладатель патента может привлечь к серьезной ответственности, подразумевающей значительные штрафы. Все зависит от конкретного иска и конкретного рода информации.

Очень опасна утечка данных о маркетинговых акциях, особенно в ритейле: перед осуществлением акции проводятся специальные исследования, анализ структуры целевой аудитории и ее потребностей, изучение результатов аналогичных акций и основанные на этом оценки планируемой прибыли. И если вся эта информация попадет к конкурентам, то те смогут реализовать акцию значительно быстрее, потому что большая часть работы, включая финансовый анализ, уже осуществлена. Когда известно планируемое время начала акции, то конкуренты могут провести акцию раньше и быстрее получить прибыль. Любая маркетинговая акция включает накладные расходы на заказ полиграфических материалов, расклейку и заказ рекламы, и если другая компания раньше вывела услугу на рынок, то деньги потеряны уже до начала кампании. И эти убытки тоже можно оценить — другое дело, что в России немногие умеют это делать. Обычно наиболее адекватное представление об этой проблеме у департаментов, занимающихся оценкой рисков. Если у компании нет такого департамента, или он только начал свою работу, то мы готовы объяснить, показать и научить, как делать оценку рисков в бизнесе и в ИБ, и тогда дальнейшее развитие организации будет гораздо проще.

Что такое системы Antifraud?

Antifraud (англ.; произносится «антифрод») — это относительно новый термин, поэтому рассказ о нем начнем с азов. Если рассматривать зарубежные практики, то на Западе с мошенничеством активно борются 4 основных сегмента компаний: банки, страховые компании, телеком-операторы и ритейл. Сейчас системы противодействия мошенничеству выходят на отечественный рынок — так же неспешно, как и несколько лет тому назад они выходили на Западе. Полностью внедрили их в России считанные единицы. Направление для нашей страны является новым, и двигателем для его развития стали банки. Это связано с новым законом о платежной системе, вступающем в силу с 1 января 2013 года, согласно которому при мошенничестве банк должен возместить ущерб клиенту, если тот не принял все необходимые требования банка по защищенности. Страховые компании тоже проявляют большой интерес к этой тематике, обращаются, консультируются и т.д. Телекомы используют узкоспециализированные решения в своей сфере, которые представляют собой западные разработки, усовершенствованные собственным штатом программистов. На данном этапе в первую очередь банки борются с внешним мошенничеством: внутреннее отошло на второй план в связи с законом о национальной платежной системе, и, кроме того, банки не склонны предавать эту информацию огласке.

Пример внутреннего мошенничества — использование «спящих» счетов, к которым редко обращаются и на которые не начисляются проценты. Деньги с них переводятся на другие, процентные счета, а если вдруг владелец «спящего» счета пришел за ним, то деньги возвращаются назад. Также мошенничество может быть связано с выдачей кредита — получающему кредит предоставляются определенные льготы, на которые он не должен иметь права. Есть некоторые телекомы, которые заключают договоры о беспроцентном переводе средств с платежными системами. Но схемы мотивации в компаниях при этом могли остаться те же: премии сотрудников могут начисляться в зависимости от объема средств, перетекающих между компаниями. И не всегда эти показатели означают реальный рост сотрудничества: иногда деньги просто переводятся туда-обратно. Встречаются виды мошенничества, связанные с фальсификацией оценок ущерба в страховых компаниях или оформлением несуществующих ДТП. Обычно для борьбы с этим выделяются специальные сотрудники, которую анализируют статистику по обращениям в компанию.

С точки зрения противодействия мошенничеству для услуг Softline характерен комплексный подход: от проработки вариантов до внедрения и сопровождения. Это аналитика возможных способов мошенничества на основе зарубежных практик, разработка вариантов решений по противодей-

ствию мошенничеству, описание правил для выявления мошенничества и внедрение антифродовых систем.

Внедряем антифродовую систему

Антифрод-системы можно разделить на 2 класса: первые работают по факту, т.е. сначала собираются данные, которые затем используются для вынесения вердикта о том, было ли совершено мошенничество; вторые работают по модели. Для них разрабатывается модель лояльного клиента, его поведение, то, как он осуществляет платежи, куда переводит средства. Создаются среднестатистические модели и модели для конкретного рода клиентов. Потом модель описывается, заносится в систему и та начинает выявлять отклонения. Циклы внедрения тоже различаются. Модельный тип внедряется намного дольше, в то время как система, функционирующая по правилам, может начать работу уже через несколько недель после запуска. Кроме того, сроки внедрения зависят от того, насколько хорошо клиент представляет возможные схемы мошенничества в своей компании.

В настоящий момент в России разработкой антифродовых систем занимаются в основном производители программ ДБО (дистанционного банковского обслуживания). Они создают узкоспециализированные решения, ориентированные на конкретного заказчика — например, они борются только с внешним мошенничеством, но не с внутренним. Любая система, которая предназначена для широкого распространения, должна иметь определенный цикл зрелости — пройти стадию обучения и внедрения у широкого круга заказчиков.

В отношении антифродовых систем иногда говорится, что они блокируют не только мошеннические операции — например, в некоторых интернет-магазинах проходит только половина платежей по кредитным картам. Так каким же образом лучше «отсеивать» законные операции от незаконных?

Рассмотрим для примера банковскую сферу. Раньше антифрод-системы там работали по следующим правилам. Составлялся портрет пользователя — некий аналог модели. Например, если говорить о юридических лицах, то пользователь, который производит платежи — это, как правило, бухгалтер. Обычно он делает это с рабочего места, находящегося на территории Российской Федерации. Если платежи неожиданно происходят из, например, Вьетнама и Багамских островов, это вызывает подозрение. С учетом этого многие хакеры стараются имитировать поведение пользователя и проводить платежи от его лица. Если говорить о взломах банкоматов с помощью скиммеров, которые считывают информацию о кредитной карте, то мошенники, собравшие такие данные, обычно стараются как можно быстрее снять как можно больше денег со всех счетов, которые попали к ним в доступ. Подобное поведение несложно отследить.

При управлении банковским счетом через Интернет у пользователя тоже есть определенная модель поведения. Когда хакер получает чей-либо логин и аккаунт, он первым делом направляется на страничку, где можно снять весь остаток, и сразу же производит платеж. Он не заглядывает на другие закладки, не изучает акции, историю платежей, а сразу приступает к снятию средств. Таким образом, можно сказать, что антифрод руководствуется здравым смыслом и выделяет все странное поведение. В том, что касается остановки платежей, на данный момент банки не готовы осуществлять подобные превентивные меры — невозможно настолько быстро проанализировать легальность транзакции, с учетом того, что законодательство определяет сроки выполнения транзакций, — но они могут с успехом использоваться в ритейле и страховой сфере, где срок проверки не критичен.

Тот, кто хочет воровать деньги, всегда старается делать это как можно быстрее и незаметнее. Здесь всегда будет вестись борьба между защитой и нападением, и преимущество будет то у одной стороны, то у другой.

Что еще нужно учесть?

В первую очередь, заострите внимание на информационной системе, которая используется в компании: на каких решениях она построена, по каким протоколам передаются данные, как эти данные зашифрованы, как функционируют текущие средства защиты, какое клиентское и серверное ПО используется. Если система разработана неправильно с точки зрения логики или архитектуры приложений, используется некорректный программный код, то хакер может получить привилегированный доступ к системе. Так что сама по себе покупка DLP или антифрода — это еще не панацея, нужно также следить за своими приложениями, делать проверку кода на наличие уязвимостей. Зарубежные компании нередко отдают свой код сторонним экспертам на проверку, хотя в России это пока не принято.

Внедрение antifraud-систем — процедура дорогостоящая и долгосрочная, поэтому любая такая система проходит пилотное тестирование. Это делается для того чтобы посмотреть, как она работает, из чего состоит, как она интегрируется в сетевую архитектуру, как устроена связь с клиентскими приложениями, легко ли ее обслуживать, создавать новые правила и задачи, и насколько она эффективна для данного клиента. Нередко бывает, что после «пилота» становится ясно, что данное решение не подходит, и предлагаются другие варианты. В среднем пилотные внедрения требуют 1–2 месяца, иногда и более.

Преимущества Softline как интегратора

Мы предлагаем услуги по анализу возможных видов мошенничества внутри компании, исследование внешней защищенности, тесты на проникновение, анализ правильности программного кода клиента, поиск в нем уязвимостей. Также Softline осуществляет экспертную оценку моделей поведения в antifraud-системах и построенных бизнес-процессов (например, использование разделения полномочий, необходимость утверждения решения несколькими сотрудниками и т. д.). При внедрении системы по борьбе с мошенничеством ее нужно интегрировать с другими системами, поэтому наличие экспертизы и высокая техническая квалификация специалистов Softline являются особенно важным преимуществом. Когда у интегратора есть мощности, есть ресурсы и есть специалисты, которые обладают знаниями по самым разнообразным системам, то с таким интегратором гораздо легче работать. Борьба с мошенничеством и с утечками — это сокровенная тема для любого клиента, поэтому заказчик заинтересован в том, чтобы все работы выполнял один исполнитель, и у Softline есть все средства для этого.

Тенденции

Во всем мире растет количество мобильных устройств и интерес компаний к облачным услугам. Границы защищаемого периметра начинают размываться. Западные разработчики еще год назад начали работу над новыми средствами защиты информации, проходящим через мобильные и облачные каналы. Вендоры Symantec и McAfee уже предлагают средства контроля мобильных средств, причем Symantec вывел на рынок средство для защиты iPad, чтобы контролировать все данные, проходящие через устройство. Кроме того, в ближайшее время уже должны появятся агенты для Mac.

Если говорить о применении DLP-систем для защиты облачных технологий, то новым трендом является защита от утечек конфиденциальной информации через сервисы для совместной работы вроде Dropbox. Подобная функция пока есть не у всех DLP-решений, но в будущем предполагается дополнительное развитие.

Требования заказчиков в DLP- и антифрод-системам растут, конкуренция на рынке высокая. Поэтому производители стараются активно выпускать новый функционал — для того, чтобы надежнее защитить конфиденциальные данные вашей компании.

PCVEXPO

11-я международная специализированная выставка

22 – 25 октября 2012 года
Москва, ЦВК «Экспоцентр»

В сердце Москвы, в центре успеха!

- насосы
- компрессоры
- арматура
- приводы и двигатели

получите билет на сайте www.pcvexpo.ru

Организаторы:

MVK
В составе группы компаний ITE
Тел.: +7 (495) 935 81 00
E-mail: Medvedeva@mvk.ru

РАПН

АСКОМП

Генеральные информационные партнеры:

НАСОСЫ и ОБОРУДОВАНИЕ

Информационные спонсоры:

ТПА

АКВАТЕРМ

СФЕРА НЕФТЕГАЗ

Газовая промышленность

Четко и ясно: compliance management

Понятие «комплайенс» (англ. compliance) означает выполнение требований стандартов, законодательства и т.д.) и соответствие им, следование букве Закона. По этому направлению компания Softline предлагает целый спектр услуг: проекты по защите персональных данных в соответствие с требованиями законодательства, по введению режима коммерческой тайны или обеспечению юридической значимости электронного документооборота, оказывает услуги по поставке и внедрению сертифицированных ФСТЭК РФ и ФСБ РФ средств защиты информации и др.

Рассказывает Виталия Лепехина, руководитель направления аудита и консалтинга Департамента информационной безопасности Softline.

Все то, что напрямую связано с областью compliance, обычно начинается с малого — и заканчивается чем-то большим. Несмотря на то, что сам проект из области compliance является комплексным и сложным, но даже такие запросы как «можете ли вы поставить сертифицированное средство защиты» или «что вы посоветуете для выполнения требований» часто превращаются в глобальные комплексные проекты, многие из которых расширяются в нескольких направлениях. Наши специалисты начинают помогать с доработкой внутренних документов, которые компания уже разработала сама, или создают их «с нуля», проведя всесторонний аудит. Ведь внутренние юристы или IT-специалисты не всегда могут разобраться во всех тонкостях законодательства в области информационной безопасности. Жесткого шаблона работы нет — мы делаем все исходя из конкретной ситуации у клиента. И успешно работаем в этом направлении уже более 5 лет!

Помощники требуются?

В первую очередь, услугами по защите персональных данных пользуются компании, которые обрабатывают большое количество данных о клиентах — физических лицах. Это банки, страховые и медицинские компании, коллекторские агенства и др. Именно эти организации первыми начали всерьез заботиться о выполнении требований законодательства. У многих компаний до сих пор присутствуют бизнес-процессы, к которым законом предъявляются особые требования — это передача информации третьим лицам, обработка данных без согласия субъекта (в частности, рекламирование товаров и услуг без предварительного согласия субъекта) и т.д. При этом компания может выполнить проект по защите персональных требований самостоятельно. Привлечение внешнего исполнителя, интегратора, является правом организации, но не обязанностью.

Интегратор, в свою очередь, обязан соответствовать определенным требованиям, он должен иметь лицензию ФСТЭК РФ на деятельность по технической защите конфиденциальной информации.

В Интернете можно найти большое количество предложений касательно подготовки пакета документов по защите персональных данных стоимостью от 9 тыс. руб. и сроком выполнения — от 30 минут. Стоит ли пользоваться услугами таких компаний — личный выбор каждого. Наше мнение таково: не надо покупать шаблоны документов весьма сомнительного качества, тем более, что эти же шаблоны можно скачать из Интернета бесплатно. Такие «документы» нуждаются в серьезной переработке, «заточке» под конкретную компанию. Более того, такие «документы» не всегда соответствуют текущим требованиям законодательства.

Хороший результат — всегда итог совместной работы Заказчика и Интегратора. Интегратор следит за тем, чтобы все созданные документы соответствовали текущим требованиям законодательства, Заказчик следит за соответствием бизнес-процессам. Тогда созданные документы не «кладутся в стол», а начинают действовать, функционировать как часть бизнес-процесса компании, приносить видимый эффект. Они не просто бумаги для соответствия регулятивным требованиям закона, а инструмент, повышающий качество работы сотрудников.

Штрафные санкции

Новостные агентства сообщают о том, что планируется значительное увеличение штрафов за нарушение требований закона о защите персональных данных. Законопроект об этом обсуждается уже очень давно. Более того, о повышении штрафов заговорили еще в 2006 году, после ратификации конвенции Совета Европы. Сегодня в КОАП есть статья 13.11, которая регламентирует штрафы, и их размеры в среднем составляют 5 или 10 тыс. руб. В сравнении со стоимостью проекта это очень незначительная сумма. Сейчас многие клиенты предпочитают по 10 лет откупаться штрафами, но не тратить деньги на внедрение. В законопроекте, о котором идет речь, штрафы за первичное нарушение для юридических лиц планируется увеличить до 200–500 тыс. руб, а за вторичное — от 500 тыс. до миллиона. Для физических лиц они тоже увеличены. Таким образом, суммы штрафа и стоимости проекта становятся сопоставимы, и компании будет проще 1 раз выполнить проект и следовать требованиям, чем постоянно платить штрафы. Помимо штрафов, законопроект содержит разделы о передаче Роскомнадзору функций передачи дел в суд и в прокуратуру, повышении срока исковой давности с трех месяцев до года. Безусловно, при его принятии возрастет и приток в бюджет и количество обращений в консалтинговые компании, а также изменится отношение к этому закону в целом — компании начнут воспринимать систему защиты персональных данных как неотъемлемый элемент своей инфраструктуры. Кроме того, сейчас информационный этап уже пройден, и субъекты персональных данных осведомлены о существовании закона. Теперь они начнут более тщательно относиться к обработке персональных данных и станут понимать, что за это компании платят серьезные штрафы — таким образом, повысится доверие к компаниям.

Популярный вопрос: предоставляют ли компании, оказывающие услуги по защите персональных данных, гарантию на результаты своей работы? Т.е., если после внедрения систем защиты персональных данных или консалтинга в этом направлении, регуляторы все равно выписывают штраф, несет ли финансовую ответственность компания, оказывавшая эти услуги?

Здесь нужно смотреть на условия договора — на то, какие гарантии клиент может получить. Есть понятие аттестации информационной системы по требованиям безопасности информации. Это процесс, который регламентируется документами ФСТЭК. Если у компании есть данный аттестат, то все претензии по выполнению или невыполнению законодательных требований можно переводить на ту компанию, которая провела аттестацию — т.к. они проверили все системы и, являясь лицензиатом ФСТЭК РФ, могут выносить суждение о соответствии либо несоответствии требованиям закона.

Аттестация

Время действия аттестации — это тот момент, из-за которого многие избегают ее прохождения вообще. Во-первых, аттестат выдается на срок до 3 лет. Во-вторых, любое изменение в этой аттестованной системе по сути аннулирует действие аттестата. Клиент не может внести в свою информационную систему практически никаких изменений, не уведомив об этом компанию, выдавшую Аттестат. Это очень непрактично, от этого страдает и безопасность, и бизнес-процессы, в то время как технологии и оборудование устаревают. С другой стороны, для государственных информационных систем аттестация является обязательным требованием. И здесь очевидно несовершенство законодательства. То, какие гарантии может дать интегратор, зависит от условий договора. Стандартные условия подразумевают следующее: если после выполнения проекта приходит проверка и выявляет какие-либо нарушения, то создается совместная комиссия, выявляется виновная сторона, которая и несет финансовую ответственность, потому что нарушение может возникнуть не только в результате некачественной работы Интегратора, но и в результате того, что клиент внес какие-либо неутвержденные изменения в свою систему, ее техническую или документационную часть. Впрочем, ни у одного из наших клиентов, которые проходили проверку после реализации проекта, нарушений выявлено не было.

Аттестация обязательна для государственных учреждений, исполнительных и муниципальных органов. Выгода есть: претензии по результатам проверки можно перенаправить на компанию, которая выполнила аттестацию. Но недостатков у нее все-таки больше. И коммерческим компаниям нет смысла ее выполнять — они попадают в очень сильную зависимость от аттестующей их организации и не имеют больших выгод. Им выгоднее вносить в договор условия о том, что если у регуляторов возникают претензии, то интересы компании будет представлять интегратор. Естественно, эта услуга оплачивается дополнительно, но это своего рода страховка.

Сейчас все образовательные учреждения обязаны выполнить Постановление Правительства РФ от 27 января 2012 г. № 36 «Об утверждении Правил формирования и ведения федеральной информационной системы обеспечения проведе-

Требования регуляторов. Что это — кошмарный сон, обуза, навязываемая услуга?

На приведение в соответствие нужны ресурсы, средства и время. И в планах этого нет… В результате нужно искать, изворачиваться, договариваться, но все же выполнять. Непросто и неприятно.

Но стоит ли относиться к этой теме однозначно негативно? Да, законодательство пока несовершенно, и удовлетворить всем его требованиям нелегко. Но есть профессионалы, которые в этом помогут разумеется, не безвозмездно.

IT-инфраструктура, в которой наведен порядок, работает надежнее и стабильнее, технический персонал вместо реагирования на мелкие запросы может заняться повышением собственной квалификации и развитием корпоративных систем, а внедренные процессы освобождают время менеджеров, которое ранее тратилось на бесконечный контроль исполнения. Дело за малым — надо лишь начать, то есть внедрить систему оценки соответствия стандартам как вашей организации, так и регуляторов.

Андрей Зеренков,
эксперт по информационной безопасности
Symantec

Противодействие угрозам ИБ имеет одно из приоритетных значений в организации бизнеса, поскольку с этим связаны существенные финансовые и репутационные риски. Compliance как решения для информационной безопасности, создаваемые «под ключ», сейчас имеют большую популярность. Для их построения необходимо иметь штат разносторонних специалистов высшего уровня. Это под силу только крупным компаниям-интеграторам, имеющим необходимый штат и опыт, поэтому сегодня все больше компаний предпочитают пойти по более простому пути приобретения готовых решений.

Владимир Чугунов,
руководитель направления по работе с государственными заказчиками компании «Аладдин Р.Д.»

ния единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего профессионального образования и региональных информационных систем обеспечения проведения единого государственного экзамена» и рекомендации Федерального Центра Тестирования по подключению к региональным (для школ) или федеральным (для техникумов, колледжей и вузов) информационным системам. Для осуществления данного подключения нужно выполнить определенные требования. Компаний, которые на текущий момент могут оказывать такие услуги на рынке, достаточно мало. Перечень средств защиты информации, которые разрешено использовать, также ограничен, есть перечень действий по оформлению документации, которые нужно выполнять. Компания должна выбрать схему подключения, по которой она будет подключаться, согласовать ее с Федеральным Центром Тестирования и затем реализовать ее, причем выполнить это все нужно до 1 октября. Уже этим летом прием студентов должен был идти через федеральную информационную систему и все ВУЗы должны быть подключены к ней, но если учесть, что соответствующее постановление вышло в январе, в то время как в мае-июне уже начались госэкзамены, то сейчас эта проблема стала наиболее актуальной. Но даже после 1 октября эта услуга все равно останется востребованной.

СТО БР ИББС и Закон «О Национальной платежной системе»

СТО БР ИББС — это банковский стандарт, который относится только к организациям кредитной системы и банкам. Это верхнеуровневый документ для правильной организации системы управления информационной безопасностью банковских организаций. Он не является в чистом виде обязательным, и стандарт может быть банком как принят, так и не принят. Но если приказом по банку этот стандарт принимается, то его исполнение становится обязательным. Более того, текущая версия Стандарта Банка России вступает в противоречие с законодательными актами по защите персональных данных. В частности, была понижена категория персональных данных, АБС выносится за рамки информационной системы, обрабатывающей персональные данные и т.д. И если до принятия поправок в июле 2011 г. принятие Банком Стандарта позволяло понизить требования регуляторов при проверке, то сейчас регуляторы проверяют одинаково, независимо от того, принят стандарт или нет. Другое дело, что Стандарт комплексно рассматривает создание системы информационной безопасности от технических систем до менеджмента, не упираясь в одну только защиту персональных данных.

Закон «О Национальной платежной системе» похож на ФЗ «О персональных данных», в нем содержатся основные определения и термины, а так же устанавливаются требования к организации деятельности всех участников платежной системы.

Несомненным плюсом закона о НПС является принятие правовых и организационных основ национальной платежной системы, регулирующих порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а так же определение требований к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе.

С 1 января 2013 г. вступает в законную силу положения ст. 9 ФЗ №161 «О НПС», которая обязует оператора по переводу денежных средств (кредитные организации) возмещать клиенту сумму операции, совершенной без согласия клиента. Таким образом, после того как клиент уведомит банк о факте хищения денежных средств с его лицевого счета, банк обязуется возместить клиенту всю похищенную сумму и провести внутреннее разбирательство по данному инциденту. Результатом данной проверки будет определена сторона, виновная в реализации угрозы ИБ и хищения денежных средств. В случае признания таковой стороной клиента банка формируется запрос на возврат полный суммы денежных средств переведенных банком в связи с данным инцидентом.

Для выполнения требований по обеспечению безопасности участниками национальной платежной системы при осуществлении переводов денежных средств, необходимо смотреть подзаконные акты ФЗ-161. В данных актах интегрированы требования СТО БР ИББС и PCI DSS и ЗПДн, так как в платежных системах циркулируют и персональные данные, и платежная информация, и данные платежных карт.

Угрозы в области платежных систем

Наиболее актуальными угрозами информационной безопасности в платежных системах являются угрозы, реализуемые на стороне клиента и в «облачной» среде взаимодействия платежных систем. Ярким примером нарушения конфиденциальности информации может стать массовая утечка данных клиентов одной известной международной платежной системы, через оператора по переводу денежных средств — компании Global Payments.

Противодействовать актуальным ИБ-угрозам в платежных системах можно путем выполнения всех требований по обеспечению безопасности переводов денежных средств. Выполнение комплексных проектов по информационной безопасности, начиная с обследования и заканчивая периодическим аудитом построенных систем защиты информации, поможет минимизировать риски.

2012 CEE-SEC(R)
Software Engineering Conference in Russia

VIII Международная научно-практическая конференция «Разработка ПО»

1-2 ноября 2012 г. Москва. Центр Digital October

Аудитория:
до 800 делегатов
из 250+ компаний
и 20+ стран

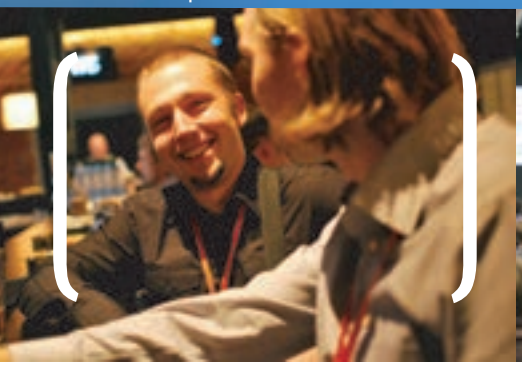
Приз 1000 Евро
за лучший
исследовательский
доклад

Бесплатное
участие для
докладчиков

Приглашаем

- Программистов и инженеров качества
- Системных аналитиков и архитекторов
- Лидеров команд и менеджеров проектов
- HR-специалистов и руководителей производства
- Исследователей, студентов и аспирантов
- Продуктовые компании, компании, реализующие ПО «в облаке»
- Центры разработки и филиалы транснациональных компаний
- Аутсорсинговые компании и ИТ-департаменты государственных учреждений

Подробнее: www.secr.ru, contact@secr.ru, +7 812 336 93 44



Спонсоры

РВК
<epam>
FIRST LINE SOFTWARE
EMC²

Партнеры

РУС СОФТ
OMG
Cloud Standards Customer Council
Agile Russia
РАСПО
ISDEF
Software Russia
Хостинг Центр

BYOD значит любит

Сейчас почти у каждого есть какое-нибудь мобильное устройство — нетбук, планшет или хотя бы смартфон. И конечно, многие сотрудники компаний и организаций приносят все это на работу, хотят подключиться к сети и другим ресурсам из офиса и даже вне офиса. О плюсах и минусах этого явления рассказывает Алексей Лукацкий, менеджер по развитию бизнеса компании Cisco

— Алексей, на ваш взгляд, концепция BYOD приносит бизнесу больше пользы, нежели неудобств?

— Я начну со статистики. Недавно мы в Cisco провели опрос в разных странах мира, задав пользователям простой вопрос: «Без чего вы не можете обойтись в своей жизни?»

Ответы были обескураживающими с точки зрения психологии, но интересными с точки зрения информационных технологий. 43% респондентов не может представить свою жизнь без своего партнера. 64% — без автомобиля, 84% — без Интернета. И целых 97% не могут представить своей жизни без мобильного устройства.

То есть, хотим мы того или нет, но мобильность прочно вошла в нашу жизнь, и изменить эту ситуацию нам не под силу даже путем тотальных запретов. Концепция BYOD («Bring your own device» или «Принеси свое устройство») всего лишь узаконивает то, с чем уже и так сталкивается почти каждая организация, даже режимная. Почти в любом госоргане, в котором мне приходится бывать, либо у руководства, либо у айтишников есть удаленный доступ с собственных мобильных устройств к электронной почте, календарю, адресной книге, а может и к оборудованию для его настройки. Что уж говорить об обычных компаниях, в которых нет никаких режимных требований. Поэтому концепция BYOD — это данность, с которой надо не мириться, а направлять в правильное русло.

Что же касается плюсов, то основной из них — рост производительности, который выражается сразу в нескольких показателях. При наличии собственного мобильного устройства, подключенного к корпоративной или ведомственной сети, работа следует за вами, а не вы за работой. Это позволяет работать везде, где есть Интернет. Другой плюс проявляется в крупных городах, особенно в Москве. Согласно данным Росстата среднестатистический москвич работает всего 5 с половиной часов в день (при наличии восьмичасового рабочего дня). А все из-за пробок, заставляющих людей больше времени проводить в дороге, а не на работе. Концепция BYOD помогает и тут. Могу поделиться опытом компании Cisco — переход на мобильный удаленный доступ позволил повысить производительность сотрудников на 10–40% в зависимости от их роли. Средняя продолжительность рабочего дня увеличилась на 1–1.5 часа. Разумеется, утверждать, что доходы компании Cisco также увеличились на 10–40% я не буду, но рост пропорциональный. Увеличение лояльности тоже присутствует, хотя его сложно оценивать. Однако есть косвенная оценка даруемых преимуществ. По оценкам Cisco, во всем мире 66% сотрудников готовы к снижению заработной платы на 10% при наличии возможности время от времени работать дома.

— С какими угрозами безопасности приходится сталкиваться компаниям, сотрудники которых используют на работе персональные мобильные устройства?

— Согласно опросам Cisco, до 70% сотрудников признаются в нарушении правил информационной безопасности ради облегчения своей жизни. А все потому, что большинство нарушаемых правил «традиционны» и не учитывает специфику мобильных устройств. Именно человеческий фактор является основной угрозой безопасности. Вторая основная угроза — попытка применить к мобильному устройству традиционные подходы в области ИБ, или вовсе отсутствие каких бы то ни было подходов. Чего только стоит желание выстраивать традиционную периметровую защиту в организации, в которой сотни мобильных устройств, причем половина, а то и 2/3 из них принадлежат не компании, а сотрудникам! А мечта создать контролируемую зону по документам наших регуляторов, разработанных в 90-х годах? Чисто технологические угрозы — вредоносное ПО, утечки данных, хождение через незащищенные сети, установка ПО из непроверенных источников — давно известны и для обычных ПК. Почти ничего нового с технологической точки зрения в безопасности мобильных устройств нет. Есть просто акценты, которые надо расставлять при защите мобильного устройства.

— Какие мобильные платформы представляют наибольшую угрозу с точки зрения безопасности?

— Картина регулярно меняется, но одно можно сказать точно. Платформы, изначально разрабатываемые для корпоративного применения, защищены больше. Речь идет о BlackBerry. С точки зрения информационной безопасности компания RIM сделала очень много и остается пока непревзойденной. Однако, сделав ставку только на корпоративное применения, RIM упустила свой шанс и постепенно теряет долю рынка, уступая ее другим платформам, которые комбинируют интересы корпораций и частных пользователей, потребности бизнеса и личной жизни.

Второй по защищенности я бы назвал платформу iOS компании Apple. С одной стороны, закрытость платформы, а с другой — полный контроль всех приложений, распространяемых через AppStore. Это дает возможность считать эту платформу лучшим выбором с точки зрения безопасности, не говоря уже про наличие огромного количества приложений для личной жизни и бизнеса. Платформа Android завоевывает популярность у пользователей, но в корпоративной среде ее применяют не так уж и часто — слишком уж много вредоносных и просто уязвимых приложений распространяется через Google.Play. Хотя именно для BYOD-устройств платформа Android, пожалуй, самая популярная.

Платформы Bada и Symbian сдают свои позиции, а в отношении Windows Phone пока рано что-то говорить — очень уж она молодая. В целом же, защищенность платформы зависит не от ее изначальной уязвимости, а от того, насколько правильно пользоваться заложенными в нее механизмами защиты и общей стратегии безопасности BYOD, принятой в организации.

— Корпоративные мобильные устройства: часто ли организации выдают их сотрудникам для работы? Защищать их ведь намного легче, чем личные устройства.

— Мы прошли и через этот этап, но он за кажущейся простотой несет в

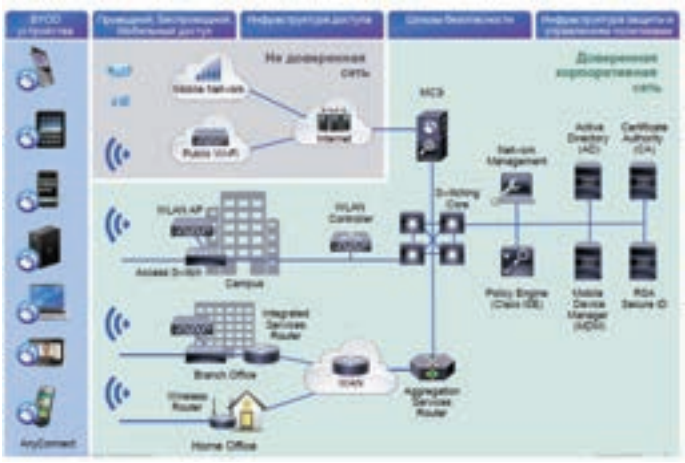
себе и ряд проблем. Во-первых, это существенный рост капитальных затрат на приобретение мобильных устройств. Во-вторых, это рост операционных затрат на IT-поддержку таких устройств. И, наконец, это снижает со временем лояльность, как ни парадоксально. Оказывается, что через полгода-год пользования мобильным устройств его владелец хочет сменить платформу на более новую и модную. А с корпоративным устройством это не срабатывает — срок амортизации еще не закончился. Что делать пользователю? Либо оставаться с немодным устройством, либо параллельно использовать купленный за свои деньги гаджет. Обычно большинство идет по второму варианту, вновь приходя к концепции BYOD, но уже тайком от службы IT и безопасности.

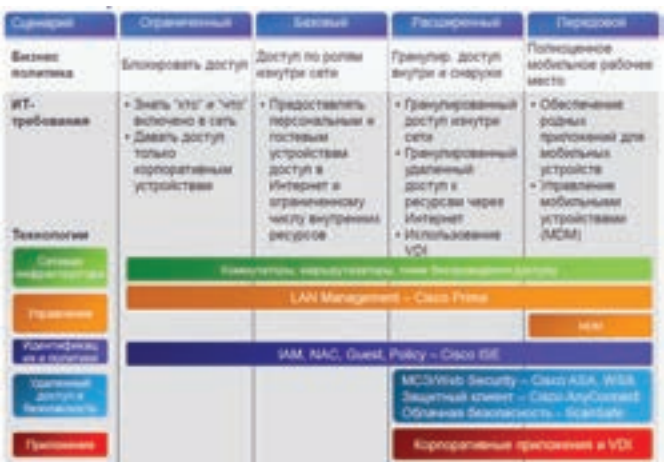
Поэтому через вариант использования корпоративных устройств проходят многие компании, но быстро понимают, что это не выход. С другой стороны, защита собственного устройства пользователя не сильно отличается от защиты корпоративного. Зачем тогда выбирать не лучший сценарий?

— Как должна выстраиваться политика безопасности для BYOD? Как соблюсти баланс интересов между работниками, желающими иметь доступ к любой корпоративной информации из любой точки мира, и службой безопасности? Как выглядит «правильная» политика – что регламентирует, как исполняется, контролируется и т.д.?

— Этому вопросу можно посвятить целую статью, поэтому я ограничусь перечислением тех тем, которые должны быть включены в правильную политику:

- Анализ рисков и модель угроз. От чего защищаемся? Только ли от вредоносного кода? Или проникновения на мобильное устройство? Какого отношения придерживаемся к утечкам данных? Будем ли мы контролировать доступ к сайтам, ненужным для работы?
- Отношение к BYOD. Если нет, то почему? Если да, то какие требования должны соблюдаться пользователями таких устройств при нахождении в офисе (например, сдавать ли их в камеру хранения при входе) или подключении их в корпоративную сеть?
- Используемые мобильные платформы. Любые или из ограниченного списка? Большинство компаний ограничивает применение iOS, BlackBerry и Android, но встречаются и Windows Phone 7, Symbian, webOS и т.д.
- Доступ изнутри сети. Принципы защиты и контроля доступа мобильных устройств внутри корпоративной сети (сертификаты и т.д.).
- Доступ извне сети. Аналогично предыдущему, но для доступа извне. Например, доступ только через VPN и никак иначе. Применение средств контроля доступа NAC на периметре. Использование отдельной точки входа для таких устройств. Вариантов может быть масса. В этом же разделе должны быть описаны приложения и сервисы, к которым имеют доступ сотрудники извне. Например, только к почте и адресной книге. А может быть, еще и к календарю, бизнес-приложениям.
- Отношение к Jailbreak. Хотя по статистике число взломанных устройств очень незначительно — около 8-10%, это нельзя сбрасывать со счетов. Ведь взломанное устройство — это потенциальная угроза для установки уязвимых приложений.
- Приложения. Есть ли ограничения на используемые приложения? Планируется ли собственная разработка? Магазины приложений — новый канал проникновения вредоносных программ на мобильное устройство. Есть ли ограничения на установку приложений с Интернет-магазинов? Какова процедура установки? Напрямую из Интернета или только через ПК, где приложение можно проверить на вирусы?
- Функция «антивор». Как искать украденное или потерянное устройство (например, в iPhone/iPad эта функция является встроенной)? Как дистанционно удалить данные на устройстве? Как дистанционно заблокировать устройство? Как защититься при смене SIM-карты?
- Шифрование данных на устройстве. Встроенное шифрование или внешняя система? Шифровать все или только отдельные разделы устройства?
- Удаленное управление и контроль. Как организовать удаленное управление и контроль использования? Делается ли это централизованно или отдается на откуп пользователям? Необходимо ли отключать удаленно отдельные аппаратные компоненты — Wi-Fi, камера, Bluetooth, диктофон и т.д.?
- Compliance. Надо ли обеспечить соответствие регулятивным требованиям (ФЗ-152, СТР-К и т.д.), или этот риск принимается как неактуальный или несущественный?
- Соответствие политикам IT и ИБ. Как контролируется установка патчей? Как обеспечить наличие нужных локальных настроек? Как проверяется наличие нужных программ на мобильном устройстве? Как снять конфигурацию удаленно? Как «накатить» новую конфигурацию на устройство? Как провести инвентаризацию устройства?
- Аутентификация. Локальная аутентификация на устройстве (правила выбора PIN-кода). Аутентификация при доступе к корпоративным ресурсам. Аутентификация при доступе к локальным приложениям (например, к почте). Возможен ли удаленный доступ администратора к пользовательскому устройству? А если оно принадлежит не компании?
- Антивирус.





- Личная защита. Ведение черного списка номеров (в том числе и для защиты от SMS-спама). Скрытие от посторонних глаз любой информации по отдельным абонентам (включая SMS, почту и т.д.).
- Контентная фильтрация. Перенаправление всего трафика на корпоративные средства контентной фильтрации. Использование облачных технологий защиты Web-доступа (например, Cisco ScanSafe). Как контролировать утечки информации по электронной почте и другим каналам? Защита от спама (включая SMS-спам).
- Используемые механизмы защиты. Ориентация на встроенные механизмы (например, ActiveSync) или внешние средства защиты.
- Слежение за устройствами. Будем ли контролировать местонахождение устройства? Как?
- Защищенный VPN-доступ.
- Восстановление и резервное копирование.
- Управление инцидентами. Как осуществляется расследование? Как собираются доказательства на мобильных платформах? Управление журналами регистрации событий.
- Управление. Как управляются мобильные устройства с точки зрения вышеперечисленных задач? Как осуществляется troubleshooting?

Основное сомнение, которое высказывается службами ИБ при внедрении концепции BYOD заключается в том, что они вторгаются в частную жизнь пользователя, который может быть против установки на его устройство средств защиты. Однако посмотрите с другой стороны. Если вы пускаете чужое устройство в корпоративную сеть, то вы хотите его контролировать. А если сотрудник хочет работать удаленно на своем мобильном устройстве, то у него нет выбора, как только разрешить четко регламентированное «вмешательство» в его собственный гаджет. Если же он отказывается от этого, то и доступа в корпоративную сеть не получает.

— Как совместить использование собственных устройств и требования ФЗ-152, если вы попадаете под его действие?

— Если мы говорим об истинно мобильных устройствах (смартфонах и планшетниках), то однозначного ответа тут нет. Если с мобильных устройств передаются ПДн по Интернету, то позиция ФСБ на момент написания статьи однозначна — должны применяться сертифицированные средства криптографической защиты, которых не так уж и много для мобильных платформ, а для некоторых попросту нет (например, для iOS). Попытки обойти это ограничение есть, но все они достаточно спорны. Поэтому единственная универсальная рекомендация в данной случае — не обрабатывать ПДн на мобильном устройстве, или применять технологии терминального доступа.

— В чем заключаются сложности управления привилегированными учетными записями? Какие риски влечет его отсутствие? Как защититься или минимизировать риски от инсайдерства среди привилегированных сотрудников?

— В информационной безопасности существует принцип минимума привилегий, который позволят снизить число инцидентов с привилегированными сотрудниками. Однако полностью исключить риск инсайдерства невозможно, и тут нам на помощь приходят технологии контроля утечек информации, которые существуют и для мобильных устройств. Они при правильном применении позволяют еще больше снизить число реальных инцидентов. И, наконец, никто не отменяет работы с персоналом.

— Каков подход компании Cisco в области практики BYOD?

— Для нас концепция BYOD — это не что-то новое. Мы внедрили у себя удаленный доступ еще в конце 90-х годов, а разрешили работу сотрудникам с их мобильных устройств в середине 2000-х. А так как мы в своей сети, как ни странно, используем свои же собственные решения, то именно на себе и проверяли, насколько наши технологии и подходы эффективны. Мы не делаем разницы между мобильным и традиционным доступом, между проводным и беспроводным, между доступом изнутри сети и снаружи. Все это осуществляется через сетевую инфраструктуру, которая и является основной для обеспечения как обычного доступа мобильных корпоративных устройств, так и защищенного доступа собственных устройств сотрудников. Поэтому ничего нового в нашем подходе нет — из года в год мы улучшаем наши технологии и решения. Основой для построения защищенного доступа выступает сервер политик Cisco Identity Service Engine (ISE), который принимает на себя основной удар по принятию решений о предоставлении доступа к запрошенным ресурсам в зависимости от полномочий пользователя или устройства, запрашивающих доступ. Правила политики доступа реализуются на сетевой инфраструктуре, состоящей из традиционных и виртуализированных коммутаторов, маршрутизаторов, точек беспроводного доступа и межсетевых экранов. Мобильные устройства защищаются с помощью унифицированного защитного клиента Cisco AnyConnect, работающего под управлением Apple iOS, Windows Mobile/Phone, Android, Symbian, Windows, Linux, MacOS и т.д. А дополнительный уровень контроля и защиты обеспечивают наши традиционные средства обеспечения безопасности — межсетевые экраны Cisco ASA, средства контентной фильтрации и контроля утечек Cisco Web Security Appliance и Cisco E-mail Security Appliance, а также средства облачной безопасности Cisco ScanSafe.

— Насколько трудоемко внедрение и поддержка данной технологии на базе решений Cisco?

— Как я уже упомянул выше, для нас нет разницы — организуется ли традиционный проводной доступ с ПК на базе Windows или мобильный доступ с «чужого» устройства на базе Android или iOS. Политика на базе Cisco ISE едина для всех типов мобильных и традиционных устройств и распространяется на любые сетевые устройства, через которые осуществляется доступ. Поэтому никакой разницы между обычным построением сети и организацией BYOD-доступа для компании Cisco нет. Но если стоит задача дополнительного контроля самих мобильных устройств, а не только их доступа по сети, в игру вступают решения из так называемого MDM-сегмента (Mobile Device Management) — Zenprise, Afaria, Mobile Iron, Good, AirWatch и т.д. Именно они берут на себя дополнительную защиту и контроль уже самого мобильного устройства и хранящихся на нем данных и приложений. А Cisco ISE в свою очередь может быть интегрирован с этими MDM-решениями и включать в политику доступа мобильных устройств дополнительные параметры.

Отдельно хочется отметить автоматизацию основных рутинных задач, в частности по идентификации и профилированию мобильных устройств, подключающихся к корпоративной сети. За счет заложенных в Cisco ISE возможностей устройства iOS iPhone могут быть отделены от iOS iPad, Android от BlackBerry, Windows от Linux, а Cisco IP Phone 7960 от Cisco IP Phone 7941G. Помимо этого Cisco ISE включает в себя свыше 90 профилей, позволяющих идентифицировать продукцию различных производителей — от Motorola и Nortel до NetGear и Sony PSP. Такая идентификация наряду с интеграцией с Active Directory позволяет провести четкую грань между теми, кого пускать в сеть, а кого нет. При этом такое решение не является бинарным (пускать или нет). Оно включает в себя множество оттенков — когда пускать, откуда пускать, с какого устройства, какое приложение и т.п. Именно это позволяет решениям Cisco реализовать полноценный принцип минимума привилегий и существенно снизить число инцидентов безопасности с применением мобильных устройств.

allsoft.ru®

MS Office 2010

Электронные ключи MS Office 2010
Очевидная экономия и мгновенная доставка ключей по e-mail

Microsoft Office — популярный офисный пакет приложений, в состав которого входит программное обеспечение для работы с различными типами документов: текстами, электронными таблицами, базами данных и др. Универсальный набор инструментов программы позволяет использовать ее на предприятиях малого и среднего бизнеса, а также для дома и учебы.

MS Office для дома и учебы 2010

Цена коробочной версии: ~~2 967,11 р.~~

Цена электронной версии: **2 699,00 р.**

MS Office для дома и бизнеса 2010

Цена коробочной версии: ~~9 346,45 р.~~

Цена электронной версии: **8 490,00 р.**

MS Office профессиональный 2010

Цена коробочной версии: ~~18 246,71 р.~~

Цена электронной версии: **16 200,00 р.**

8 800 200 2233
(бесплатно по России)

www.allsoft.ru | sales@allsoft.ru

Снижаем сложность и стоимость выполнения требований PCI DSS!

Продукт для комплексной защиты серверов Trend Micro Deep Security

Готовясь к прохождению аудита на соответствие стандарту PCI DSS, многие компании сталкиваются со сложностью выполнения множества технических и организационных требований стандарта. Выполнение большинства техтребований означает эффективное использование соответствующих подсистем ИБ, таких как подсистема межсетевого экранирования, обнаружения и предотвращения атак, подсистема антивирусной защиты и т.д.

Денис Безкоровайный, CISA, CISSP, CCSK,
технический консультант компании Trend Micro в России и СНГ

Выполнение требований — долго и дорого?

Для каждой подсистемы ИБ необходимо тщательно выбрать продукт, позволяющий выполнять требования стандарта, а затем внедрить решение в инфраструктуру.

Стандартный цикл включает в себя выбор продукта, проектирование архитектуры решения на его основе, разработку соответствующей проектной и эксплуатационной документации, обучение администраторов безопасной работе с продуктом, и, наконец, внедрение.

Какие же ИБ-решения нужны для успешного выполнения требований PCI DSS? Наличие некоторых из перечисленных ниже продуктов явно требуется по стандарту, оставшаяся часть может существенно облегчить и упростить компании выполнение ряда указаний стандарта. Давайте перечислим все:

- **антивирусная защита;**
- **межсетевое экранирование с динамической фильтрацией;**
- **системы обнаружения и предотвращения вторжений;**
- **шифрование данных при хранении;**
- **шифрование сетевых коммуникаций (при использовании незащищенных сетевых протоколов);**
- **контроль целостности;**
- **сбор и анализ журналов регистрации событий;**
- **система управления учетными записями и правами доступа;**
- **системы двухфакторной аутентификации пользователей;**
- **сканер безопасности для сканирования на уязвимости;**
- **межсетевой экран для web-приложений (web-application firewall);**
- **сканер для обнаружения беспроводных сетей;**
- **система предотвращения утечек и обнаружения конфиденциальных данных.**

Как видно, перечень достаточно обширный, использование в компании всех этих систем может затронуть значительную часть ИБ-бюджета. Затраты компании на приведение в соответствие складываются в том числе и из стоимости самих продуктов, технического проектирования, обучения ИБ-администраторов, стоимости инфраструктуры для развертывания продуктов ИБ, а также стоимости дальнейшего администрирования и поддержки всех подсистем информационной безопасности.

Как упростить процесс соответствия требованиям стандарта?

Во-первых, задача упрощается, если в компании уже внедрены какие-либо необходимые продукты и приняты защитные меры, но нередко в организации функционирует лишь часть всех требуемых подсистем.

Во-вторых, можно сократить цикл проектирования, обучения и внедрения, если внедряемым продуктом можно «закрыть» сразу несколько подсистем ИБ, то есть с помощью одного продукта выполнить несколько требований PCI DSS. Здесь проявляется эффект масштаба: чем больше требований одновременно выполняет продукт, тем меньше будет общая стоимость внедрения и владения в расчете на каждую подсистему ИБ.

В большинстве компаний, перед которыми стоит задача соответствия PCI DSS, можно найти очень разнообразную гетерогенную вычислительную среду: платежные приложения, системы интернет-банкинга, процессинг, бэк-офис. Все эти системы могли развиваться в разное время и базироваться на абсолютно разных технологиях. Нередко в таком ЦОДе требуется защищать всю палитру серверных операционных систем — это и различные версии Linux, Windows, Solaris на экзотических платформах, HP-UX, AIX и прочие. Важно, чтобы решение по безопасности, используемое для выполнения требований PCI DSS, могло одинаково хорошо защищать весь этот серверный парк.

Также стоит помнить, что и к самим решениям по безопасности, и их системным компонентам также должны применяться требования стандарта PCI DSS. Например, в системе защиты должно быть реализовано разделение полномочий пользователей, ведение записей аудита всех действий привилегированных пользователей, возможность настройки парольной политики и прочие функции, необходимые по требованиями PCI DSS.

Есть ли комплексные решения?

Рассмотрим продукт Trend Micro Deep Security, в котором реализовано несколько подсистем ИБ, позволяющих выполнять множество требований PCI DSS, среди которых:

- антивирусная защита;
- межсетевое экранирование с динамической фильтрацией;
- система обнаружения и предотвращения вторжений, виртуальный патчинг;

- контроль целостности;
- анализ журналов регистрации событий;
- межсетевой экран для web-приложений (web-application firewall).

Система позволяет защищать различные операционные системы (Windows, Linux, Solaris, AIX, HP-UX) и выполнять множество требований PCI DSS на базе одного агента, с единой консолью и логикой управления для всех защитных модулей. Архитектура продукта Deep Security включает агентов безопасности и виртуальный апплаенс для безагентской защиты в виртуальных средах VMware. Реализация в виде программного решения и низкие требования к каналам связи между агентской и серверной частями позволяют эффективно и без существенных затрат использовать Deep Security в распределенных инфраструктурах.

Фукционал Deep Security с точки зрения требования PCI DSS

Trend Micro Deep Security обеспечивает комплексную защиту критически важных серверов и рабочих станций, в том числе виртуальных. Описание подсистем и функционала с упоминанием соотвествующих пунктов стандарта приведено ниже.

- Подсистема межсетевого экранирования (1.2, 1.3, 1.3.6, 1.4). В состав продукта входит полноценный программный межсетевой экран уровня хоста, который отслеживает и блокирует трафик. Обеспечивается динамическая (stateful) фильтрация трафика, требуемая в п.1.3.6. Межсетевое экранирование может применяться как дополнительная защитная мера для реализации стратегии Defense in depths, для сегментации сети и логического разделения ресурсов, с целью уменьшения области действия PCI DSS.
- Антивирусная защита (5.1, 5.1.1, 5.2). Модуль антивирусной защиты реализован как на традиционном агенте, так и на виртуальном апплаенсе, позволяя защищать физические и виртуальные машины от вредоносного ПО.
- Система обнаружения и предотвращения вторжений, виртуальный патчинг (11.4, 6.1, 6.2). Deep Security использует глубокий пакетный анализ для выявления и предотвращения атак, направленных на эксплуатацию уязвимостей в ОС и приложениях. Выделенный центр аналитиков информационной безопасности — Trend Micro Security Center — своевременно получает информацию об уязвимостях из десятков источников, а также непосредственно от производителей программного обеспечения, например, участвуют в программе Microsoft Active Protections, что позволяет получать информацию об уязвимостях еще до выхода официальных патчей, устраняющих найденные уязвимости. На базе этой информации аналитики Security Center выпускают обновления правил для Deep Security, которые блокируют возможность использования уязвимостей, даже без установки патчей от производителей ПО (виртуальный патчинг).

  Для облегчения внедрения и эксплуатации Deep Security использует механизм сканирования машин (физических и виртуальных) для выявления отсутствующих программных обновлений, установленных приложений и их версий. После этого система выдает рекомендации — набор защитных правил, наиболее точно подходящих к каждой конкретной машине.

  Также виртуальный патчинг может использоваться в качестве компенсирующей меры для систем, на которые патчи от производителей не могут быть установлены по какой-то причине в течение 1 месяца, как того требует п. 6.1.
- Защита web-приложений (SQL Injection, XSS) как дополнение к процессу анализа уязвимостей web-приложений (6.6). Модуль глубокого пакетного анализа позволяет проверять все запросы к web-серверам, выявлять и блокировать попытки использования типовых атак на web-приложения, такие как SQL Injection и Cross Site Scripting (XSS) и другие, в том числе атаки на web-серверы и их ОС. Продукт позволяет «из коробки» останавливать эти и многие другие атаки. Функционал модуля защиты web-приложений во многом соответствует рекомендуемым PCI требованиям к системам класса Web Application Firewall.
- Контроль целостности (11.5, 10.5.5). Deep Security позволяет контролировать целостность важных файлов и ключей реестра операционных систем и приложений, в том числе журналов регистрации событий, с целью поиска вредоносных и незапланированных изменений. Система позволяет проводить сканирование по требованию, по расписанию или в реальном времени.
- Анализ журналов регистрации событий (10, 10.3, 10.5.3, 10.6). Deep Security реализует сбор и анализ журналов событий операционных систем и приложений для обнаружения важных событий, относящихся к безопасности. Система может автоматически выявлять из сотен тысяч событий события безопасности, следы подозрительной деятельности, действия привилегированных пользователей, или же собирать абсолютно все события с подконтрольных систем. Если в компании уже используется SIEM-система или централизованный Syslog-сервер, то Deep Security может пересылать в них события для дальнейшей корреляции, формирования отчетов и архивации.
- Профили безопасности (2.2). Вся логика защиты в продукте Deep Security основывается на правилах, описывающих, от каких атак или уязвимостей происходит защита, и что делать в случае обнаружения атаки. Все правила сгруппированы в удобные для использования профили защиты — наборы защитных механизмов, характерных для какого-либо типа сервера или приложения. Например, из коробки доступны следующие профили защиты: Windows Server 2003, Linux Server, Solaris Server, Windows 7 Desktop и др.

  Управление всеми защищаемыми машинами и защитными компонентами (межсетевой экран, глубокий пакетный анализ, анализ журналов и контроль целостности и др.) происходит через единую консоль управления — Deep Security Manager.
- Защита виртуальной среды. Рекомендации PCI в части использования виртуализации указывают на специфичные риски, которые должны быть учтены при использовании виртуализации для обработки данных держателей платежных карт. В продукте Deep Security используется виртуальный апплаенс и интеграция с системой управления VMware vCenter для снижения таких рисков, как:
  - включение ранее остановленных виртуальных машин, на которых устарели средства антивирусной защиты и отстутствуют необходимые критические обновления ОС и приложений;
  - создание новых машин, не соответствующих корпоративной политике безопасности, например, без средств антивирусной защиты.

  Deep Security использует механизмы VMware для защиты виртуальных машин без необходимости установки агента: специальный компонент Deep Security Virtual Appliance устанавливается прямо в среду ESX-сервера и благодаря использованию VMSafe NET API и vShield Endpoint API защищает сразу все виртуальные машины, работающие на защищаемом ESX/ESXi.

Найти универсальное решение для выполнения требований PCI DSS, подходящее сразу всем компаниям, невозможно в силу различия в архитектуре, наличия в организации уже используемых средств ИБ и многих других факторов. Одно можно сказать точно — существенно снизить временные затраты и стоимость защитных мер можно за счет многомодульных продуктов, способных выполнять сразу множество требований стандарта, и одинаково эффективно защищать операционные системы и приложения в гетерогенной среде современных финансовых организаций.

Защитим малый бизнес вместе!

Знаете ли вы, какой «дикий запад» творится до сих пор на ниве защиты среднего и малого бизнеса от информационных угроз? Заказчики данного сектора упорно не хотят признавать ряд серьезных проблем, пользуются бесплатными или нелегальными средствами обеспечения безопасности и тем самым рискуют своим бизнесом. Исследование проблем и тенденций в области IT-безопасности в сегменте малого и среднего бизнеса, проведенное нами в 22 странах мира, наглядно демонстрирует ситуацию и подсказывает, как стоит действовать.

Олег Гудилин,
руководитель управления маркетинга
в России, странах Закавказья и Средней Азии
компании «Лаборатория Касперского»

Что мешает малому бизнесу обеспечить безопасность?

Согласно проведенному исследованию, треть российских компаний СМБ-сектора считает, что преимущества коммерческих антивирусов по сравнению с бесплатным ПО не оправдывают затрат на их приобретение. Чуть меньше (23%) респондентов по этой же причине считают для себя допустимым использование нелицензионного ПО. Более того, свыше четверти специалистов отметили, что вынуждены использовать бесплатные или нелицензионные версии антивирусных продуктов из-за жестких бюджетных ограничений в компании. В регионах России эта проблема стоит особенно остро: о вынужденном переходе на бесплатные и нелицензионные решения заявили 32% региональных компаний. В Москве этот показатель чуть ниже — 23% организаций.

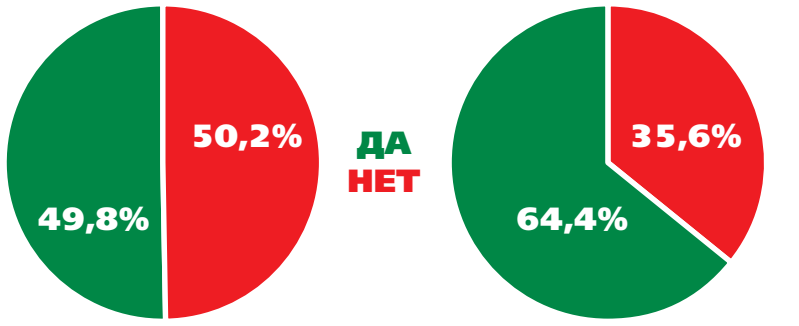
Проблески разума, тем не менее, встречаются среди наших потенциальных клиентов. 49% ответивших отдают себе отчет в том, что бесплатный сыр бывает только в мышеловке, и справедливо полагают, что обеспечить необходимый уровень безопасности способны лишь полноценные коммерческие решения для защиты корпоративной сети.

Есть и случаи серьезного беспокойства! Как показало исследование, многие компании малого и среднего бизнеса обеспокоены вопросами угроз информационной безопасности. Так, 41% небольших предприятий России считает киберугрозы одним из своих главных бизнес-рисков. IT-специалисты отметили, что в настоящий момент уделяют максимум внимания в основном защите данных (42%) и обеспечению стабильной и бесперебойной работы IT-систем (30%). Почему же существует это противоречие? Дело в том, что тот, кто осознает опасность, и тот, кто принимает решения о повышении уровня защиты, — не один и тот же человек.

Сложившуюся ситуацию респонденты склонны объяснять, прежде всего, жесткими бюджетными ограничениями, установленными в компании (45%), непониманием со стороны руководства (45%) и отсутствием квалифицированных IT-специалистов (39%). При этом вопрос ограниченного бюджета стоит более остро для региональных небольших компаний (48%), чем для московских организаций (40%).

Традиционно наивность и простодушие являются нашей главной бедой. Ведь, несмотря на очевидные проблемы в системах защиты большинства небольших компаний в России, 56% респондентов полагают, что их корпоративные сети защищены достаточно хорошо. Проявлением излишней самоуверенности и фатализма можно считать и тот факт, что каждая четвертая компания малого и среднего бизнеса считает себя надежно застрахованной от киберугроз, утверждая, что вирусные инциденты чаще случаются с другими компаниями, нежели с

Достаточен ли уровень инвестиций в IT-безопасность?



ней самой. Более того, 30% российских СМБ-предприятий убеждены в том, что большинство проблем с безопасностью невозможно предсказать, а значит, нельзя предотвратить. Вот они, герои народного фольклора и наша главная цель!

Что угрожает малому бизнесу?

Однако наше исследование предлагает вашему вниманию не только данные по проблемам обеспечения безопасности, но и неумолимую статистику угроз. Так, за последний год 96% небольших компаний России хотя бы раз сталкивались с информационными угрозами, опережая по этому показателю коллег из США и Европы, где данный показатель не превышает 91%.

Чаще всего российские малые и средние предприятия страдают от спама (74%) и вредоносных программ (71%) — вирусов, червей и шпионского ПО. Такое положение вещей в равной степени характерно для московских и региональных предприятий. В США и Европе подобные типы угрозы распространены в значительно меньшей степени.

В России 40% подобных инцидентов закончились потерей корпоративных данных, чаще всего — финансовой информации. Для сравнения, в США и Европе этот показатель составляет лишь 23%. Таким образом, по эффективности защиты данных российские компании сегодня серьезно проигрывают. Радует хотя бы то, что СМБ-сектор следит за угрозами: 42% респондентов в России отмечают, что количество кибератак за последний год увеличилось.

Не будем забывать, что малые и средние предприятия являются наиболее многочисленным сегментом российского бизнеса. Поэтому незащищенность таких компаний означает уязвимость экономики в целом.

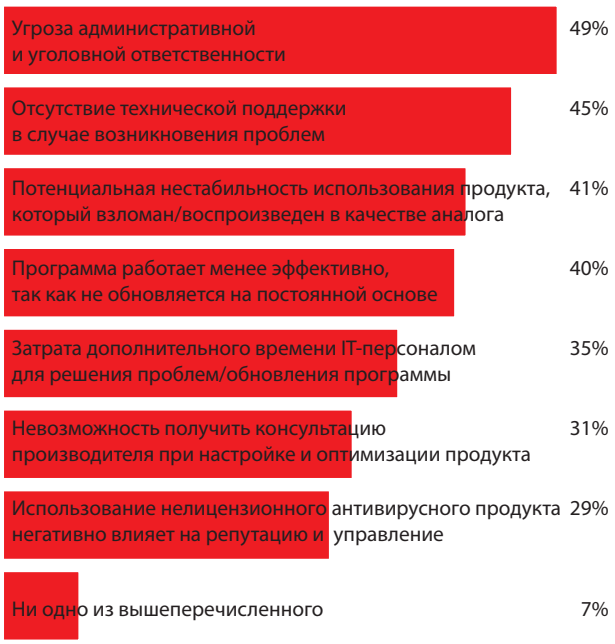
Мы не приводим данных по плачевным исходам реализованных рисков: все-таки мы общались с компаниями, которые, несмотря на свою легкомысленность, держатся на плаву. Но необходимо всегда помнить, чем грозит выведение из строя информационных систем предприятия: если малый бизнес не будет работать несколько дней, он вообще может прекратить свое существование.

Что мы можем дать малому бизнесу?

Даже в условиях ограниченных ресурсов простые меры, такие как обучение сотрудников и применение лучших практик, а также проактивный подход к обеспечению безопасности позволят значительно повысить степень защищенности представителей СМБ от кибератак. И наша задача — сообщить об этом потенциальным клиентам, поддержать их на пути к обеспечению безопасности IT-среды. Вооружившись знаниями, которыми мы поделились в данной статье, вы вполне можете приняться за освоение все еще слабо освоенного среднего и малого бизнеса в России. Ознакомиться с результатами исследования «Информационная безопасность малого и среднего бизнеса», а также со специальными возможностями для небольших организаций можно на сайте http://www.kaspersky.ru/business_products

Преимущества лицензионного защитного ПОс точки зрения российских малых и средних компаний

Недостатки нелицензионного защитного ПО с точки зрения российских малых и средних компаний



Как защитить информацию в небольших компаниях?

Объем корпоративной информации растет чуть ли не экспоненциально. С небольшим запаздыванием, но не менее стремительно растут суммы потерь организаций от утечек данных. За первую половину 2012 года зафиксированы факты утечек из таких компаний, как Microsoft, Yahoo!, IKEA, Samsung, Toshiba. В этом же списке нашлось место даже ФБР и Минобороны Великобритании.

Автор: Алексей Калгин, руководитель продуктового направления EgoSecure компании InfoWatch

Прямой ущерб исчисляется десятками миллионов долларов. А косвенный, связанный со снижением лояльности клиентов, расходами на ликвидацию последствий инцидентов в системах информационной безопасности, оценивается в пределах сотен и тысяч миллионов.

Так уж повелось, что журналисты во всем мире с завидной регулярностью «клюют» на громкие имена, создавая ложное впечатление, мол, утечки — проблема крупных компаний. Более глубокий анализ показывает, что небольшие организации также подвержены этой болезни. Значительное число утечек вызвано вовсе не злонамеренными действиями внешних хакеров или внутренних злоумышленников. Согласно исследованиям InfoWatch, примерно в половине случаев информация ушла из компании случайно, в связи с халатностью сотрудников: забытые документы на принтере, письмо, отправленное не по тому адресу и т.д.

Резонный вопрос: если целые отделы информационной безопасности в крупных компаниях не могут справиться с утечками данных, что делать малому бизнесу? Ведь там за безопасность отвечают не специально обученные сотрудники, а системные администраторы. Или сами руководители бизнеса, владельцы информации. О том, как при минимальных усилиях добиться максимальной защищенности, мы сегодня и поговорим.

Разнообразие систем защиты

Производители защитных систем давно сегментировали рынок. Для компаний побольше и побогаче предлагаются решения с развесистым функционалом, качественным сервисом, возможностью практически бесконечной кастомизации. Средним организациям подойдут решения «из коробки», с преднастроенными правилами — политиками безопасности. Вот только малому бизнесу ни первый, ни второй вариант, как правило, не подходит. Не по карману.

Казалось бы, достаточно «порезать» функционал «большого» корпоративного решения, и мы получим менее мощное, но более дешевое, как раз для малых компаний. Ан нет, не работает,

решение все равно остается сложным (в развертывании, в поддержке) и при этом умеет меньше, чем его старший брат.

Более перспективный путь — создание продукта для малого бизнеса «с нуля», с учетом ограниченных возможностей небольших компаний, под конкретные потребности пользователей — системных администраторов и руководителей. По большому счету, достаточно контролировать 20% наиболее очевидных каналов распространения информации, чтобы получить приемлемый уровень безопасности. Правило Парето — в действии!

О перечне достаточного функционала для защитной системы уровня малого бизнеса можно дискутировать бесконечно. Однако очевидно, что такая система должна:

1. **устанавливаться на конечное устройство — рабочую станцию или ноутбук пользователя;**
2. **иметь единую консоль управления;**
3. **интегрироваться со службами каталогов;**
4. **контролировать перемещение информации с рабочих станций на съемные носители (CD, флешки и пр.);**
5. **вести логи действий пользователей в системе.**

Программный комплекс InfoWatch EgoSecure Endpoint

Пример такого продукта — InfoWatch EgoSecure Endpoint. Концепция защиты, реализованная в EgoSecure, получила романтическое название C.A.F.E. За аббревиатурой скрываются термины контроль (Control), аудит (Audit), фильтрация (Filter) и шифрование (Encryption). Эти функции реализуются в одной системе, предоставляя администраторам все необходимое для гибкого управления защитой данных и проведения последующих расследований инцидентов.

На конечные устройства, стационарные и мобильные компьютеры, устанавливается специальный клиент, работающий на уровне ядра операционной системы. Согласно политикам безопасности, принятым в компании, он может блокировать установку и запуск определенных приложений, подключение внешних устройств и съемных носителей.

Программный комплекс устанавливается на физический или виртуальный сервер, интегрируется с Microsoft Active Directory и Novell eDirectory, позволяя администратору быстро и удобно задать политики доступа и правила использования данных для уже имеющихся групп пользователей. Режим обучения позволяет постепенно адаптировать настройки под стиль работы и потребности каждого отдельно взятого сотрудника.

Нетривиально реализована возможность шифрования информации. В отличие от других разработчиков, создатели InfoWatch EgoSecure Endpoint не стали изобретать велосипед и остановились на использовании стандартных средств шифрования операционной системы Windows. Шифрование данных при записи на мобильные носители происходит в фоновом режиме и абсолютно прозрачно для пользователя. От него не требуется никаких дополнительных действий, он привычным для себя образом сохраняет, копирует или открывает документы. Вся информация перед записью на внешние носители зашифровывается агентом InfoWatch EgoSecure Endpoint и хранится уже в зашифрованном виде.

Одним из самых интересных аспектов работы с EgoSecure Endpoint можно считать дополнительную консоль управления для iOS. Это значит, что администратор, используя свой iPad или iPhone, может в любое время выдать или отменить разрешения, а также отслеживать в реальном времени отчеты системы безопасности. Администратор может изменять права доступа в режиме online, подключаясь к центральному серверу через защищенный канал связи со своего мобильного устройства. Таким образом, вместе с EgoSecure время, затрачиваемое IT-специалистами на управление безопасностью, сокращается до нескольких прикосновений к экрану iPhone.

Работая с EgoSecure? не нужно запрещать внешние носители или ограничивать доступ к принтерам: данная система позволяет индивидуально настраивать разумные критерии разрешений и запретов, адаптируя средства защиты к стилю работы пользователя, а не наоборот. Вообще разработчики продукта уделили пользователю особое внимание. При необходимости получить разрешение на совершение запрещенной операции пользователь может сделать запрос непосредственно из интерфейса агента или совершить звонок IT-специалисту, если он находится в командировке, а выход в Интернет отсутствует. Для временного изменения политик безопасности необходимо ввести специальный код, который будет передан пользователю в случае одобрения запроса.

Что касается администратора, ему нужно лишь произвести начальную установку клиентов на все управляемые ПК и ноутбуки, а дальнейшие настройки будут происходить централизовано — с рабочего компьютера или через глобальную сеть с использованием мобильного устройства Apple.

Эффективность — это как?

Мы не зря в начале статьи затронули тему эффективности. Грамотные руководители выбирают системы безопасности, исходя не только и не столько из функциональных возможностей защитных продуктов. Главный критерий — соответствие полученного результата потраченным деньгам. Проще говоря, замок не должен стоить дороже сарая, двери которого он запирает. Собственно, этот подход — от затрат и преимуществ — укоренился в бизнес-среде давно и прочно. Но если затраты все участники процесса работы с информационными ресурсами воспринимают более-менее одинаково, то преимущества все видят по-разному.

Для пользователя эффективность напрямую связана с возможностями. Во многих случаях полный запрет на копирование данных ведет к потере в эффективности работы. Требуется соблюсти баланс между запретительными мерами и удобством.

Системный администратор рассматривает вопрос эффективности по-своему. Более эффективными с точки зрения управления и настройки будут те решения, которые требуют минимального количества действий для организации защиты и создания исключений. Так, использование единой консоли для управления всеми параметрами защиты — это повышение эффективности, а отсутствие возможности интеграции с другими информационными системами — ее потеря.

Эффективность для бизнеса — это отсутствие инцидентов и своевременная прозрачная отчетность. Руководитель компании платит за то, что система, во-первых, не мешает работать ни ему, ни его сотрудникам, и, во-вторых, справляется со своей задачей — действительно обеспечивает безопасность информации в рамках завяленных производителем возможностей.

Про необходимый набор защитного функционала мы уже сказали. Действительно, перегружать решение нужными лишь изредка функциями неправильно. Разумный баланс цены и качества появляется тогда, когда разработчик при создании продукта ставит во главу угла интересы пользователя. Так и получилось с InfoWatch EgoSecure Endpoint. Продукт ориентируется на сценарии работы администраторов, функционал и интерфейс подчинены одной идее — удобству применения. Именно снижение количества рутинных операций и оптимизация работы, как пользователя, так и администратора, позволяет назвать EgoSecure Endpoint действительно эффективным решением для защиты данных небольших и средних компаний.

Quest InTrust Управление журналом событий для безопасности и соблюдения требований

InTrust безопасно собирает, сохраняет, составляет отчеты и уведомляет о событиях в системах Windows, Unix и Linux, помогая обеспечивать соответствие внешним требованиям, правилам внутренней политики и безопасности.

InTrust помогает обеспечить соблюдение нормативных требований посредством аудита пользовательского доступа к критически важным системам, а также путем обнаружения подозрительных событий, связанных с доступом. С помощью этого инструмента можно собирать, анализировать, составлять отчеты и генерировать автоматизированные оповещения в реальном времени для всех соответствующих событий, связанных с доступом, в пределах вашей неоднородной сети.

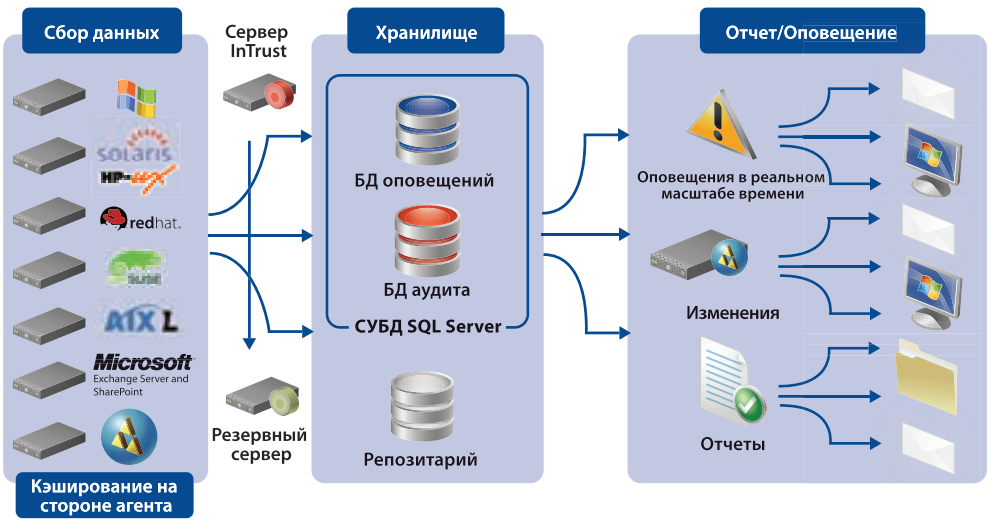
С помощью этого единого решения для контроля доступа к критически важным системам на различных платформах упрощайте управление журналом событий, экономьте средства на управление хранением, улучшайте информационную безопасность, минимизируйте риски, снижайте затраты и повышайте эффективность безопасности, оперативной отчетности и отчетности о соблюдении нормативных требований.

Возможности решения

- Ключ к соблюдению нормативных требований: решает вопрос соблюдения нормативных требований путем сбора отчетности по журналам всего пакета IT, контроля доступа к важным системам и приложениям, выполняя экспертный анализ пользователей и активности системы, основанный на данных, содержащих историю событий.
- Отслеживание активности пользователей: собирает события о деятельности пользователей и администраторов различных расширенных систем и приложений, представляет их в удобной и полной форме для составления текущей отчетности и анализа. Извлекает важные детали доступа пользователей, например, кто выполнил действие, его последствие, сервер и рабочую станцию события.
- Автоматизированный сбор журналов: автоматизирует надежный сбор журналов событий, уменьшая рабочую нагрузку.
- Сжатие данных журналов: обеспечивает долгосрочное сжатие в отличие от хранения того же объема данных событий в базе данных.
- Защищенность журнала: позволяет создавать на каждом удаленном сервере кэшированное место, где можно дублировать журналы по мере их создания, не позволяя тем самым неавторизированным пользователям и администраторам менять данные в журнале проверки безопасности.
- Экспертный анализ: предоставляет инструменты интерактивного поиска по хронологии событий журнала для оперативного расследования проблем и нарушений, связанных с безопасностью, для подготовки судебного иска.
- Оповещение в режиме реального времени: отправляет в режиме реального времени уведомления о несанкционированной или подозрительной активности пользователей на ваш электронный адрес или на приложения мониторинга третьей стороны, например, Microsoft Operations Manager (MOM).
- Гибкая отчетность: дает вам уникальный доступ к заранее определенным и настраиваемым отчетам с поддержкой большого числа файловых форматов, включая HTML, XML, PDF, CSV и TXT, а также Microsoft Word, Visio и Excel.
- Устойчивость к сбоям: автоматически резервирует сервер при сбое, позволяя быстро перемещать все конфигурации и работы с вышедшего из строя сервера на резервный для обработки всех видов деятельности и сокращения потери файлов из-за сбоев.

Преимущества InTrust

- Снижение затрат за счет автоматизации работ по сбору и сжатию информации о событиях во всех подконтрольных гетерогенных средах.
- Строгое соблюдение нормативов и политик защиты информации.
- Обеспечение полной достоверности журналов аудита за счет кэширования на стороне агентского модуля.
- Повышение уровня внутренней безопасности за счет идентификации пользовательских учетных записей, которые использовались в ходе нарушений корпоративной политики.
- Отслеживание и превентивное оповещение в реальном времени о любой активности в любом почтовом ящике Exchange.
- Оповещения в реальном времени и мгновенная реакция на важнейшие события или изменения в каталоге AD и объектах групповых политик GPO.



Quest ChangeAuditor

Аудит изменений в режиме реального времени инфраструктуры Windows

Интеллектуальный подробный анализ для аудиторов и руководителей. Снижает риски, связанные с повседневными изменениями.

Регистрация событий и отчеты об изменениях для корпоративных приложений и услуг — трудоемкие и долговременные задачи, которые иногда невозможно выполнить с помощью внутренних средств аудита. К счастью, существует ChangeAuditor от компании Quest Software. Это семейство решений проверяет, предупреждает и сообщает обо всех изменениях и удалениях, внесенных в Active Directory, Exchange, SharePoint, VMware, EMC, NetApp, SQL Server, файловые серверы Windows, запросы LDAP AD в режиме реального времени и без собственного аудита. Центральная консоль устраняет необходимость и сложность использования множественных решений IT-аудита.

Положитесь на решение ChangeAuditor, которое поможет вам:

- выполнить задачу аудита по соблюдению нормативных требований с помощью встроенных отчетов SOX, PCI DSS, HIPAA, FISMA, SAS 70 и др.;
- упростить IT-управление для предотвращения нарушений правил внутренней и внешней безопасности;
- повысить производительность предприятия с ПО для управления изменениями, которое контролирует и анализирует работу до и после внесения изменений.

О рисках — более детально

В качестве примера того, какие риски несет в себе отсутствие детального аудита действий пользователей и администраторов, касающихся Active Directory, можно привести следующие ситуации:

1. Произведены некорректные или злоумышленные изменения в Active Directory, имевшие негативные последствия для всей системы. Информация в стандартном журнале событий отсутствует (перезатерта более новыми записями), либо недостаточна (штатные средства) для того, чтобы установить причину и источник вредоносных изменений.
2. Ошибочное или злоумышленное изменение некоторых параметров Active Directory может вызывать остановку работы ключевых бизнес-приложений на долгий срок. Поэтому имеет смысл запретить выполнение некоторых действий даже администраторам без предварительного согласования с третьими лицами.
3. Невозможно пройти внутренний или внешний аудит безопасности ввиду отсутствия необходимой и достаточной информации.

Потенциальное решение

Решение компании Quest Software ChangeAuditor for Active Directory позволяет вести полный детальный аудит действий пользователей и тем самым уменьшить риски, связанные с повседневными изменениями в Active Directory.

Quest ChangeAuditor for Active Directory отслеживает и предупреждает о существенных изменениях в конфигурации Active Directory в режиме реального времени. Таким образом, вы всегда будете знать, кто, где, когда, откуда и какие изменения осуществил — все в простой и понятной форме. Продукт показывает предыдущие и текущие значения свойств измененных объектов. В любой момент времени вы сможете быстро создать и предоставить детальные экспертные отчеты для аудиторов, администрации, проведения внутренних расследований и т.д.

ChangeAuditor for Active Directory также обеспечивает дополнительную защиту от нежелательных и несанкционированных изменений наиболее критичных объектов Active Directory без их предварительного согласования и одобрения авторизованными лицами, включая изменение параметров групповых политик — даже при наличии у конечного пользователя или администратора достаточных прав такие изменения произвести.

Контакты

Мы с радостью ответим на любые вопросы о продуктах Quest.

Пишите: quest@softline.ru

Наш сайт: http://quest.softline.ru

QUEST SOFTWARE® ELITE PARTNER

Комплексная антивирусная защита ОС, ПО и данных ПК

Продукт, к началу 2012 г. удерживающий второе место в России по числу пользователей комплексных антивирусов.

Защита от всех видов Интернет-угроз, сертифицированная в 2010-2012 гг.: в 10 тестах — журналом Virus Bulletin за обнаружение вредоносного кода без ложных срабатываний; в 5 тестах подряд — порталом Anti-Malware.ru за быстродействие, надежный фаервол, проактивную и самозащиту; в 5 тестах — порталом Matousec.com, рекомендовавшим Outpost за противодействие новым и неизвестным угрозам как для 32-битных, так и для 64-битных Windows XP/Vista/7.

Outpost Security Suite Pro (v 7.5) — Performance Edition

- «Антивирус + Антишпион» с 5-кратным ускорением повторных проверок SmartScan.
- Двусторонний брандмауэр для защиты от вторжений по сети и утечки данных.
- Проактивная защита для превентивной блокировки новых угроз.
- Новинка! Технология цветовых подсказок SmartDecision — помощь пользователям в вопросах безопасности.
- Web-контроль с оптимизированным контент-фильтром.
- Защита системы и приложений от изменения вредоносным кодом.
- Новинка! Защита автозагрузки USB-устройств от вирусов.
- Мониторинг приложений для отслеживания активности файлов и реестра
- Режим развлечений (игры, видео) и Автообучение 2.0 (для новичков).

Комплексную безопасность дополняют: обучаемый спам-фильтр; самозащита от злонамеренного отключения Outpost; автоматическая настройка безопасности сети (включая Ethernet, Wi-Fi, Wi-Max, xDSL, сотовые и dial-up соединения); облачная система ImproveNet, поставляющая автоматические настройки безопасности и новые правила принятия решений для брандмауэра и проактивной защиты.

Быстрый и эффективный Антивирус + Антишпион

Резидентный монитор доступа постоянно производит поиск и обезвреживание вредоносных объектов, обнаруженных в системном реестре, а также в почте и на web-страницах.

Сканер в версии 7.5 (Performance Edition) с технологией SmartScan4 проверяет только модифицированные части системы без проведения повторной проверки файлов, не менявшихся с момента последнего сканирования. В результате антивирус работает до 3-5 раз быстрее предыдущих версий.

Модуль «Проактивная защита»

Блокирует все изощренные виды взлома, направленные на кражу данных, и защищает от несанкционированной рассылки спама и вирусов от вашего имени вашим адресатам.

Фильтрация почтовых вложений

В режиме реального времени перехватывает подозрительные вложения при отправке и получении почты. Любой подозрительный файл можно поместить в карантин для последующей обработки.

Интерактивное содержимое

Блокирует установку и активацию нежелательного и вредоносного кода через браузер.

Защита от кражи данных

Модули «Защита системы» и «Защита приложений» избавляют вас от опасности утечки личных данных.

Outpost Network Security (ONS) 3.2.

Централизованная защита рабочих ПК

При помощи централизованно управляемого комплекса антивирусной и сетевой безопасности вы можете сделать компьютеры своей сети неуязвимыми для внешних и внутрисетевых атак.

Основные возможности

- Круговая защита от вирусов, шпионских модулей и других вредоносных программ.
- Сетевой экран с двунаправленной фильтрацией и защитой интрасети.
- Ограничение доступа к ненадежным элементам web-страниц.
- Защита ключевых компонентов от несанкционированного отключения.
- Централизованная установка и администрирование.
- Централизованный запуск антивирусной проверки.
- Протоколирование событий в реальном времени и ведение журнала операций.
- Централизованное ограничение доступа к USB-устройствам хранения.
- Централизованное ограничение доступа к ненадежным URL-адресам.

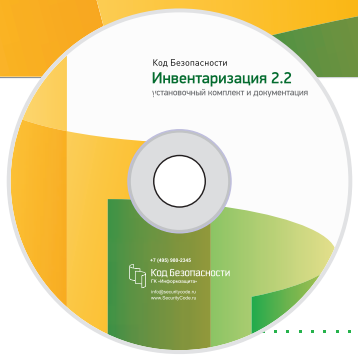
ONS позволяет защитить вашу организацию от всех видов вредоносного ПО, кражи данных, а также лимитировать и обезопасить доступ в сеть. Проверка удаленных машин «на лету» осуществляется автоматически в фоновом режиме, в то время как файловый сканер, оснащенный технологией SmartScan3, позволяет быстро и эффективно проверить все подверженные заражению области.

Клиентский агент Outpost Network Security 3.2 — комплексный антивирус Outpost Security Suite Pro, дающий администратору следующие возможности управления:

- неограниченное число консолей. Лицензируется только число защищаемых клиентских ПК. Консоль может устанавливаться независимо от наличия агента на любое количество ПК;
- централизованные политики. Защита осуществляется под управлением системного администратора организации согласно групповым политикам;
- удаленный просмотр клиента. На клиентский агент можно залогиниться из консоли и осуществлять управление им в графическом интерфейсе в режиме реального времени;
- тонкая настройка безопасности. Правила для приложений на агенте можно настроить под нужды конкретного пользователя.

agnitum

Код Безопасности
ГК «Информзащита»



Код Безопасности: Инвентаризация 2.2

Программный комплекс, предназначенный для сбора, обработки и систематизации информации о программном и аппаратном обеспечении компании.

- Политики управления ПО и оборудованием
- Приведение в соответствии со стандартами
- Отслеживание изменений
- Оптимизация закупок лицензий и оборудования
- Отчеты для специалистов ИТ и ИБ
- И не только…

itexpert ВЫБОР ЭКСПЕРТА 2011 продукт года

Компания « Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Gatewall Mail Security

GateWall Mail Security — это решение для защиты корпоративной почты от вирусов, фишинга, спама и прочих вредоносных сообщений, позволяющее также предотвращать утечки конфиденциальной информации. Продукт обеспечивает архивацию сообщений, предоставляет возможность мониторинга почты, поддерживает синхронизацию по IMAP с MS Exchange 2003 и Lotus Domino, а также может работать с любыми другими почтовыми серверами.

GateWall Mail Security оснащен модулем защиты от потери данных (DLP — Data Loss Prevention), предотвращающим утечки конфиденциальной или другой нежелательной информации, а также проникновение ее извне.

В зависимости от настроек система позволяет блокировать, задерживать сообщения, или оповещать инженера безопасности об отсылке подозрительного письма. Защита позволяет определять все зашифрованные сообщения и определять, какие действия должны к ним применяться.

GateWall Mail Security поддерживает следующие методы фильтрации спама:

- на основе DNS (DNSBL, RHSBL, Backscatter, MX, SPF, SURBL);
- на основе распределенной антиспамси стемы (облачный антиспам);
- на основе статистики (собственная реализация фильтрации Байеса).

Одним из важных достоинств облачного антиспама является крайне низкий уровень ложного срабатывания — менее 1 на 1,5 млн сообщений. При этом уровень детекции спама составляет более 97%.

Кроме этого, GateWall Mail Security поддерживает контроль SMTPп.ротокола (контроль правильности команд в соответствии с RFC), ограничивает максимальный размер письма, максимальное количество получателей и т.п.

В продукт интегрированы 3 антивирусных модуля: облачный антивирус Commtouch Zero.Hour, антивирус Касперского и Panda Antivirus. Модули предназначены для проверки SMTP.трафика.

В GateWall Mail Security реализована интеграция с IMAP.сервером MS Exchange или Lotus Domino. Интеграция предоставляет возможность создания общей папки IMAP на удаленном почтовом сервере и обработку сообщений в этих папках.

Защита от утечек персональных данных и иной конфиденциальной информации

В GateWall Mail Security используется 3 типа фильтрации:

- «Регулярные выражения» (Regexp);
- «Сравнение документов» (Docmatch);
- «Лемматизатор» (Lemmatizer).

Каждый из них посредством разных способов поиска информации в теле, теме, вложениях и других частях письма исследует почтовые сообщения на наличие в них определенных ключевых слов или фраз и проводит сравнение передаваемых данных с образцами конфиденциальной информации.

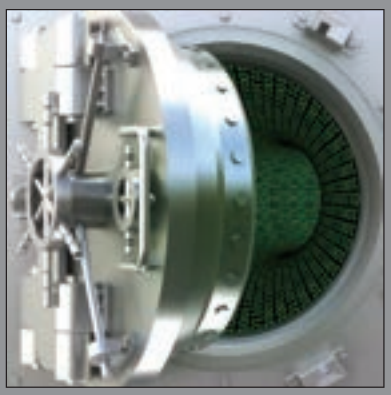
GateWall Mail Security предоставляет информацию обо всех сообщениях, обработанных сервером. Мониторинг сообщений позволяет выполнять фильтрацию по дате, по статусу обработки (доставлено/заблокировано), по адресу источника или назначения, выполнять принудительную отправку сообщений, заблокированных как спам, а также создавать списки исключений.

BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

ЕЖЕКВАРТАЛЬНЫЙ ОТРАСЛЕВОЙ ЖУРНАЛ

Первый и единственный специализированный журнал
по информационной безопасности банков
и кредитно-финансовых организаций



Содержит актуальную и достоверную информацию по различным аспектам отрасли:

- источники угроз и способы защиты информации;
- обзор изменений и нововведений в законодательстве, а также практика его применения;
- новости отрасли и новшества в образовании;
- динамика развития рынка предложений интеграторов;
- освещение деловых специализированных мероприятий.

Ознакомьтесь с журналом и оформите подписку на сайте:

www.ib-bank.ru/bis

Издатель: ООО «Авангард Центр».
101000, г. Москва, Колпачный пер., д. 6, стр. 4.
Тел./факс: +7 (495) 927-02-47.
По всем вопросам обращайтесь по адресу: bis@ib-bank.ru.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство ПИ № ФС77-41563 от 13 августа 2010 г.

DeviceLock 7 DLP Suite

Самым действенным способом укрепления дисциплины сотрудников и элементом обеспечения безопасности данных на корпоративных компьютерах в современных условиях является применение специализированных средств предотвращения утечек данных (Data Leak Prevention). Такие DLPр.ешения должны устранять «человеческий фактор» и пресекать нарушения дисциплины, блокируя утечки данных с компьютера для максимально возможного числа их сценариев.

DLP.система должна фиксировать и сохранять все факты и детали нарушений, обеспечивая возможность расследования, выявления нарушителей и привлечения их к ответственности. Эффективное DLP.решение должно контролировать не только сетевые коммуникации, но и локальные каналы ввода.вывода данных, включая копирование на съемные устройства памяти, печать документов, копирование данных через системный буфер обмена, а также синхронизацию со смартфонами — те потенциальные каналы утечки, которые в принципе невозможно защитить сетецентрическими DLP.решениями.

В 2011 г. компания «Смарт Лайн Инк» (www.smartline.ru) представила рынку новую версию своего продукта — DeviceLock 7 Endpoint DLP Suite1, включающую в себя два новых модуля — NetworkLock и ContentLock. Благодаря новым компонентам комплекс DeviceLock не только предотвращает утечки через порты и устройства, подключаемые к рабочим компьютерам, но и контролирует различные сетевые коммуникации и, что особенно важно, использует технологии контентной фильтрации передаваемых во всех контролируемых каналах данных (как через периферийные порты и устройства, так и через сетевые коммуникации). Комплекс DeviceLock 7 является полноценной DLP.системой, причем первой такой системой отечественной разработки.

NetworkLock: контроль сетевых коммуникаций на рабочем месте

Модуль NetworkLock позволяет контролировать и протоколировать использование на рабочих станциях сетевых протоколов и коммуникационных приложений независимо от используемых ими портов, обеспечивая контроль сообщений и сессий с выделением передаваемых данных и файлов для их оперативного анализа, событийное протоколирование и теневое копирование данных. В числе контролируемых NetworkLock сетевых коммуникаций, приложений и сервисов как повседневно необходимые каналы передачи сообщений по открытым и SSL.защищенным SMTP.сессиям или MAPI/Exchange (с раздельным контролем сообщений и вложений), web.доступ по протоколам HTTP/HTTPS, файловый обмен по протоколам FTP/SFTP, так и наиболее популярные сетевые приложения и сервисы: web.почта, службы мгновенных сообщений, социальные сети, а также Telnet.сессии.

Все каналы контролируются независимо от способа выхода сотрудника в Интернет — как через корпоративные шлюзы, так и через любые другие каналы подключения. Другая немаловажная особенность — способность NetworkLock задавать гибкие политики контроля различных каналов, применимых к конкретным пользователям и группам в зависимости от разных условий, таких как направление передачи, используемые сетевые порты и адреса, временные диапазоны и т.п.

Как и для контроля USB.устройств в DeviceLock, в модуле NetworkLock реализован «белый список» сетевых протоколов, позволяющий гибко предоставлять доступ ключевым сотрудникам только к тем сервисам и узлам, которые необходимы для выполнения их бизнес.задач. Например, можно запретить всем пользователям доступ к протоколам SMTP и Web Mail, а затем использовать «белый список», чтобы разрешить определенным пользователям отправлять электронную почту на указанные адреса. Применение таких гибких DLP.политик снижает риск утечки и кражи данных.

ContentLock: контентная фильтрация данных

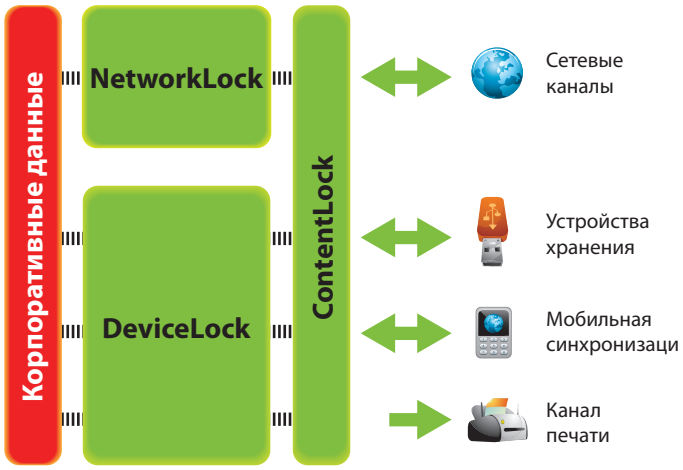
Модуль ContentLock, выполняющий функцию контентного анализа передаваемых файлов и данных, позволяет разрешать или запрещать доступ к информации, основываясь на целом ряде параметров и условий: на определении типа файла, шаблонах регулярных выражений с различными численными и логическими условиями соответствия проверяемых данных критериям и ключевым словам. Распознавая более 80 форматов файлов и типов данных, ContentLock извлекает и отфильтровывает их текстовое содержимое при копировании на внешние устройства хранения или передаче по сетевым каналам. Кроме того, ContentLock позволяет задать правила фильтрации для данных теневого копирования, что дает возможность сохранять только те файлы и данные, которые действительно значимы для расследования инцидентов информационной безопасности и анализа журналов теневого копирования. Это на порядки снижает объем данных, хранимых в базе данных теневого копирования, и существенно снижает нагрузку на сеть, вызванную передачей этих данных на сервер с БД теневого копирования.

Исключительная гибкость и эффективность DLPпо литик DeviceLock достигается за счет возможности их формирования для любых комбинаций отдельных пользователей и их групп, а также типов портов, устройств и сетевых протоколов.

Кроме того, ContentLock контролирует архивированные файлы, последовательно осуществляя проверку каждого файла, содержащегося в архиве, причем вложенные архивы также распаковываются и проверяются один за другим. Встроенная в ContentLock технология детектирования текста на изображении позволяет выделять две группы графических изображений: изображения, содержащие текст, например, отсканированные документы или экранные снимки документов, и изображения без текста, и устанавливать для них разные политики контроля. Кроме того, ContentLock обеспечивает анализ изображений, встроенных в документы Microsoft Office, а также файлы Adobe PDF и RTF.

DeviceLock Endpoint DLP Suite: интеллектуальная защита от утечек

Сочетание функционала новых компонентов NetworkLock и ContentLock дает ИБ.службам как весь необходимый инструментарий для аудита и анализа активности пользователей в Сети, так и средства для контроля передачи конфиденциальной информации в различных каналах сетевых коммуникаций. Комбинирование и сочетание правил контроля и аудита, задаваемых в DeviceLock DLP Suite, позволит оградить рассеянных и забывчивых сотрудников от несанкционированных утечек данных со сменных носителей, случайной отправки в сеть ценной корпоративной информации, при этом блокируя сознательные нарушения со стороны злонамеренных работников.



Ваши заказчики полагаются на вас.

А на кого полагаетесь вы?

Киберпреступники не останавливаются ни перед чем, когда речь идет о краже данных и взломе сайтов. Вот почему решения Symantec Website Security предлагают гораздо больше, чем просто SSL-сертификаты, а именно: ведущие отраслевые технологии шифрования SSL, проверку сайтов на вредоносное ПО, маркировку сайтов в поисковых выдачах значком Seal-in-Search™, оценку уязвимостей и сертификаты высокой надежности (EV). Вы можете положиться на Symantec, если хотите защитить свой сайт и своих заказчиков. **Узнайте, как мы можем помочь вам взять свой сайт под контроль прежде, чем это сделает кто-то другой.**

Norton™ SECURED
powered by VeriSign

Symantec™

Softline запустила виртуальную тестовую лабораторию symdemolab.softline.ru

Компания Softline расширяет спектр услуг по направлению информационной безопасности и объявляет об открытии виртуальной тестовой лаборатории symdemolab.softline.ru, которая даст возможность заказчикам из любой точки мира в режиме онлайн знакомиться с полнофункциональными версиями решений Symantec.

Демонстрационный стенд SymDemoLab работает на базе новейших технологий виртуализации VMware и Citrix, которые позволяют объединить множество решений Symantec в рамках единой платформы, предоставив при этом доступ к сервису всем желающим.

В настоящий момент в виртуальной лаборатории представлены наиболее популярные среди заказчиков решения:

Symantec Endpoint Protection 12.1 — для защиты рабочих станций и серверов,
Symantec Data Loss Prevention 11.1 — для защиты от утечек данных,
Symantec AItiris IT Management Suite 7.1 — для управления ИТ-инфраструктурой,
Symantec NetBackup — для резервного копирования (для крупных компаний с гетерогенной IT-инфраструктурой),
Symantec Backup Exec 2010 — для резервного копирования (для компаний с Windows/ VMware ориентированной средой).

Помимо возможности самостоятельного удалённого тестирования продуктов пользователи могут оформить заказ на услуги:

- организации веб-демонстрации с участием сертифицированного технического специалиста Softline,
- обучения работе с представленными продуктами, в т. ч. в рамках мастер-классов;
- индивидуального моделирования конфигураций заказчиков.

Для того чтобы воспользоваться новым сервисом, необходимо оставить заявку на сайте **http://symdemolab.softline.ru**.

О корпорации Symantec

Корпорация Symantec — один из мировых лидеров в области решений для обеспечения безопасности, хранения данных и управления системами, которые помогают предприятиям и индивидуальным пользователям всего мира защищать свою информацию и управлять ею.
www.symantec.ru

«Открытие виртуальной тестовой лаборатории — это еще один способ общения с нашими заказчиками. Благодаря SymDemoLab клиенты получат самую свежую информацию о продуктах, смогут протестировать их в действии, оценить качество, удобство и соответствие возложенным на решения задачам, а также оставить отзывы о ПО, которые будут непременно переданы вендору и учтены при выпуске следующих версий продуктов».

Дмитрий Васильев,
руководитель направления Symantec компании Softline

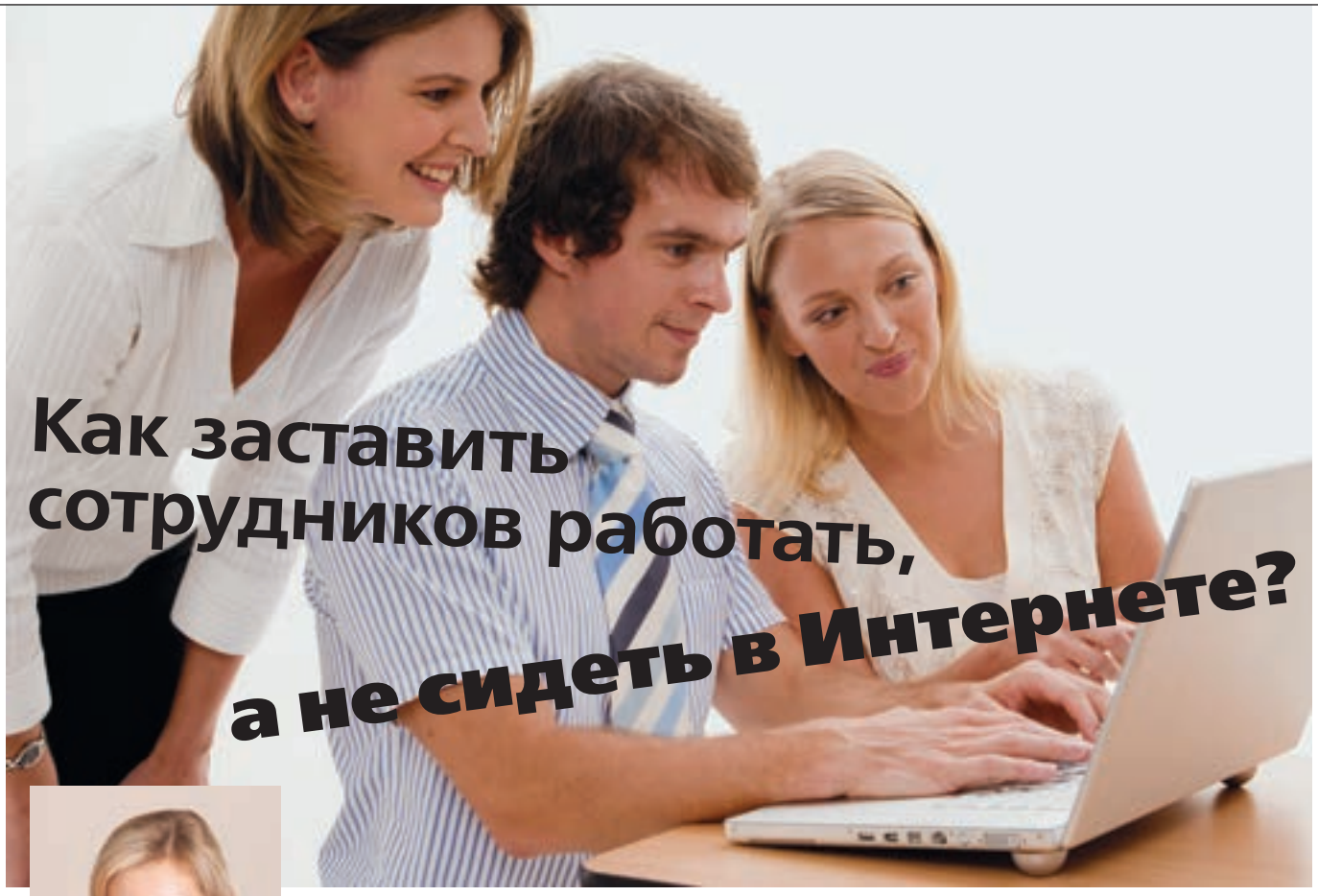
«Виртуальные демонстрации — это необычайно удобный инструмент для демонстрации наших программных решений. Благодаря возможности виртуального тестирования наши клиенты смогут минимизировать свои риски и получить полное представление о работе системы еще до начала пилотного проекта».

Олег Шабуров,
руководитель группы информационной безопасности Symantec в России и СНГ

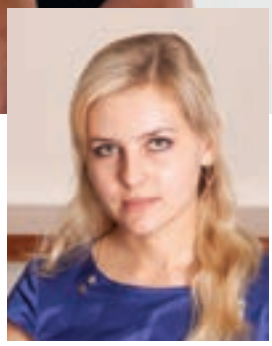
Передовая защита сред VMware®

Безопасность. Резервное копирование.

Symantec™



Как заставить сотрудников работать, а не сидеть в Интернете?



Практически каждая компания страдает от чрезмерного использования своими сотрудниками интернет-ресурсов в личных целях. И, казалось бы, думает пользователь, посмотреть ролик на Youtube или скачать фильм или архив с фотографиями — это же так незначительно для компании! На самом деле, с точки зрения организации возникают три проблемы, которые она должна в этой связи решить.

Автор: Виктория Носова, консультант по безопасности,
компания Check Point Software Technologies (Russia)

Работать, а не тратить время

Первая проблема заключается в том, что сотрудники в рабочее время занимаются своими личными делами, а не обязанностями, выполнение которых им, собственно, и оплачивается. Видеоресурсы, социальные сети, flash-игры отлично помогают недобросовестным сотрудникам «отработать» свой рабочий день. Поэтому компания должна иметь возможность контролировать доступ пользователей к интернет-ресурсам такого рода.

Необходимо иметь решение, которое позволяет создавать гранулируемую политику доступа к сайтам и интернет-приложениям. Естественно, что политики доступа должны применяться к группам пользователей, а не IP-адресам их компьютеров. Иначе отчеты и журналы регистрации событий будут малоинформативными, так как в них сложно будет сопоставить IP-адрес компьютера и пользователя, который обращался к определенному сайту. Дополнительно вы можете определить несколько групп пользователей, которым все же будет разрешен доступ к некоторым нежелательным ресурсам, например, социальным сетям, а остальным пользователям в компании он будет запрещен.

Формирование отчетов об использовании сотрудниками тех или иных web-ресурсов позволит руководству понять, кто работает, а кто создает иллюзию работы. В любом случае, на руках появится основание для вынесения предупреждения или другого наказания. Кроме того, подобные отчеты помогут понять, какие сайты используются в организации и насколько активно.

Также очень эффективным инструментом для снижения использования Интернета в личных целях на работе является механизм, позволяющий оповещать пользователя о том, что доступ к определенным сайтам/приложениям запрещен или нежелателен. Видя сообщение такого рода, пользователь понимает, что его контролируют. Впредь сотрудник будет думать прежде, чем смотреть видеоролики или запускать скачивание torrent-файла.

Упомянем еще один важный момент, который необходимо учесть при запрете какого-либо ресурса. Естественно, не все сайты имеют сугубо развлекательный характер, например, тот же Youtube может использоваться для просмотра обучающих материалов, необходимых для работы. Поэтому хорошо, если для некоторых ресурсов система защиты будет иметь возможность запросить у пользователя цель использования и записать выбор в журнал регистрации событий.

Конечно, пользователи могут быть осведомлены о наличие web-сайтов или программ-прокси, так называемых анонимайзеров, которые часто помогают обмануть защиту многих организаций. Важно, чтобы выбранная система защиты осуществляла разбор трафика в рамках HTPP-протокола и имела широкую базу данных интернет-приложений.

Бесплатный «кинотеатр»? Только не здесь!

Вторая проблема заключается в том, что просмотр видео в Интернете и скачивание torrent-файлов увеличивают загрузку интернет-канала всей организации.

Очень частая «головная боль» компаний — это torrent-клиенты. Данные программы при скачивании torrent-файлов используют максимальную пропускную способность канала. И так как пользователи обычно не особо заботятся о том, чтобы уменьшить в настройках параметры «Скорость загрузки» и «Скорость отдачи», в итоге получается, что канал загружен практически на 100%.

Таких сотрудников достаточно много, особенно среди тех, кто использует в качестве корпоративных ПК ноутбуки. Чаще всего, поставив дома фильм на закачку, на работе пользователь может просто забыть об этом или сознательно не остановить процесс, исходя из того, что Интернет в компании очень быстрый, значит и фильмы загрузятся быстрее.

Но из-за этого остальным коллегам будет уже достаточно проблематично получить доступ в Интернет по рабочим вопросам, не смогут полноценно работать с серверами приложений удаленные сотрудники или партнеры, и другие критичные ресурсы компании будут недоступны для внешних пользователей. Также нужно учитывать, что многие torrent-клиенты могут работать в зашифрованном режиме. Поэтому внедряемая система защиты должна уметь блокировать трафик от таких клиентов во всех режимах их работы — иначе эффекта не будет.

Если работу таких приложений, как torrent-клиенты и анонимайзеры, рекомендуется блокировать, то для использования некоторых сайтов, к примеру, Youtube, было бы неплохо настроить ограничения полосы пропускания. В этом случае, даже если пользователь получил доступ к Youtube, при ограничении полосы пропускания для данного приложения до 64 Кбит/с удовольствие от просмотра вряд ли удастся получить. Очень удобно создать ограничивающее правило для всех или только для самых активных пользователей таких ресурсов.

Было бы неплохо также выдавать уведомление о том, что сотруднику разрешено использование данного Интернет-ресурса только с указанной скоростью. Таким образом, пользователь будет понимать, что его контролируют, и что уже нет нужды звонить администратору сети и жаловаться на «медленный Интернет».

И никаких утечек!

Третья проблема заключается в том, что чем больше интернет-ресурсов разрешено, тем больше брешей в системе безопасности организации. Сотрудник получает больше возможностей передать конфиденциальную информацию посторонним людям и конкурентам. Это возможно сделать и посредством клиентов системы быстрого обмена сообщений таких, как Skype, ICQ, Gtalk и т.п, ресурсов web-почты, например, Yandex, Mail.ru, Gmail и т.п. и с помощью файлообменников таких, как Rapidshare, deposite.ru и т.д.

Помимо контроля протокола SMTP почтовой системы компании система защиты должна также контролировать и web-трафик. Необходимо отметить, что кроме протокола HTTP должен проверяться и HTTPS, так как все больше сайтов переходит на использование SSL-шифрования.

Приведу пример. Сотрудник не успел доделать отчет и решил поработать дома. Поэтому он пытается отправить отчет с конфиденциальными данными себе на web-почту на gmail.com или выкладывает на файлообменник deposite.ru. И, к сожалению, он не догадался поместить отчет в архив и установить пароль. Получается, конфиденциальный документ размещен на ресурсе сторонней компании. Есть еще более неприятный вариант: сотрудник может отправить или выложить конфиденциальный документ для сторонней организации.

Итого, система защиты должна позволять компании минимизировать вероятность утечки конфиденциальных данных. Но при этом она все же не должна мешать работе сотрудников. Как правило, после внедрения большинства DLP-систем, пользователи испытывают трудности с отправкой каких-либо документов потому, что системе просто указывают конфиденциальные документы, которые нельзя отправлять, и несколько исключений; если же пользователь попытается абсолютно легально отправить документ партнеру компании, но данный файл попадает под шаблон блокируемых документов, приходится обращаться к администратору и долгое время разбираться, есть ли право на отправку. Такие системы защиты — головная боль для системных администраторов.

Поэтому лучше использовать систему, позволяющую запрашивать пользователя о цели пересылки определенных типов документов или данных. Обоснование сотрудника можно использовать для дальнейшего разбора ситуации.

Естественно, пользователь, увидев запрос такого рода, лишний раз подумает о том, действительно ли стоит отправлять документ, и осознает свою ответственность за отправку конфиденциальных данных.

Данный механизм — отличное средство для информирования сотрудников о том, что в компании внедрения система контроля документооборота.

И следует также не забывать о решениях, позволяющих контролировать использование портов на компьютерах. Они разработаны не просто так: даже если в компании внедрена новейшая система контроля web-трафика и использования интернет-приложений, контроль будет осуществляться, только если трафик проходит через шлюз безопасности, на котором активирована данная система защиты.

Поэтому для того, чтобы обойти систему защиты, сотрудник может использовать USB-модем, например, производства компании Yota, сотовых операторов или др., создав альтернативный интернет-канал. Такой маневр позволяет использовать все web-приложения без каких-либо ограничений или запретов и отправлять конфиденциальные файлы без фиксации в журналах регистрации записей.

Система защиты от Check Point

Отличным вариантом решения, покрывающего все вышеуказанные проблемы, является система защиты от Check Point, включающая в себя набор Программных блейдов для контроля доступа к Интернет-ресурсам (Application Control), для предотвращения от непредумышленных утечек данных (DLP) и для учета групп пользователей в политике безопасности (Identity Awareness). Данная система защиты отлично справляется со своими задачами контроля почтового трафика, имеет механизм уведомления и опроса пользователя об использовании того или иного сайта или отправки определенного документа. Благодаря собственной системе корреляции событий система позволяет создавать 3D-отчеты о событиях безопасности, связанных с контролем web-трафика и документооборота. Данные отчеты помогают собрать статистику о самых используемых ресурсах, о самых активных пользователях, о документах, которые были отправлены. Также отчеты такого рода являются достаточным документом для руководства для понимания масштабов использования ресурсов компании и для обоснования необходимости данной системы защиты, как таковой.

В арсенале продуктов компании Check Point имеется решение для контроля использования портов на рабочей станции (Media Encryption), применение которого позволяет предотвратить создание альтернативного интернет-канала на ноутбуке или ПК.

Приобретая продукты компании CheckPoint, ваша компания присоединяется к числу организаций, которые уже решили все вышеперечисленные проблемы.

Безопасность «облаков» — миф или реальность?

В том, что будущее — за удобными, рентабельными и эффективными облачными технологиями, сегодня уже мало кто сомневается. Однако вопрос, насколько безопасно переносить бесценные данные и критичные для бизнеса приложения в «облака», беспокоит очень многих. О безопасности облачных решений в этом интервью рассказывает Денис Безкоровайный, вице-президент RISSPA, Ассоциации профессионалов в области информационной безопасности (Russian Information Systems Security Professional Association).

Многообразие «облаков» и их защита

— Термин «облачные технологии» объединяет различные по архитектуре и принципам организации информационные системы. Чем отличаются вопросы безопасности и подходы к их решению в разных типах «облаков»?

— Действительно, термин неоднозначный, и для использования общей терминологии рекомендуется обратиться к стандартам NIST. Для начала следует различать частные и публичные «облака». Если речь идет о частном «облаке», владелец строит его сам или с помощью подрядчика, и, соответственно, сам несет ответственность за его работоспособность, сам должен прогнозировать нагрузки, сам должен выбрать и задействовать средства защиты.

Если мы говорим о публичном «облаке», то возможностей самостоятельных действий гораздо меньше. Ситуация зависит от того, какой именно тип облачной архитектуры реализован в «облаке» — SaaS, IaaS или PaaS. Но в любом случае у пользователя здесь гораздо меньше ответственности и возможностей, многие вещи вы, естественно, не сможете контролировать, например, физический доступ.

Если вы пользуетесь архитектурой IaaS, вы вполне можете поставить на виртуальную машину те средства защиты, которые считаете нужными. Здесь часто имеет смысл использовать средства, специально приспособленные под облачную архитектуру.

— Например?

— Например, средства, позволяющие переносить часть функционала безопасности на уровень операционной системы. В традиционном дата-центре межсетевое экранирование, как правило, аппаратное. А если вы хотите защитить от вторжений гостевую операционную систему в облачной среде, вам понадобится программный межсетевой экран, который вы в эту гостевую систему поставите. То же самое с контролем целостности, предотвращением вторжений и так далее.

Если говорить о SaaS, пользователь получает готовое прикладное решение, реализация которого находится за кадром. С точки зрения безопасности заказчик получает тот функционал, который предоставляет сервис-провайдер в рамках этого SaaS-приложения, например, механизм разграничения доступа на основе ролей или механизм усиленной аутентификации.

Также пользователи SaaS-приложений могут использовать наложенные средства безопасности. Это могут быть решения, которые шифруют данные, хранящиеся в «облаках», например, шлюз шифрования для Salesforce. Данные в SaaS-приложении хранятся в зашифрованном виде, а пользователь обращается к ним через шлюз. Подобные приложения узкоспециализированные, и на сегодня их уже появилось достаточно много.

PaaS можно считать промежуточным вариантом между IaaS и SaaS, и здесь «платформа как сервис» предоставляет пользователю некоторый набор функционала, в который входят и средства безопасности. Из них можно спроектировать и собрать необходимые средства защиты приложений и данных.

Риски: не игры с огнем, а трезвая оценка

— Пользователи, размещающие в «облаке» те или иные системы, беспокоятся о сохранности данных и приложений, которые больше не находятся у них в офисе. Насколько объективны эти опасения?

— И сейчас и год назад, и в России и за рубежом пользователей волнует по большей части конфиденциальность их данных в «облаке». Первая мысль — может ли получиться так, что мои данные станут доступны сотруднику провайдера, соседу по «облаку» или всему Интернету в результате какой-то ошибки или злого умысла. О других рисках люди думают гораздо реже, хотя они есть. Например, зависимость от провайдера — это тоже риск информационной безопасности, связанный с доступностью данных.

Реален ли риск доступа к данным третих лиц? В общем, да, случаи нарушения конфиденциальности были зафиксированы. Например, арендуя дополнительное дисковое пространство, пользователи могли обнаружить там данные других заказчиков, которые хранились там раньше.

— По вине провайдера?

— Изначально по вине разработчика гипервизора, который используется в данной системе виртуализации. Но с точки зрения пользователя, конечно, по вине провайдера.

Доступ к данным клиентов со стороны сотрудников провайдера теоретически возможен, но в реальности таких случаев у крупных и известных провайдеров, получивших огласку, не было зафиксировано.

Чаще встречается другой риск — несоответствие фактического уровня доступности заявленному. Такое происходит в результате оверселла мощностей провайдера или в результате недостаточной отказоустойчивости архитектуры — мы уже видели как «валился» Amazon. К сожалению, у российских провайдеров пока сбои происходят чаще, чем у западных: прецеденты временной недоступности сервиса и даже потери данных клиента, к сожалению не единичны.

Еще один риск, про который заказчики не всегда вспоминают — это выполнение законодательных требований по защите данных. Сейчас у нас есть закон о защите персональных данных, и использование «облаков» во многих случаях затрудняет его выполнение.

Риск инсайдера достаточно критичный, потому что чисто техническими средствами его невозможно на 100% ликвидировать. Существует также риск привязки к определенному провайдеру, важный, хотя не очень актуальный для нашей страны: у нас мало кто держит в «облаках» значительную часть информационных систем. А на Западе все больше распространяется практика резервного облачного провайдера. То есть мало иметь одного провайдера и даже резервирование в рамках этого провайдера. Нужно иметь наготове второго провайдера, готового перехватить нагрузку. Тут встают вопросы совместимости данных, репликации и

т.д., однако уже есть целый класс решений по управлению облачной нагрузкой, позволяющих быстро перекинуть ее с одного провайдера на другого.

Но пользователи действительно больше всего думают о риске нарушения конфиденциальности.

— А риск изъятия серверов с данными судебными приставами стоит принимать в расчет?

— Есть разные точки зрения на этот вопрос. Есть заказчики, которые считают разумным все выносить на Запад, чтобы предотвратить изъятие носителей информации силовыми структурами. Но есть и мнение, что в цивилизованной западной стране остановить сервис, например, по письму из Генеральной прокуратуры России даже проще. Это неожиданно, но я уже не раз слышал от разных людей, что отключить сервис и вынести данные из российского провайдера может быть для наших госорганов дольше и сложнее, чем из западного. За рубежом они законопослушные: по запросу из госорганов отключат, а потом уже будут разбираться.

Есть, конечно, и сервисы в менее цивилизованных странах, там могут и хакеры без проблем хоститься. Туда сколько ни пиши, ни звони, никто ничего отключать не будет, тем более изымать. Но там совсем другие риски.

Управление доступом и верность политике ИБ

— Огромное значение в облачной среде играет надежная аутентификация. Не становится ли слабым звеном пользователь с небрежным хранением паролей?

— Этот вопрос всегда возникает при использовании «облаков» в компаниях. Пользователь может использовать один пароль для своей учетной записи ВКонтакте и для корпоративной почты, например. А это уже серьезный риск.

Одним из решений может стать система управления учетными записями и доступом, специально разработанные, чтобы реализовать единую политику идентификации и доступа. Большинство провайдеров поддерживает интеграцию с такими системами благодаря открытым протоколам. То есть, используя у себя в офисе некую систему identity management, вы сможете интегрировать ее с облачным сервисом. Технически это вполне реализуемо, хотя и требует определенных затрат.

Вообще, я считаю, что развитие облачных сервисов в ближайшее время будет подстегивать развитие систем управления учетными записями и доступом. Такие системы существуют уже давно, крупные компании их уже внедрили, но сейчас они развиваются, чтобы удовлетворить требованиям облачных сред. Один из трендов — переход систем аутентификации и идентификации в те же «облака», где они становятся доступными по подписке. Пользователи облачного сервиса сначала обращаются к другому облачному сервису, который отвечает за аутентификацию. Такие системы могут предоставлять механизмы усиленной аутентификации: аппаратные токены, sms, а не просто логин и пароль.

— А что делают традиционные производители решений по безопасности для облачных сред?

— Большинство вендоров переориентируется на облачную реальность, в которой мы все оказались. Продукты адаптируют либо под облачную модель потребления либо под некое взаимодействие с «облаком». Например, системы очистки и контроля web-трафика и электронной почты многих вендоров стали доступны напрямую из «облака».

Есть и компании, которые выпускают продукты, изначально рассчитанные на облачную среду. Например, решения могут интегрироваться с системой управления Amazon.

— Это решения для провайдеров или для конечных пользователей?

— И для тех, и для других. Например, систему шифрования данных клиенты могут использовать самостоятельно. Либо же провайдер может предлагать шифрование как дополнительный сервис.

— Какие моменты должны быть оговорены в корпоративной политике безопасности, когда речь идет об «облаке»?

— Это обширный вопрос. В отношениях клиента и сервис-провайдера нужно предусмотреть очень много моментов, связанных с безопасностью и касающихся различных областей. Это физическая безопасность, разграничение доступа, возможность аудита и анализа защищенности.

Чтобы не изобретать велосипед, лучше обратиться к существующим документам. Организация Cloud Security Alliance публикует документы, которые помогают клиентам сориентироваться и учесть все, в том числе и на русском языке, на сайте RISSPA, которая представляет CSA в России. Опубликован, например, опросник Consensus Assessment Questionary, где собрано около 200 вопросов, которые клиент должен задать провайдеру перед тем, как начать работать.

Важная тема — сохранение имеющихся политик и наработок по безопасности при переходе в «облака». Конечно, серьезный клиент, у которого безопасность уже выстроена, должен, обращаясь к сервис-провайдеру, убедиться, что эти политики можно реализовать, как минимум, не хуже, чем уже есть в собственном дата-центре. Нужно обговорить возможность проверить это, обеспечить, если надо, доступ к логам, доступ на площадку и так далее.

Мировые стандарты как пример для подражания

— А у кого из глобальных лидеров, таких как Amazon, Salesforce, Google, Microsoft Azure, по вашему мнению, дела с безопасностью обстоят лучше других?

— Я бы сказал, что среди западных лидеров, которые вы назвали, к вопросам безопасности серьезно подходят практически все, и это хороший пример для российских провайдеров, которые пока отстают.

Важная западная черта — открытость. Компании проактивно делятся с заказчиками большей частью информации о том, как они защищают данные, какие процессы используют. Например, тот же опросник от CSA они сами заполняют и предоставляют клиентам для ознакомления.

Более того, они по собственной инициативе проходят сертификацию по таким стандартам как ISO 27001 и SSAE 16 и доказывают правдивость декларируемых мер защиты с помощью независимых аудиторов. Переход к таким провайдерам для многих организаций, особенно малых и средних, будет означать, что они свою безопасность повышают. Российские компании, к сожалению, далеко не все готовы делиться информацией о том, какую архитектуру безопасности они используют.

— Как вы думаете, будут ли отечественные провайдеры подтягиваться к мировым стандартам?

— Я очень надеюсь, что будут. Российское отделение Cloud Security Alliance в лице RISSPA активно этим занимается. Уже сейчас некоторые облачные провайдеры используют сертификацию по стандарту ISO 27000, чтобы подтвердить, что они данные клиентов действительно защищают. К сожалению, это происходит не у всех и зачастую фрагментарно. На Западе сертификация по стандартам ISO 27000, SSAE 16 — массовое явление, фактически стандарт для компаний, предоставляющих сервисы.

Отдельная тема — сертификация компаний, оказывающих услуги госорганизациям. В США существует и активно используется стандарт FEDRAMP, и он обязателен для компаний, желающих оказывать услуги государственным компаниям.

Опыт показывает, что лучшие мировые практики в области IT усваиваются и у нас, хотя зачастую и с опозданием. Сегодня многие российские заказчики обращаются к отечественным провайдерам просто потому, что это удобнее: не всех устраивает тот же Amazon, который принимает оплату только по кредитной карте и вообще неизвестно, где находится. Но я думаю, что уже в недалеком будущем соответствовать мировому уровню будет и качество сервиса.

Защита персональных данных в Alliance Healthcare Russia

Цель проекта — обеспечить соответствие требованиям ФЗ-152 «О персональных данных».

Работы в рамках проекта проводились по классической схеме, разработанной в компании Softline для реализации комплексных решений по защите персональных данных и прошедшей многократную успешную апробацию на практике. Эксперты Softline провели аудит всех бизнес-процессов компании, участвующих в обработке персональных данных, а также внутренних документов, регламентирующих обработку персональных данных сотрудников и клиентов компании. Был осуществлен анализ существующей документации и проведена оценка ее соответствия требованиям законодательства РФ о персональных данных.

По итогам реализации проекта были подготовлены рекомендации по приведению данных документов в соответствие требованиям, а также разработан необходимый комплект организационно-распорядительной документации, регламентирующей процессы обработки и защиты персональных данных.

О заказчике

Alliance Healthcare Russia является национальным фармацевтическим дистрибьютором России и частью международной фармацевтической группы Alliance Boots — европейского лидера в области красоты и здоровья. Компания имеет разветвленную сеть филиалов и представительств — работает более чем в 50 регионах, охватывая почти все часовые пояса России.

Елена Ващук, Директор Юридического департамента Alliance Healthcare Russia:

«Компания Softline зарекомендовала себя как профессиональный партнер, предоставивший оптимальное предложение по цене и оказавшего квалифицированную консультацию. Главным результатом реализованного проекта мы считаем то, что благодаря качественной работе, проделанной специалистами Softline, вся документация нашей компании, регламентирующая обработку персональных данных, стала соответствовать требованиям современного законодательства. Мы довольны экспертным уровнем специалистов Softline, умением эффективно решать поставленные задачи в заявленный срок».

Виталия Лепехина, руководитель направления аудита и консалтинга компании Softline:

«Нам было очень приятно работать с компанией Alliance Healthcare Russia. Наши специалисты провели анализ всех бизнес-процессов, связанных с обработкой персональных данных, а также существующей документации в этой сфере. По полученным результатам было предложено и реализовано оптимальное решение существующих проблем. Все работы были выполнены в запланированные сроки. Мы уверены, что это важный шаг Alliance Healthcare Russia на пути построения эффективной безопасности бизнеса, которая будет отвечать мировым стандартам».

Защита конфиденциальных данных НПО «Сатурн»

Перед специалистами Softline стояла задача защитить конфиденциальную информацию от угроз хищений со стороны внешних злоумышленников и рисков, связанных с ее непреднамеренным раскрытием или умышленной кражей внутренними пользователями — сотрудниками компании и лицами, имеющими доступ к конфиденциальным данным.

Сотрудники Softline провели общее обследование инфраструктуры предприятия, процессов обеспечения информационной безопасности и процессов обработки конфиденциальной информации в ряде бизнес-подразделений. Совместно со специалистами НПО «Сатурн» был определен порядок отнесения информации к конфиденциальной, подлежащей защите с использованием DLP-системы. На основании полученных данных разработано техническое задание на систему, включающее политики, определяющие способы реакции DLP-системы на различные события, в зависимости от типа рабочего места, бизнес-подразделения и степени конфиденциальности информации.

Инженерно-аналитическая команда Softline предложила клиенту решение McAfee Endpoint Data Loss Prevention, как наиболее соответствующее политике компании в отношении организации защиты информационных ресурсов от внутренних угроз. Совместно со специалистами НПО «Сатурн» был определен перечень рабочих мест для развертывания системы и произведено пилотное внедрение в соответствии с техническим заданием. В рамках проекта специалисты Softline осуществили пилотное внедрение DLP-системы на 150 рабочих мест, позволившее организовать управление потоками конфиденциальных данных в пилотной зоне и обеспечить их защиту от утечек по различным каналам (электронная почта, Интернет, съемные носители и т. д.).

О компании

Научно-производственное объединение НПО «Сатурн» — одно из крупнейших в России предприятий ВПК по производству и обслуживанию газотурбинных двигателей, в том числе для самолетов марки «Сухой». Продукция завода ориентирована на гражданскую и военную авиацию, а также военно-морской флот. Выручка компании от реализации продукции составляет 10,5 млрд. руб., а чистая прибыль — 53,3 млн руб. (данные 2011 года).

Антон Афанасьев, руководитель направления прикладных решений информационной безопасности компании Softline:

«Успешность проекта по защите конфиденциальной информации от утечек во многом зависит от уровня доверия и взаимопонимания между заказчиком и исполнителем. Квалификация сотрудников НПО «Сатурн» и их активное участие в проекте позволило выполнить работы раньше установленных сроков и с высоким уровнем качества».

Сергей Кожевников, начальник отдела информационной безопасности НПО «Сатурн»:

«Решение McAfee Endpoint DLP, предложенное специалистами компании Softline, оптимально подошло под решаемые нами задачи. В процессе реализации проекта мы по-новому взглянули на проблему утечки данных с учетом специфики работы каждого из подразделений предприятия. Важно отметить, что DLP-система органично дополняет существующие средства и меры защиты, не нарушая при этом существующие бизнес-процессы. Проведенная аналитическая работа обеспечивает комплексный подход к защите конфиденциальных данных от утечек, а также возможность масштабирования решения в будущем с меньшими трудозатратами».

***Портал** – безусловный лидер среди СМИ отрасли безопасности на российском медиарынке. Это связующее звено между производителями и конечными потребителями, между поставщиками оборудования и монтажными организациями, между интеграторами и заказчиками. SEC.RU – это простой и эффективный сервис, который уже в течение многих лет является незаменимым инструментом каждого специалиста в области безопасности.*

SEC.RU

КОРОТКИЙ ПУТЬ
К ИНФОРМАЦИИ

ФОРУМ

Огромная отраслевая площадка для общения профессионалов. Самые актуальные темы, консультации у ведущих специалистов, обсуждение новостей, статей, материалов. Спрашивайте, делитесь опытом, общайтесь на Форуме SEC.RU.

ВЕБИНАРЫ

Этот новый сервис Портала SEC.RU позволит провести онлайн-мероприятие, на котором любой из зарегистрированных пользователей сможет выступить как участником, так и докладчиком независимо от своего местоположения.

ГИПЕРМАРКЕТ

Сервис SEC.RU, позволяющий оперативно найти и подобрать оборудование по любой ценовой категории, ознакомиться с полным ассортиментом производителя, рассмотреть разные предложения и отыскать поставщиков в своем родном городе.

WWW.SEC.RU

Внедрение защищенной сети передачи данных в Национальном банке «ТРАСТ»

Цель проекта — повысить контроль и безопасность передачи данных во всех узлах корпоративной сети банка.

Ранее в сетевой архитектуре компании использовались программно-аппаратные комплексы Cisco и Juniper. Однако значительное увеличение клиентской базы, географическое расширение сети филиалов, рост интенсивности бизнес-процессов, повысили актуальность модернизации сети передачи корпоративных данных. Инженерно-аналитическая группа Softline проанализировала существующую сетевую инфраструктуру банка и предложила схему внедрения аппаратных решений и их интеграции с существующей сетевой архитектурой. Развертывание решений проводилось в тестовой зоне и явилось образцом конфигурации данных решений для дальнейшей промышленной эксплуатации.

Антон Чернов, руководитель проектов компании Softline:

«На момент реализации проекта в сетевой архитектуре компании использовались программно-аппаратные комплексы таких производителей, как Cisco и Juniper. Инженерно-аналитическая группа, работавшая на проекте, осуществила их интеграцию с оборудованием CheckPoint».

Владимир Трояновский, директор по поддержке информационных систем банка «ТРАСТ»:

«Деятельность банка «ТРАСТ» связана с большим объемом передаваемой и обрабатываемой информации. В связи со значительным увеличением клиентской базы, расширением географии регионального присутствия и ростом интенсивности бизнес-процессов повышается актуальность модернизации сети передачи данных. В наших планах – дальнейшая реализация проектов по внедрению решений безопасности для сети банка».

О заказчике

Национальный банк «ТРАСТ» предоставляет полный спектр услуг частным и корпоративным клиентам. Имеет одну из самых масштабных региональных сетей: филиалы представлены в 170 городах России, 278 офисов от Калининграда до Владивостока.

Внедрение системы web-фильтрации в ОАО «Каустик» (группа компаний НИКОХИМ)

Для того, чтобы оптимизировать web-трафик и повысить эффективности работы интернет-каналов, на предприятии было внедрено решение Cisco IronPort Web Security.

Взаимодействие в рамках проекта началось с предварительного анализа и сравнения решений web-фильтрации трех производителей, из которых всем требованиям заказчика соответствовало лишь одно — Cisco IronPort Web Security. Инженерная команда Softline разработала оптимальную схему внедрения выбранного решения, произвела необходимые настройки в соответствии с политиками безопасности клиента. Специалисты провели пилотное тестирование решения в инфраструктуре заказчика, во время которого IronPort Web Security проявил себя как эффективное и гибкое решение, позволяющее настроить сложные правила обработки и блокировки трафика.

О компании

ОАО «Каустик», входящая в группу компаний НИКОХИМ, является одним из крупнейших промышленных предприятий России, занимает лидирующие позиции в химической отрасли страны по выпуску синтетической соляной кислоты, товарного хлора, жидкой и твердой каустической соды.

Данил Ананьев, начальник отдела администрирования сетевой инфраструктуры, ОАО «КАУСТИК»:

«Как крупная промышленная компания с развитой IT-инфраструктурой мы понимаем все преимущества комплексной контентной фильтрации для защиты и обеспечения непрерывности бизнес-процессов. Главным результатом реализованного проекта мы считаем то, что благодаря профессиональной консультационной поддержке и слаженной технической работе специалистов Softline мы получили надежный инструмент защиты от нежелательного трафика, оптимизированный интернет-трафик и возможности легкого администрирования процессов его фильтрации».

Александр Мосягин, ведущий консультант компании Softline:

«В процессе реализации проекта Softline провела демонстрацию решений на своей площадке, проконсультировала специалистов заказчика по вопросу выбора подходящего продукта, произвела работы по тестовому внедрению и, после успешного тестирования, помогла перевести решение в промышленную эксплуатацию. Тем самым этот проект прошел все стадии — от постановки задачи до внедрения — в тесном взаимодействии с ОАО «Каустик» и полностью отражает подход Softline к работе с клиентами. В результате весь парк ПК компании надежно защищен от нежелательного трафика и проникновения в IT-инфраструктуру вредоносных программ. В дальнейшем мы планируем расширять сотрудничество с компанией «Каустик» и уже проводим демонстрации новых технологий в области виртуализации и резервного копирования».

XXIII ежегодная выставка информационных и коммуникационных технологий

30 ОКТЯБРЯ - 2 НОЯБРЯ
Москва, ВВЦ
павильон №69

ГЛАВНОЕ СОБЫТИЕ В ОБЛАСТИ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ — 2012 год

SofTool

специальные проекты: выставки «ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА», «САПР-экспо»

основные направления:
Технологии управления
Электронное государство, ЭЦП, ЦОД
Банковское, финансовое и экономическое ПО
Региональные и муниципальные системы
Информационная безопасность
ПО для бирж и инвестиционных компаний
Универсальная электронная карта
Технологии автоматической идентификации
Cloud Computing, Технологии образования
САПР, Электронный документооборот
Свободное ПО, Прикладное ПО
Суперкомпьютеры, Управление проектами,
Интернет, Мобильные технологии
Встраиваемые системы, сетевые решения
Аутсорсинг, ИТ-услуги, Компьютеры
Оборудование, Электронные развлечения

главное событие: Всероссийский национальный форум «ИНФОРМАЦИОННОЕ ОБЩЕСТВО»

цели выставки: Выявление, поощрение и продвижение на рынок наиболее значительных и перспективных разработок в области ИКТ. Популяризация и стимулирование развития ИКТ в России. Организация содействия и поддержки российских ИКТ-компаний.

Официальная поддержка

Российская академия наук
Министерство связи и массовых коммуникаций Российской Федерации
Министерство образования и науки Российской Федерации
Российский фонд фундаментальных исследований
Федеральное космическое агентство
РОСАТОМ Госкорпорация по атомной энергии «Росатом»

После регистрации на сайте Вы получите электронный билет

Став участником выставки, Вы получите новых клиентов

В конференциях примут участие ведущие ИТ-специалисты

В рамках Softool состоятся:

Конференция «Электронное государство XXI века»
- Пленарное заседание
- Заседание Совета главных конструкторов информатизации регионов РФ
- Конференция «Безопасность в современном обществе»
- Конференция «Облачные технологии и услуги Электронного правительства»
- III Московский суперкомпьютерный форум

Мастер-классы по системам автоматизированного проектирования

Конкурс «Softool: Продукт года»

ПРОДУКТ ГОДА SOFTOOL

Объявляется конкурс лучших решений в области ИТ «Softool: Продукт года»! Учредители конкурса: Российская академия наук, Министерство связи и массовых коммуникаций РФ, Российский фонд фундаментальных исследований, издательство «Открытые системы» и компания «ИТ-экспо»

ИНФОРМАЦИОННОГО ОБЩЕСТВА ТЕХНОЛОГИИ

САПР ЭКСПО

По оценкам экспертов Softool - это лучшая российская компьютерная выставка, предоставляющая посетителям максимальный комфорт и необходимые условия для бизнеса

ИТ-ЭКСПО
ООО "ИТ-экспо"
ул. Рождественка, 6/9/20, стр.1, г. Москва, 107031
Тел.: +7 (495) 624-7072/4556
softool@softool.ru

Встретимся на Softool'е!

Защита корпоративной сети
ООО Коммерческий Банк «Камский горизонт»

Внедрение решения Kaspersky Business Space Security позволило создать надежную систему защиты корпоративной сети банка — рабочих станций и файловых серверов.

Ситуация

Информационная инфраструктура ООО Коммерческого Банка «Камский горизонт» представляет собой доменную сеть с 50 рабочими станциями, защиту которых необходимо было обеспечить отделу автоматизации банковских операций. Наиболее важным критерием при выборе продукта было наличие таких функций, как мониторинг уязвимостей и контроль активности программ.

Решение

«Продукт «Лаборатории Касперского» был выбран из ряда других антивирусных решений по результатам тестов, проведенных в КБ «Камский горизонт». Внедрение Kaspersky Business Space Security повысило уровень информационной безопасности и обеспечило непрерывность бизнес-процессов в банке. Используя новые технологии защиты данных, ООО КБ «Камский горизонт» совершенствует и свой бизнес», — говорит Александр Дьяконов, программист отдела автоматизации банковских операций ООО «Камский Горизонт».

«Внедрение Kaspersky Business Space Security стало логичным шагом на пути к построению системы комплексной безопасности организации. Надеемся, что наше сотрудничество в этом направлении продолжится, мы со своей стороны готовы приложить максимальные усилия для реализации всех необходимых задач заказчика», — отмечает Евгений Робинов, руководитель направления по информационной безопасности Softline в Казани.

Результат

Kaspersky Business Space Security позволил обеспечить оптимальную защиту информационных ресурсов КБ «Камский горизонт» от современных интернет-угроз, а также обезопасить рабочие станции и файловые серверы от всех видов вирусов, троянских программ. Решение призвано обеспечить сохранность информации и мгновенный доступ пользователей к сетевым ресурсам. Продукт разработан с учетом повышенных требований к серверам, работающим в условиях высоких нагрузок. Благодаря всем этим характеристикам внедрение Kaspersky Business Space Security позволило повысить уровень информационной безопасности и обеспечило непрерывность бизнес-процессов в банке.

О компании

ООО Коммерческий Банк «Камский горизонт» осуществляет свою деятельность в г. Набережные Челны Республики Татарстан с 1993 года. Банк, ориентированный на работу со средними и мелкими клиентами, оказывает высококачественные банковские услуги юридическим и физическим лицам.

Softline обеспечила IT-безопасность сети спортивных магазинов «Чемпион»

Заказчик

Федеральная сеть спортивных магазинов «Чемпион» сегодня — это 24 мультибрендовых магазина в городах: Уфа, Стерлитамак, Салават, Нефтекамск, Оренбург, Тольятти, Казань, Набережные Челны, Бугульма, Самара, Красноярск, Новокузнецк, Новосибирск, Тюмень, Омск, Челябинск. Магазины работают в двух форматах: спортивный супермаркет медиум-класса и спортивный супермаркет эконом-класса.

Ситуация

IT-среда компании «Чемпион» имеет территориально распределенную структуру с центром в Уфе и 15 филиалами по России, с парком ПК, насчитывающим более пятисот машин.

Для обеспечения защиты рабочих станций и файловых серверов от вредоносного и нежелательного ПО перед компанией встала задача приобретения антивирусного решения. Выбор в пользу продукта «Лаборатории Касперского» — Kaspersky Business Security — был сделан благодаря тому, что это программное обеспечение помимо главной функции (антивирусной защиты) обеспечивает также сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Решение

Программное обеспечение Kaspersky Business Space Security защищает рабочие станции и файловые сервера от всех видов троянских программ и вредоносного ПО, предотвращает вирусные эпидемии, обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам. Продукт разработан с учетом повышенных требований к серверам, работающим в условиях высоких нагрузок.

Поставщиком выступила компания Softline, партнер «Лаборатории Касперского» в Уфе с наивысшим партнерским статусом — Enterprise Partner.

В штате представительства Softline Уфа работают сертифицированные специалисты по антивирусной защите, готовые оказать своим клиентам полную консультационную поддержку и сопровождение, провести внедрение и техническое обслуживание средств защиты. По желанию заказчика преподаватели Учебного центра Softline проводят курсы для IT-специалистов по применению антивирусной системы — как в классах, так и дистанционно.

Результат

«Благодаря решению Kaspersky Business Space Security обеспечена защита рабочих станций от вредоносного и нежелательного ПО. Мы довольны качеством предоставленных услуг и выгодными ценовыми предложениями», — отметил Ренат Богданов, руководитель IT-подразделения сети спортивных магазинов «Чемпион».

Защита сети компании «ТМК Инструменты»

Softline осуществила поставку в сеть магазинов «ТМК Инструмент» более 300 лицензий на использование Kaspersky Work Space Security — решения для защиты рабочих станций, ноутбуков и смартфонов от всех видов современных компьютерных угроз.

О компании

Компания «ТМК», успешно работающая на рынке электроинструмента и оборудования уже более 15 лет, входит в тройку крупнейших специализированных розничных операторов России. В сети «ТМК» — 76 магазинов (из них 32 собственных и 44 — франчайзи) в Нижнем Новгороде, Нижегородской области, Татарстане, Кирове, Уфе, Ульяновской области, компания осуществляет поставки в более чем 200 городов России. «ТМК» имеет 2 авторизованных сервисных центра в Нижнем Новгороде и Казани, является партнёром ведущих производителей электроинструментов и оборудования: Bosch, Skil, Black & Decker, DeWALT, SPARKY, Makita, Husqvarna, Stiga, Belle Group.

Ситуация

«На сегодняшний день в компании «ТМК» более 300 рабочих станций и 30 серверов. При поиске решения для защиты от вирусных угроз основными критериями отбора ПО стали: централизованная управляемость, простота внедрения и «доступность» интерфейса для пользователей. Решающую роль сыграло средство администрирования Kaspersky Security Center, т.к. оно позволяет централизованно управлять всеми рабочими станциями. Внедрение заняло 14 дней», — рассказывает начальник IT-службы «ТМК» Андрей Евдокимов.

Решение

Поставка была осуществлена компанией Softline, обладающей наивысшими компетенциями и многолетним опытом работы с клиентами в области IT, что подтверждается высоким партнерским статусом от «Лаборатории Касперского» — Kaspersky Enterprise Partner.

«Softline хорошо понимает структуру бизнес-процессов «ТМК Инструменты» и особенности ее корпоративной информационной сети. IT-инфраструктура представляет собой множество территориально распределенных по всей России офисов, что, несомненно, сказывается на выборе подхода в вопросе обеспечения ИБ. Программный продукт Kaspersky Work Space Security подходит компаниям, имеющим широкую сеть представительств, поскольку дает возможность быстрого подключения удалённых офисов и обладает функцией централизованного управления», — говорит руководитель представительства Softline в Нижнем Новгороде Роман Яшин.

Результат

«Прозрачность и управляемость системой антивирусной защиты рабочих станций, стабильность работы и минимизированные простои компьютерной техники, — вот основные результаты, которых мы достигли благодаря внедрению продукта Kaspersky Enterprise Partner», — говорит Андрей Евдокимов.

Kaspersky Work Space Security обеспечивает защиту рабочих станций, ноутбуков и смартфонов в мультиплатформенных корпоративных сетях.

Kaspersky Enterprise Space Security для ООО «Столичный ювелирный завод»

Федеральный отдел конкурсных продаж компании Softline завершил поставку защитного решения Kaspersky Enterprise Space Security в ООО «Столичный ювелирный завод». Проект позволил обезопасить рабочие станции, ноутбуки, файловые и почтовые сервера заказчика от вредоносных программ и хакерских атак.

Ситуация

«Информационная инфраструктура компании состоит из центрального офиса, оптовой и розничной сетей, и все объекты этой цепочки соединены каналами связи. В корпоративной сети работает около 400 пользователей. Антивирусное программное обеспечение используется более 15 лет. В этом году ООО «Столичный ювелирный завод» принял решение о закупке защитного ПО «Лаборатории Касперского» — Kaspersky Enterprise Space Security.

Решение

«Основными критериями отбора программного обеспечения для защиты от вирусных угроз стали многолетний успешный опыт присутствия продукта на рынке, возможность централизованного управления и контроль доступа к устройствам», — рассказывает директор по IT ООО «Столичный ювелирный завод» Сергей Адмиральский.

Лицензирование осуществила компания Softline, обладающая наивысшими компетенциями и многолетним опытом работы в области IT, что подтверждается и высоким партнерским статусом от «Лаборатории Касперского» — Kaspersky Enterprise Partner. Softline представила клиенту оптимальное коммерческое предложение, позволившее минимизировать временные и материальные затраты заказчика.

Результат

«Столичный ювелирный завод является нашим давним хорошим партнером. Когда возник вопрос о создании системы безопасности в обширной, развернутой производственной и торговой сети, компания сразу обратилась к нам. В кратчайшие сроки проект был реализован, и вот уже на протяжении 15 лет совместная работа продолжается, охватывая все большее и большее число защищаемых объектов. Несомненно, это оптимально решение для нашего партнера: выгодное, легко реализуемое и надежное», — рассказывает Павел Просекин, менеджер Федерального отдела конкурсных продаж компании Softline.

Заказчик

ООО «Столичный ювелирный завод» является бесспорным лидером российского ювелирного рынка. По объемам производства ювелирных изделий из драгоценных металлов он опережает любого другого российского производителя ювелирных изделий более чем в 2 раза. Партнерами ООО «Столичный ювелирный завод» — являются ООО «АДАМАС-Ювелир» — партнер по оптовым продажам продукции, а также ООО «АДАМАС-Ювелирторг» — розничная сеть, насчитывающая более 200 магазинов по всей территории России. Ювелирные изделия ООО «Столичный ювелирный завод» официально экспортируются в Украину, Беларусь, Казахстан.

О продукте

Программное обеспечение Kaspersky Enterprise Space Security защищает рабочие станции, файловые и почтовые серверы от всех видов современных интернет-угроз. Решение Kaspersky Enterprise Space Security гарантирует свободный обмен информацией внутри компании и безопасные коммуникации с внешним миром, а также удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

О «Лаборатории Касперского»

«Лаборатория Касперского» — крупнейший в Европе производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама. Компания входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности. По итогам 2010 года, выручка компании выросла на 38%, превысив 500 млн долларов США. В «Лаборатории Касперского» работают более 2300 высококвалифицированных специалистов. Продукты компании надежно защищают компьютеры и мобильные устройства более 300 млн пользователей во всем мире, технологии используются в продуктах крупнейших мировых поставщиков программных и аппаратных решений.

Новая концепция. Новый подход. Новое решение ваших задач.

Корпоративный портал DeskWork

на базе SharePoint 2010

Microsoft SharePoint

Эффективные коммуникации

Плодотворное сотрудничество

Экспресс-документооборот

Быстрое согласование и утверждение документов

Автоматизация рабочих процессов

Устранение беготни и рутины

Единый доступ к информации

Все всегда на своем месте

DeskWork

Информационные блоки

Максимум информации о компании

Центр задач

Ответственность и контроль

Видео-конференции

Удобно. Близко. Очевидно.

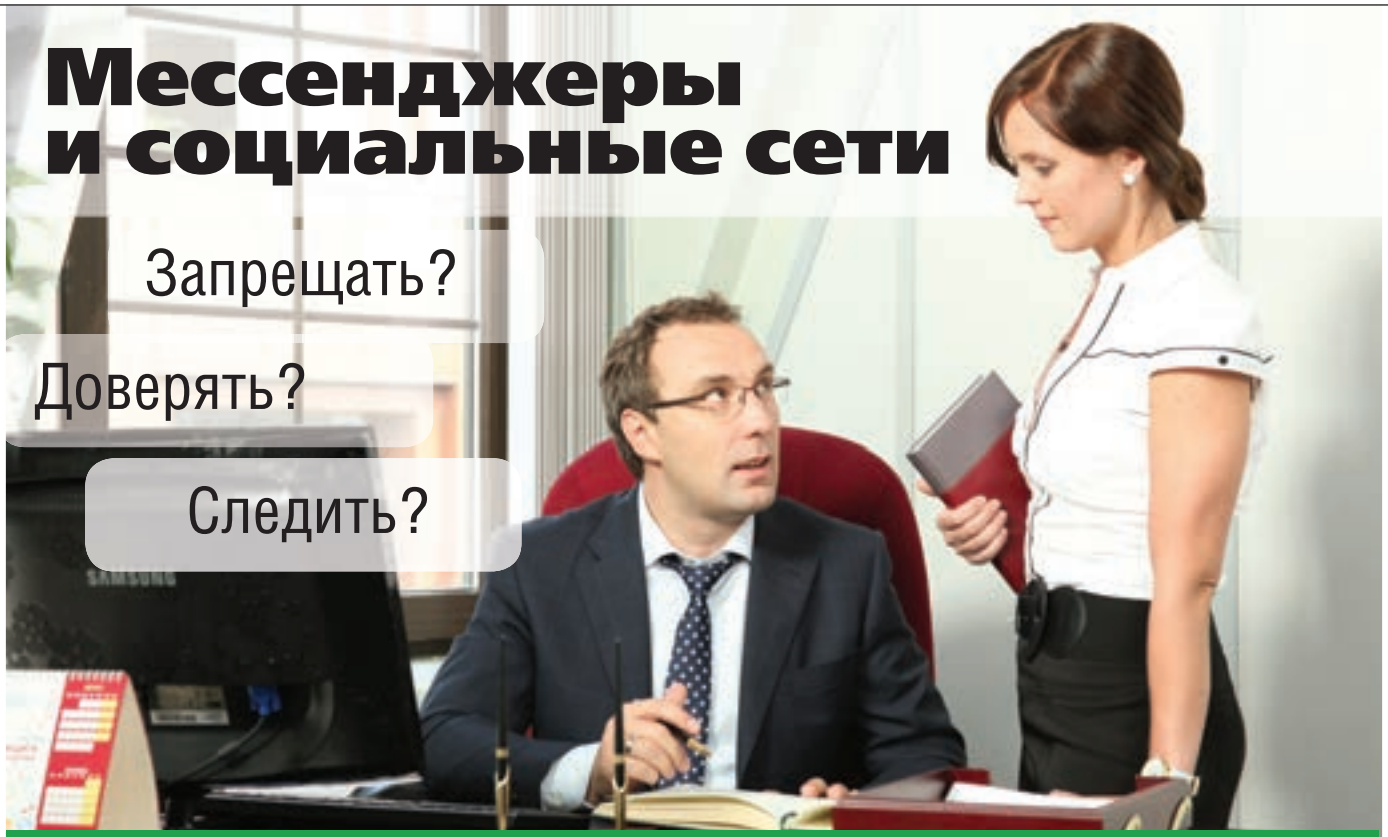
Графический построитель бизнес-процессов

Простое создание произвольных маршрутов

Департамент DeskWork и программных разработок

T +7 (495) 232 00 23 доб. 0590 | sales@deskwork.ru

Мессенджеры и социальные сети



А как **ВЫ** обеспечиваете безопасность внутри своих компаний?

Петр Федоров, технический эксперт компании Agnitum, руководитель проекта Outpost AV Service

Мы не запрещаем нашим сотрудникам доступ к социальным сетям и мессенджерам. Дело в том, что на первом месте у работника должно быть понимание опасности: какой вред это наносит рабочему процессу.

Кроме того, когда у сотрудника большая загрузка и много задач, ему просто некогда в социальных сетях сидеть!

А по поводу заражения вирусами из Интернета — есть 2 способа противостояния: защита периметра настройками безопасности и обучение всех сотрудников элементарным правилам «гигиены» в сети. В силу специфики нашей работы, в нашей компании с этим проблем не возникает!

Сергей Вахонин, IT-директор компании «Смарт Лайн Инк»

Любой сотрудник, увлекшись общением, может забыть о требованиях конфиденциальности и «невзначай» поделиться в своем блоге, группе любимой социальной сети или на публичном форуме знанием важных нюансов бизнеса компании, ее структуры и т.п. С участием в социальных сетях связаны повышенные риски заражения рабочего компьютера троянами и другими вредоносными программами.

Да, очень часто компании просто запрещают своим сотрудникам пользоваться мессенджерами и перекрывают выход в социальные сети и почтовые сервисы на корпоративном брандмауэре, но при этом все равно остается риск подключения компьютеров к Интернету, минуя блокировки с помощью персональных Wi-Fi подключений или модемов для сотовых сетей.

Проще всего было бы «закрыть и не пускать» — но нельзя не признать, что социальные сети и другие сервисы Web 2.0 стали необходимым бизнес-инструментом для целого ряда подразделений большинства компаний, особенно маркетологов, кадровых служб и т.п. Кроме того, компьютеры сотрудников могут выходить в Интернет не только через корпоративные шлюзы и брандмауэры, но и обходя их контроль посредством персональных USB-модемов и разнообразных адаптеров беспроводного доступа. Так что для изобретательного ума тотальный запрет ряда сайтов на корпоративном брандмауэре большой проблемой не является.

Чтобы не искать виновных в рядах службы ИБ и не считать убытки после реальной утечки важной информации, стоит позаботиться об укреплении дисциплины сотрудников, а для ее технического обеспечения — применять средства защиты информации: прежде всего, средства предотвращения утечек данных с корпоративных компьютеров (Endpoint Data Leak Prevention). Такие DLP-решения, во-первых, должны сводить социальный фактор к минимуму и пресекать нарушения дисциплины, блокируя утечки данных непосредственно с компьютера. Во-вторых, DLP-решение должно фиксировать и сохранять все факты и детали нарушений, чтобы у службы безопасности была возможность выявлять нарушителей и привлекать их к ответственности.

В DLP-комплексе DeviceLock 7 Endpoint DLP Suite представлен весь необходимый инструментарий как для аудита и анализа активности пользователей в социальных сетях и других web-сервисах, так и средства для контроля передачи конфиденциальной информации в форумы социальных сетей.

Борис Грейдингер, директор по IT российского представительства компании ESET

Социальные сети и мессенджеры, безусловно, несут в себе различные риски для корпоративной сети компании. Мы стараемся подходить к вопросу обеспечения безопасности сбалансировано: используем аппаратно-программные комплексы защиты, обучаем сотрудников правилам поведения в сети.

Все сисадминские чудеса на одной поляне

В последние выходные июля в Калужской области прошел седьмой по счету Всероссийский Слет Системных Администраторов (www.SletAdminov.ru). Участниками мероприятия стали более 5 000 человек со всех городов России, СНГ и ближнего зарубежья, собравшихся, чтобы в кругу коллег и единомышленников отметить свой профессиональный праздник.

Бессменным организатором Слета, начиная с его истоков в 2006 году, является компания Softline, в этом сезоне к организации мероприятия подключилось рекламное агентство EfficientCom (www.facebook.com/EfficientCom).

Пятиборье, костер и даже термы

Для проведения праздника было выбрано новое место — Центр культуры и туризма «Высокие Берега» (Калужская область), уютно расположившийся на живописном берегу Оки.

Темой Слета стали «7 сисадминских чудес» и то, как их себе представляют сами участники мероприятия. На протяжении трех дней на Поляне творились удивительные вещи, царила атмосфера праздника и всеобщего веселья.

Партнеры и организатор Слета подготовили для всех участников интересные программы. Все желающие могли покататься на «ЗаОблачном чуде» — огромном воздушном шаре от Softline и компании «Лаборатория Касперского» и посмотреть на площадку Слета с высоты птичьего полета; поучаствовать в веселых конкурсах от Allsoft.ru и «Доктор Веб», сразиться с противниками в «водных боях» от ActiveCloud, получить заветную красную шляпу от Red Hat или просто расслабиться и отдохнуть в пляжной зоне Symantec — «безопасных сисадминских термах». Здесь можно было вылепить сисадминское чудо из песка, а также испытать свою ловкость и перебраться на противоположный берег по «Висячим Садам Семирамиды».

Не обошлось и без традиционного пятиборья с метанием мышей и клавиатур, перетягиванием каната, собиранием клавиатуры по памяти, а также с поднятием 70-килограммовой штанги из мониторов. Самых сильных, метких и ловких награждала компания Microsoft.

Но на этом сюрпризы не закончились. Кроме конкурсов и развлекательных программ организаторы подготовили обширную конференционную часть с выступлением ведущих специалистов и экспертов IT-сферы.

Еще одним «чудом» стала самая настоящая пирамида, возведенная компанией Softline. В ней можно было не просто послушать доклады от представителей таких компаний, как Softline, Microsoft, Symantec, «Доктор Веб», Red Hat, Allsoft, Tekmi и ActiveCloud, но и побеседовать с ними, задать интересующие вопросы или поделиться своим мнением.

Поможем детям!

«Сейчас можно с уверенностью сказать, что Слет удался, и нам очень приятно читать позитивные отзывы и благодарности от его участников. Но творить чудеса, пусть даже и небольшие, можно не только раз в году. Поэтому компания Softline инициировала благотворительную акцию — «Сисадмины России помогут детям Калужской области», области, которая вот уже в седьмой раз радует всех участников своим теплом и уютом. Часть денег, вырученных от продажи билетов за мероприятие, будет направлена в Калужскую детскую областную больницу», — рассказывает Роман Агафонов, главный организатор Слета.

Цель благотворительной акции — предоставить детям, которые на долгое время остаются в больнице, возможность учиться по школьной программе. Для организации класса были закуплены Wi-Fi-роутер, ноутбуки, столики для ноутбуков и др. Волонтеры со Слета наладили работу компьютерной сети.

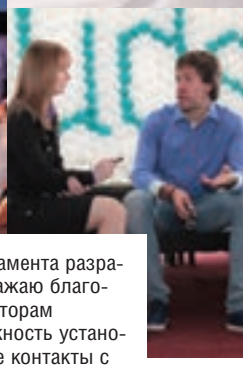
Компании «Лаборатория Касперского» и Microsoft предоставили лицензионное программное обеспечение.

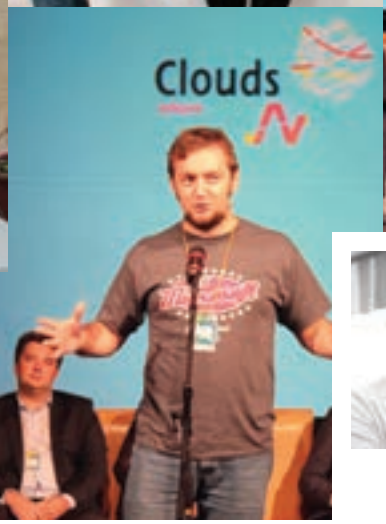
Викто Михайлов, Главный врач ГУЗ «Калужская областная детская больница», отмечает: «В связи с тем, что болезнь может иметь крайне затяжной характер, дети, особенно школьного возраста, вынуждены год, а иногда и больше проводить в стенах больницы. Для того, чтобы ребята не отставали от школьной программы, было решено организовать для них полноценный учебный процесс, позволяющий заниматься с преподавателями в режиме web-конференций».

Спасибо!

Компания Softline выражает благодарность участникам, партнерам и информационным партнерам Слета: журналам «Системный администратор», Business Excellence, «Национальные проекты», «Время Инноваций», «BIS Journal — Информационная безопасность банков», MSDN Magazine/Русская Редакция, «Компьютер Пресс», издательству Finestreet, интернет-порталам F1CD, SEC.RU, Astera, Proatom, IT-eburg, 3Dnews, BZZN.ru, BYTEMAG.ru, ITmozg.ru, IT-Terra Воронеж, IT-Доминанта, Bash.org.ru, IT Tube, S4b GROUP.ru, SOFTWEEK.ru, IXBT.com, Самара TECH, Telekomza, SPBIT.ru, ICT-online.ru, itsz.ru, mskit.ru, nnit.ru, it-portfolio.net, 2usb.ru, REG.RU, а также CIO Club Юг — клубу IT-директоров Юга России.

CloudsNN-2012





«Я от лица Департамента разработки Softline выражаю благодарность организаторам Форума за возможность установить долгосрочные контакты с представителями бизнеса разного сегмента и обсудить тенденции облачного бизнеса с экспертами рынка. Присутствуя в демонстрационной зоне и принимая участие в самых горячих обсуждениях, мы сполна смогли поделиться нашим экспертным мнением и опытом web-разработки сложных высоконагруженных проектов», — сказал Александр Демин, менеджер по продажам Отдела активных продаж Softline.

23–24 августа в Нижнем Новгороде состоялся Международный Форум сервис-провайдинга «CloudsNN-2012». В рамках данного мероприятия, было представлено более 60 докладов, работа проходила на протяжении почти 20 часов — в течение этого времени эксперты в сфере облачных технологий и представители ведущих международных и российских IT-компаний делились своими проектами и разработками.

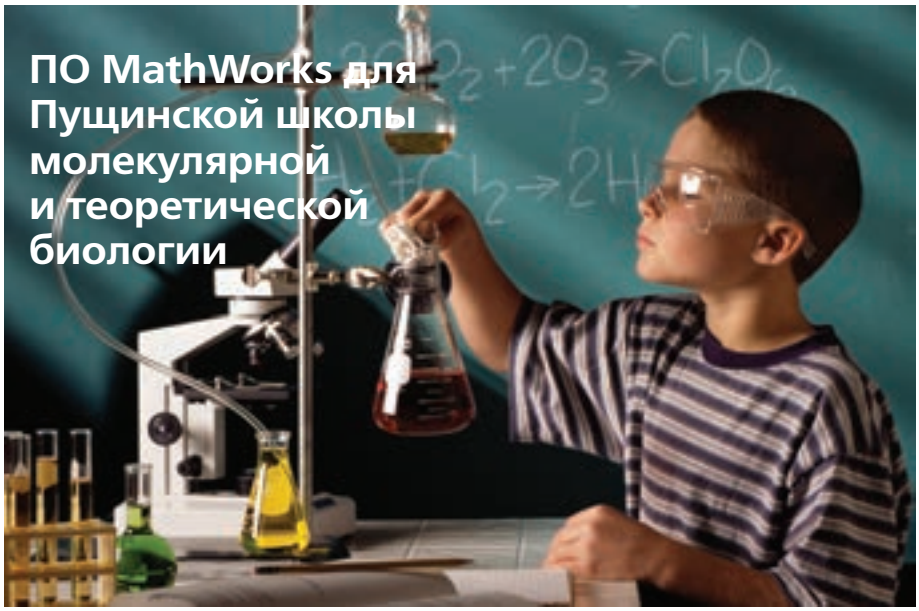
Два дня на Форуме работали шесть секций: «Облачные технологии», «Коммуникации в облаке», «Информационная безопасность», «Инновации в IT», «Управление 2.0», «Партнерство в SaaS». Специалисты обсуждали вопросы, касающиеся развития SaaS в России. На Форуме были представлены новые разработки на базе облачных платформ. Некоторые компании, которые в 2011 году посетили мероприятие в качестве слушателей, в этом году выступали уже в качестве спикеров и представляли свои облачные продукты. Кроме того, получили освещение вопросы развития IT-бизнеса, использования облачных технологий для улучшения бизнес-процессов.

Всего в Международном Форуме «CloudsNN-2012» приняли участие более 1000 человек, среди которых были представители из Нижнего Новгорода, Москвы, Санкт-Петербурга, Ростова-на-Дону, Екатеринбурга, Кирова, Тулы, Новосибирска, Челябинска, Красноярска, а также Украины и Белоруссии. Online-трансляцию просматривали более 13000 пользователей. Кроме того, в социальной сети Facebook за ходом Форума в течение двух дней следили более 100 тыс. человек, по количеству упоминаний хештега #CloudsNN мероприятие вошло в топ российского Twitter-а (2-ое место). Это означает, что Форум Clouds NN 2012 (cloudsnn.ru) активно обсуждала вся Россия!

«Так сложилось, что мы всегда поддерживали облачные инициативы компании МегаНН, поэтому не могли остаться в стороне от CloudsNN-2012. Наш «облачный десант» привез новые тенденции и решения, которые были представлены обширной аудитории форума. Мы благодарны организаторам за предоставленную возможность интересного и конструктивного диалога с нижегородскими предпринимателями!» — комментирует Заместитель директора по новым технологиям Softline Антон Салов.

«Выражаем благодарность всем спикерам, представителям компаний, СМИ, активно принимающим участие в работе Международного Форума сервис-провайдинга «CloudsNN-2012». Надеемся на дальнейшее сотрудничество и совместную работу!» — говорит руководитель Форума Денис Исмаков.


энергетика
рестораны и гостиницы
банки и страховые компании
медиа
retail
e-commerce
госсектор
строительство и проектирование
телекоммуникации
softline
Services Software Cloud
Заказная разработка интернет-решений и ПО
Департамент разработки Softline
+7 (495) 232 00 23 доб. 2085
webdev@softline.ru
services.softline.ru/webdev



ПО MathWorks для Пущинской школы молекулярной и теоретической биологии

Softline, эксклюзивный представитель компании MathWorks в России, поддержала «Школу молекулярной и теоретической биологии», прошедшем в августе в Пущино: компания предоставила проекту программное обеспечение MathWorks для биологических вычислений.

Пущинская «Школа молекулярной и теоретической биологии» — проект фонда «Династия». В рамках двухнедельной летней школы углубленного изучения биологии и смежных дисциплин 65 российских учащихся в течение двух недель принимали участие в научных исследованиях на базе лабораторий Института белка РАН.

В школе созданы условия для воспроизведения и моделирования реального исследовательского процесса, в который вовлечены школьники и научные сотрудники, в том числе ученые с международным именем. Таким образом, организаторы рассчитывают на формирование сообщества школьников, ориентированных на продолжение карьеры в наиболее динамично развивающихся областях современной биологической науки. В программу школы входят как экспериментальные биологические исследования, так и работа в смежных дисциплинах: биоинформатике, биохимии, биофизике. Учитывая междисциплинарный характер современной науки, наряду с биологией, ученики смогут пополнить свои знания по математике, программированию и другим дисциплинам.

«Наша компания заинтересована в прогрессе отечественной науки и промышленности, в подготовке новых поколений исследователей, владеющих передовыми инструментами разработок, такими как MATLAB и Simulink. Как социально ответственный бизнес Softline активно поддерживает общественные учреждения. Поэтому когда организаторы проекта обратились к нам с просьбой о предоставлении ПО MathWorks для нужд «Школы молекулярной и теоретической биологии», мы с удовольствием пошли им навстречу. Получив доступ к богатым возможностям моделирования и вычислений в MATLAB и Simulink, ученики школы смогут экспериментировать с алгоритмами, моделями и данными, пробовать разные сценарии динамики систем», — отметил Сергей Сорокин, руководитель отдела маркетинга департамента MathWorks компании Softline.

Современное образование невозможно без использования передовых технологий. Язык технических вычислений MATLAB и среда для модельно-ориентированного проектирования Simulink включены в программы обучения ведущих вузов мира: Массачусетского технологического университета, Университета Женевы, Оксфордского университета, Гарвардского университета и многих других. В России MATLAB и Simulink в свои учебные программы уже включили большинство вузов, в том числе: МГТУ им. Баумана, Санкт-Петербургский, Новосибирский, Томский государственные и технические университеты, Уральский и Сибирский федеральные университеты.

«MATLAB позволяет сместить внимание студента с формальных манипуляций в сторону постановки задачи, поиска решений и визуализации, а также уделять больше внимания фундаментальным принципам, исследовать задачи с разных точек зрения. Это мощный и гибкий инструмент, подходящий для решения широчайшего круга вопросов как сам по себе, так и в комбинации со специализированными научными пакетами. Использование MATLAB помогло нам сделать преподавание более эффективным и интересным», — рассказал Михаил Ройтберг, заведующий лабораторией прикладной математики Института математических проблем биологии РАН.

ПО MathWorks является единой средой для исследований, анализа и моделирования в различных сферах и используется такими компаниями как Pfizer, Roche, Merrimack Pharmaceuticals, Infinity Pharmaceuticals.

Услуги Softline в области обеспечения безопасности индустрии платежных карт

Мы объявляем о выходе в сегмент аудиторских услуг по обеспечению соответствия стандартам индустрии платежных карт (PCI Data Security Standard). Данный шаг является закономерным результатом стратегии развития компании в сфере укрепления позиций на рынке информационной безопасности.

Мошенничество в сфере интернет-банкинга стоит на первом месте по объему отмываемых денег, а ущерб от взлома систем дистанционного банковского обслуживания достигает десятков миллионов рублей.

Ключевые задачи, которые ставит перед собой команда Softline, выходя на новый рынок, — это помощь компаниям, деятельность которых связана с обработкой данных платежных карт, в борьбе с финансовым мошенничеством (во многом благодаря реализации требований стандарта PCI Data Security Standard), разработка эффективной политики безопасности платежных карт, повышение доверия и лояльности к брендам своих клиентов, защита их репутации. Для наиболее эффективной и полной реализации поставленных задач Softline привлекает к проектному сотрудничеству специалистов ирландской компании Sysnet, обладающей статусом Qualified Security Assessor, который дает компании право на проведение аудита информационной системы на соответствие международному стандарту PCI DSS.

В рамках партнерского соглашения компании предложат своим российским клиентам следующие услуги:

- проведение анализа расхождений и подготовку плана исправлений для достижения соответствия требованиям стандарта PCI DSS;
- устранение несоответствий, включая проектирование процессов обеспечения ИБ, разработку организационно-распорядительной документации, а также поставку и внедрение программных и аппаратных средств защиты;
- аудит на соответствие требованиям PCI DSS;
- проведение ежеквартальных ASV-сканирований;
- тестирование на проникновение.

Microsoft BizSpark™

- Если вы частная компания, которой не исполнилось еще и 3 лет, и доход которой менее 500 000$ США;
- Если вы индивидуальный разработчик или собираетесь организовать свою компанию;
- Если вы создаете тиражируемое ПО или интернет-сервис, и ваше программное решение является основой вашего бизнеса

Присоединяйтесь к программе Microsoft BizSpark™

и получайте лицензионное программное обеспечение от Microsoft и преимущества от Softline

Присоединившись к программе BizSpark, вы получите:

- Все средства разработки, серверное и клиентское ПО Microsoft, доступное в России;
- лицензии на серверные продукты Microsoft (Windows Server, SQL Server, Office SharePoint Portal Server, System Center, BizTalk Server, Dynamics CRM) для размещения Ваших сервисов в Интернете;
- доступ к профессиональной технической поддержке Microsoft;
- доступ к уникальным ресурсам MSDN;
- поддержку в продвижении на международный рынок, а также в поиске инвесторов через BizSpark Connect;
- скидки на приобретение программного обеспечения в компании Softline;
- приоритетное рассмотрение заявки на инвестиции в проект от Softline Venture Partners.

Регистрация в программе BizSpark бесплатна!

По окончании участия участники получат возможность сохранить программное обеспечение, полученное по программе BizSpark, и приобрести подписку на обновление программного обеспечения на специальных условиях.

Softline – партнер по сообществу BizSpark №1 в России

bizspark.softline.ru

Второй год работы Softline в статусе SPLA Reseller
Наши партнеры ведут бизнес в «облаках»

Получив статус Microsoft Services Provider License Agreement (SPLA) Reseller в сентябре 2010 г., компания Softline за прошедшие два года на примере своих партнеров доказала перспективность и рентабельность облачного лицензирования в России. Сегодня более 150 компаний работают по программе SPLA благодаря информационной, лицензионной, юридической и технической поддержке Softline.

Игорь Балашов, директор по развитию бизнеса Softline, рассказывает о роли программы SPLA в развитии отечественного облачного бизнеса и перспективах предоставления услуг доступа к программным продуктам.

— Уже два года вы руководите направлением, занимающимся привлечением компаний к работе по программе лицензирования SPLA. Расскажите, что изменилось за это время в отношении к облачному лицензированию, стали ли его принципы понятнее и ближе отечественному бизнесу?

— Безусловно, облачные технологии закрепились на отечественном рынке и с каждым годом привлекают все больше компаний, которые хотели бы заниматься облачным бизнесом. В этом плане показателен опыт одного из наших SPLA-партнеров — компании «Грейт», специалисты которой провели масштабное исследование заинтересованности бизнеса (причем регионального) в облачных технологиях и получении услуг доступа к IT-решениям. По итогам исследования компания «Грейт» приняла решение выходить на рынок облачных сервисов и уже год ведет бизнес в этой сфере. То есть спрос со стороны бизнеса на облачное лицензирование, безусловно, есть, и возможность для компании закрепиться и построить работу в этом секторе IT-услуг — тоже.

Другой показательный пример — опыт компании ActiveCloud, благодаря присоединению к программе SPLA увеличившей свою прибыль на 50% и сумевшей перевести более 20% клиентов с классических услуг хостинга на облачные услуги и SaaS-сервисы за счет новых пакетных предложений сервиса и аренды ПО для СМБ-организаций. Согласно прогнозам специалистов компании, подобный перевод клиентов в среднесрочной перспективе также позволит заметно повысить прибыль ActiveCloud.

Softline предлагает максимально широкий спектр программных продуктов, что для нас означает возможность постоянно развивать свои собственные направления IaaS- и SaaS-сервисов с одним проверенным партнером. Нам также важно работать с лучшими профессионалами на рынке, и мы высоко ценим экспертизу и опыт Softline.

Юрий Самойлов,
генеральный директор DataLine

В целом, если в 2011 году, подводя итоги первого года работы Softline как SPLA-реселлера, мы констатировали наличие более 60 партнеров по этому направлению, то сегодня мы можем говорить об увеличении числа партнеров в 2,5 раза. Иными словами, благодаря поддержке Softline более 150 компаний уже предлагают своим клиентам программные продукты Microsoft, лицензируемые по программе SPLA.

— Что представляет собой лицензирование по программе SPLA? В чем его ключевое отличие от традиционной модели лицензирования, когда программный продукт или IT-решение приобретается в собственность?

— Лицензирование по SPLA — это, прежде всего, возможность удовлетворить запрос клиентов на сервисно-ориентированную модель потребления IT. Становясь SPLA-партнером, компания получает право предоставлять заказчикам услуги доступа к продуктам Microsoft и решениям на их основе. При этом от организации не требуется первоначальных инвестиций в ПО, к ней не предъявляются требования по минимуму продаж. В качестве SPLA-партнера компания лишь подписывает необходимый пакет документов и ежемесячно отчитывается за лицензии на продукты Microsoft, которые использовались в данный период для оказания услуг.

В свою очередь клиент работает с IT-решением, базирующемся на лицензируемом по SPLA ПО, на аналогичных условиях регулярной (помесячной) оплаты и без первоначальных инвестиций. Благодаря SPLA клиент получает решение оптимальной стоимости (оплата только фактического использования продукта означает, что при необходимости работа с решением может быть приостановлена, а затем возобновлена без финансовых затрат на время «простоя») и высокой масштабируемости: оно может обеспечивать работу большего или меньшего числа пользователей в зависимости от потребностей конкретной бизнес-ситуации.

— Можно ли сказать иными словами, что работа по программе лицензирования SPLA позволяет компании предлагать своим заказчикам облачные продукты и разворачивать «облака» для заказчиков?

— Да, это одна из ключевых возможностей, которые доступны компании-SPLA-партнеру. Любое «облако» — публичное, общественное, частное, гибридное — может быть развернуто благодаря программе SPLA на базе продуктов Microsoft.

SPLA-партнер, к примеру, может развернуть единое «облако» для всех своих клиентов и представить в нем SaaS-решения (например, электронную почту на базе Microsoft Exchange Server, корпоративный портал на базе Microsoft Share Point). Подобные продукты сегодня более чем востребованы: малый бизнес, всевозможные стартапы и быстро развивающиеся компании обращаются к SaaS-решениям, чтобы получить все преимущества мощного IT-инструментария за оптимальную, пропорциональную фактическому использованию ПО стоимость.

Другой пример — разворачивание более закрытых, частных или близких к тако-

Контакты

Получить дополнительную информацию о программе SPLA и принять в ней участие вам поможет Игорь Балашов, директор по развитию бизнеса Softline.

Звоните: +7 (495) 232-00-23, доб. 0158

Пишите: spla@softline.ru

Наш сайт: http://soft.softline.ru/spla/

ИТ ИНФРАСТРУКТУРА БИЗНЕСА

IT Expert

Журнал для профессионалов в области IT. На страницах журнала новости и статьи о последних технологических разработках, тестирование новых продуктов, оценки рыночной ситуации в различных сегментах IT-индустрии как в России, так и за рубежом.

АДМИНИСТРАТОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

IT Manager

Настольный журнал руководителей компаний IT-бизнеса. Каждый номер содержит актуальную информацию о событиях, успешных проектах, интервью с первыми лицами компаний, аналитику рынка и путей его развития.

НОВОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

IT News

Газета о событиях, происходящих в мире информационных технологий. Газета ориентирована на корпоративных заказчиков, руководителей, менеджеров и специалистов ИТ-компаний. Издание отражает события, происходящие в таких секторах рынка, как телекоммуникации, программное обеспечение, системная интеграция, розница, дистрибуция и др.

Онлайн-проект

it·world.ru
МИР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Проект освещает наиболее важные события дня. Ежедневные обзоры создаются по материалам самых значимых и оперативных новостных сайтов России и зарубежья, а также пресс-релизам компаний. Задача ресурса — своевременная подача объективной и достоверной информации по самым актуальным тематикам: информационные технологии, телекоммуникации, IT-бизнес, защита информации.

вым по концепции «облаков». SPLA-партнер может развернуть «облако» на собственной инфраструктуре, обособив его под конкретного клиента — представителя крупного бизнеса или государственное предприятие, предъявляющее определенные требования к хранению и обеспечению конфиденциальности информации. Если же SPLA-партнер планирует работать с компаниями конкретной отрасли или предлагать специализированные, ориентированные на конкретный бизнес решения, то благодаря SPLA он также может вынести эти решения в частное «облако».

— Какие еще возможности есть у SPLA-партнера? По каким бизнес-направлениям, наряду с развертыванием «облаков», позволяет работать программа SPLA?

— Среди наших партнеров немало ЦОДов, IT-аутсорсеров и бизнес-центров, использующих SPLA для предоставления клиентам серверов и персональных компьютеров с уже установленным на нем ПО Microsoft (например, операционной системой MS, продуктами MS Office и т. д.). Техника предоставляется по описанным выше принципам: клиент получает полностью оснащенную программным обеспечением машину во временное пользование на условиях помесячной оплаты. Так, наш SPLA-партнер группа компаний «Пилот» в рамках этого варианта работы по SPLA предоставляет своим клиентам услуги доступа к корпоративной информационной платформе, физически размещенной на серверах «Пилота» и базирующейся на продуктах Exchange, Sharepoint, SQL Server, TMG. Эта же компания предлагает сервера и рабочие станции с ПО Microsoft арендаторам в рамках проекта создания регионального (астраханского) IT-парка.

Другой варианта работы по SPLA — предоставление услуг доступа к решениям независимых разработчиков ПО (ISV). Благодаря SPLA разработчики получают возможность пополнить линейку своих предложений, добавив к коробочной версии продукта его SaaS-версию, или вывести на рынок новое IT-решение, позволив пользователям «протестировать» его в SaaS-режиме. Наш SPLA-партнер компания iSolutions таким образом предлагает клиентам облачную версию своего продукта по автоматизации склада и логистики, который изначально создавался как коробочное решение; другой наш партнер, «Новые технологии», напротив, сначала представили на рынке SaaS-версию комплексного портального решения WebEDO, а уже затем, констатировав высокий спрос на продукт, подготовили версию, доступную по традиционной модели лицензирования.

— Таким образом, практически любая компания IT-сектора может работать по программе SPLA?

— Да, именно так. Компания телеком-сектора, сервис- или интернет-провайдер, хостер, аутсорсер, системный интегратор или независимый разработчик ПО — вне зависимости от специализации и опыта работы на рынке любая организация, желающая использовать продукты Microsoft для оказания услуг своим клиентам, получает такую возможность именно благодаря программе SPLA.

При этом такая организация может использовать для оказания услуг фактически всю линейку продуктов Microsoft — список доступных по SPLA решений постоянно расширяется. Сегодня в нем значатся платформа Windows Server, продукты для обеспечения взаимодействия и совместной работы (Microsoft Exchange Server, Microsoft Lync Server, Microsoft SharePoint Server), решения для управления и обеспечения безопасности инфраструктуры (Windows System Center, Microsoft ForeFront), обеспечивающее хранение данных ПО (Microsoft SQL Server), пользовательские операционные системы и приложения (Windows 7, Microsoft Office, Microsoft Visio, Microsoft Project), а также ERP и CRM-системы. Все перечисленные продукты доступны по SPLA как в последних, самых актуальных версиях, так и в предыдущих, что повышает привлекательность предлагаемой услуги с точки зрения клиента.

— Вы упомянули, что от компании-SPLA-партнера не требуется начальных вложений в ПО и что к ней не предъявляются требования минимума продаж. В чем заключаются другие преимущества программы SPLA для работающей по ней организации?

— На мой взгляд, следует отметить такое преимущество программы SPLA, как возможность четкого планирования бюджета компании, работающей по ней. Со стороны вендора цены жестко фиксируются на достаточно длительный промежуток времени, в рамках которого SPLA-партнер может самостоятельно менять стоимость своих услуг, тем самым регулируя прибыльность компании или поощряя клиентский спрос.

Также необходимо подчеркнуть отсутствие «географических» ограничений по SPLA: услуги доступа к продуктам могут оказываться для клиентов, находящихся в любой точке мира.

Наконец, безусловное преимущество программы SPLA — это простота присоединения к ней. Для этого необходимо выполнить три простых действия. Во-первых, зарегистрировать компанию, желающую стать SPLA-партнером, в программе Microsoft Partner Network, а также на ресурсах Microsoft Pinpoint и Microsoft Hosting Community. При этом Softline как SPLA-реселлер помогает своим партнерам пройти все этапы регистрации: наши специалисты проводят подробные консультации и высылают необходимые инструкции. Во-вторых, следует заключить партнерское соглашение с корпорацией Microsoft по программе SPLA с помощью специалистов Softline. Соглашение заключается на 3 года и может быть продлено в дальнейшем. Наконец, в-третьих, необходимо заключить договор непосредственно с компанией Softline. После выполнения этих условий компания получает доступ к необходимым лицензиям и может начать развертывать «облака» и предоставлять услуги доступа к решениям на базе ПО Microsoft.

— Впереди у Softline новый год работы в качестве SPLA-реселлера, и у вас, вероятно, уже сформированы планы по развитию партнерской сети, по привлечению новых организаций к работе по SPLA. Не могли бы вы в заключение сформулировать ключевую задачу Softline на этот год? Какой главный итог вы бы хотели подвести по программе SPLA следующей осенью?

— Важно понимать, что ежегодное подтверждение статуса SPLA Reseller — это не автоматическая процедура. Подтверждение статуса требует от претендующей на него компании соответствия определенным критериям и требованиям вендора. Не все компании, однажды получившие статус SPLA Reseller, смогли в дальнейшем подтвердить его. Мы уверены, что успешность Softline на этом направлении свидетельствует о качественности поддержки, которую мы оказываем своим партнерам, является признанием компетентности и надежности Softline как SPLA-реселлера. Поэтому наша главная задача на ближайший год — продолжать помогать партнерам строить бизнес в облачном лицензировании и делать это на достойном, соответствующем представлению наших партнеров и вендоров уровне.

> Сегодня Softline обладает четырнадцатью золотыми и четырьмя серебряными компетенциями Microsoft и является одним из крупнейших партнеров корпорации в России, имея более чем семнадцатилетний опыт сотрудничества с нами. Осуществляя в качестве SPLA-реселлера всестороннюю поддержку своих партнеров, и в частности, обеспечивая их взаимодействие с Microsoft, Softline не только демонстрирует стабильное увеличение числа компаний, работающих по программе SPLA, но и способствует успешному развитию их бизнеса и, как следствие, популяризации идеи облачного лицензирования в России.
>
> Дмитрий Ильин,
> руководитель направления облачных сервисов компании Microsoft

Академия Анализа Данных

Учебно-научный центр компьютерных технологий анализа данных на *STATISTICA*

Какие задачи геологоразведки Вы научитесь решать в Академии Анализа Данных StatSoft?

- Как оценивать достоверность геологической информации
- Как проводить описательный и визуальный анализ геологических данных
- Как выявлять однородные области по средствам кластерного анализа
- Как классифицировать пробы по содержанию различных веществ с помощью дискриминантного анализа, логит регрессии, деревьев классификации, нейронных сетей
- Как справиться с большой размерностью задач геологии? Отбор значимых предикторов с помощью факторного анализа, пошаговых процедур
- Геостатистические методы оценки запасов полезных ископаемых
- Построение и исследование вариограмм
- Применение методов интерполяции: кригинг и др.
- Использование технологий нейронных сетей для анализа геологических данных
- Методы добычи данных (Data Mining) в задачах анализа геологических данных

Перейдите на новый уровень проведения исследований, пройдя обучение в Академии Анализа Данных StatSoft!

Отправьте заявку на адрес sales@statsoft.ru до 20 ноября 2012г., указав код заказа №8674110A*

и получите на обучение скидку **5%**

* Оформление заявки в указанные сроки дает возможность зафиксировать скидку на прохождение обучения в StatSoft до 01.04.2013

StatSoft® • (495) 787-77-33 • info@statsoft.ru • www.statsoft.ru

Проект по переводу контроллеров домена в ЗАО «Джи Эм-АВТОВАЗ»

В результате проекта по переводу контроллеров домена компания «Джи Эм-АВТОВАЗ» получила надежную инфраструктуру на базе Microsoft Windows Server 2008 R2, а IT-департамент — новые возможности для управления инфраструктурой.

О компании

ЗАО «Джи Эм-АВТОВАЗ» — совместное предприятие, созданное General Motors, АВТОВАЗом и «Европейским Банком Реконструкции и Развития» в 2001 году.

23 сентября 2002 г. с конвейера совместного предприятия сошел первый автомобиль Chevrolet NIVA — комфортный, надежный и безопасный российский внедорожник, завоевавший признание автомобилистов. Всего с начала производства было реализовано более 400 тыс. автомобилей Chevrolet NIVA. На сегодняшний день продажи автомобилей Chevrolet NIVA осуществляют 152 дилера в Российской Федерации, 8 дилеров и 3 дистрибьютора в странах СНГ. Основная задача предприятия состоит в том, чтобы занять место полноправного производителя высококачественных, конкурентоспособных, доступных по цене автомобилей на рынках России и стран СНГ. По состоянию на 1 января 2012 года общая численность персонала «Джи Эм-АВТОВАЗ» составляет около 1500 человек. Общая площадь СП — более 137 564 квадратных метров.

Задача

Для повышения надежности инфраструктуры необходимо было провести модернизацию, так как в качестве платформы использовался Windows Server 2003. Руководитель IT-отдела ЗАО «Джи ЭМ-АВТОВАЗ» Константин Ризаев рассказывает: «Основной целью проекта было отказаться от платформы Windows Server 2003 как продукта, вышедшего из основной фазы поддержки, минимизировать риски, отказаться от существующего сетевого адресного пространства. Для этого было принято решение обновить платформу до Windows Server 2008 R2. Партнером по проекту была выбрана компания Softline, обладающая необходимой специализацией и опытом проведения подобных проектов миграции на новые платформенные сервисы Microsoft».

Этапы проекта

На подготовительном этапе специалистами «Джи Эм-АВТОВАЗ» были созданы виртуальные машины с заранее разработанными конфигурациями, которые затем подключили и к сети для дальнейшей работы. Инженеры Департамента решений Microsoft установили на эти машины Windows Server 2008 R2 и создали резервные копии текущих контроллеров домена (бэкап виртуальных машин). Схема Active Directory была расширена до версии Windows Server 2008 R2, как необходимое условие перехода, и установлены новые контроллеры домена, сопутствующие сервисы; настроены серверные роли — DHCP и DNS.

На следующем этапе инженером Softline была протестирована репликация штатными средствами Windows Server и создана резервная копия контроллеров домена. Чтобы проверить работоспособность системы, специалист «Джи Эм-АВТОВАЗ» перевел часть рабочих станций IT-дирекции и нескольких некритичных серверов на работу с новыми контроллерами через перенастройку DNS-клиента. Мониторинг работы фокусной группы в течение суток показал, что все службы работают в штатном режиме: без проблем осуществляется аутентификация пользователей, авторизация, применение различных групповых политик. Когда все сценарии были отработаны, решение было масштабировано на всех пользователей.

Результаты

«Заказчик получил надежную инфраструктуру, основанную на современных поддерживаемых системах, снизил количество простоев, получил новые возможности управления инфраструктурой с помощью расширенных инструментов групповой политики в составе Windows Server 2008 R2, успешно мигрировал в новое адресное пространство», — сказал Павел Дугаев, руководитель группы продаж Департамента решений Microsoft компании Softline в Самаре.

«В результате проекта за счет модернизации платформы повысилась надежность системы в целом, решилась проблема с репликацией данных между существующими контролерами домена, расположенными в разных сайтах компании. Мы довольны сотрудничеством со специалистами компании Softline, поэтому продолжаем работу, реализуя следующий проект — внедрение решения «Объединенные коммуникации» на базе Microsoft Lync», — отметил Константин Ризаев, руководитель IT-отдела ЗАО «Джи ЭМ-АВТОВАЗ».

Google™ Apps for Business

Совместная работа с документами и обмен сообщениями

Google Apps – это набор сервисов, позволяющих организовать полноценную работу офиса. Защищенная и функциональная корпоративная почта, совместное редактирование документов, планирование активностей через открытые календари, голосовая связь и обмен текстовыми сообщениями – обеспечивают полный спектр возможностей для бизнеса:

Gmail

Почтовая служба с объемом до 25 Гб для каждого почтового адреса с функцией голосового чата и видеочата

Google Docs

Создание и совместная работа с текстовыми документами, таблицами, презентациями

Google Talk

Бесплатные текстовые сообщения и голосовые вызовы

Google Sites

Простое создание и редактирование веб-сайтов

Google Calendar

Личные и открытые календари: планирование и координация мероприятий, SMS-оповещения

Google Video

Хостинг видеоматериалов

Google Groups

Создание групп пользователей для общения и совместной работы над документами

Google Postini

Защита входящей и исходящей почты от спама и вирусов

- Для доступа к данным в любое время из любого места нужны компьютер или мобильное устройство, доступ в Интернет и любой браузер
- Безопасность и конфиденциальность информации (соответствие стандарту SAS 70 Type II)
- Гарантия доступности сервисов 99.9%
- Установка, обновление и поддержка ПО и серверов не нужны, это делает Google
- Техническая поддержка Google и Softline на русском и английском языках
- Простая схема лицензирования

softline®

ENTERPRISE PARTNER Google Apps

Компания Softline:

- первый и единственный авторизированный поставщик Google в России;
- оказывает помощь в настройке и развертывании сервисов Google;
- обучает администраторов и пользователей;
- помогает в миграции на Google Apps;
- проводит работы по интеграции Google Analytics с Google Apps.

cloud@softline.ru
+7 (495) 232-00-23,
8-800-100-00-23
(звонок по России бесплатный)

Более подробная информация о сервисе доступна по адресу:
cloud.softline.ru

Объединенные коммуникации из «облака»

Платформа объединенных коммуникаций Unified Communications Microsoft включает в себя три сервиса: Microsoft Exchange, Microsoft SharePoint и Microsoft Lync

Microsoft® SharePoint® 2010

На сегодняшний день Microsoft SharePoint 2010 — это лучшее из существующих решений для организации единого информационного хранилища с возможностью предоставления доступа сотрудникам к внутренним информационным процессам, средствам обмена и поиска информации, а также совместной работы с ней.

Microsoft SharePoint 2010 «из облака» — это:

- 1 ГБ места для каждого пользователя
- Централизованное хранение документов, адресная книга сотрудников
- Форумы, блоги, фотогалерея, виджеты, бизнес-аналитика
- Интеграция с AD
- Работа с файлами Microsoft Office
- Доступ к сервису из любого места при наличии подключения к интернету
- Интеграция с офисными приложениями Microsoft Office и Microsoft Exchange
- Быстрый запуск решения
- 99,9 % аптайм (доступность) сервиса с финансовыми гарантиями, обеспеченными SLA (Service Level Agreement – соглашение об уровне услуг)
- Техническая поддержка по почте и телефону 24/7

Интегрировано с Hosted Exchange 2010

За счет использования интегрированного набора функций, Microsoft SharePoint 2010 предоставляет возможность улучшить формальное и неформальное общение между сотрудниками, клиентами и партнерами. Обеспечивая поддержку совместной работы в самом широком смысле этого слова, SharePoint 2010 помогает организовывать работу новым, более эффективным способом. Основные функциональные возможности Microsoft SharePoint 2010:

- Корпоративный поиск
- Сообщества и сети
- Управление контентом
- Сайты
- Бизнес-аналитика
- Конструктор

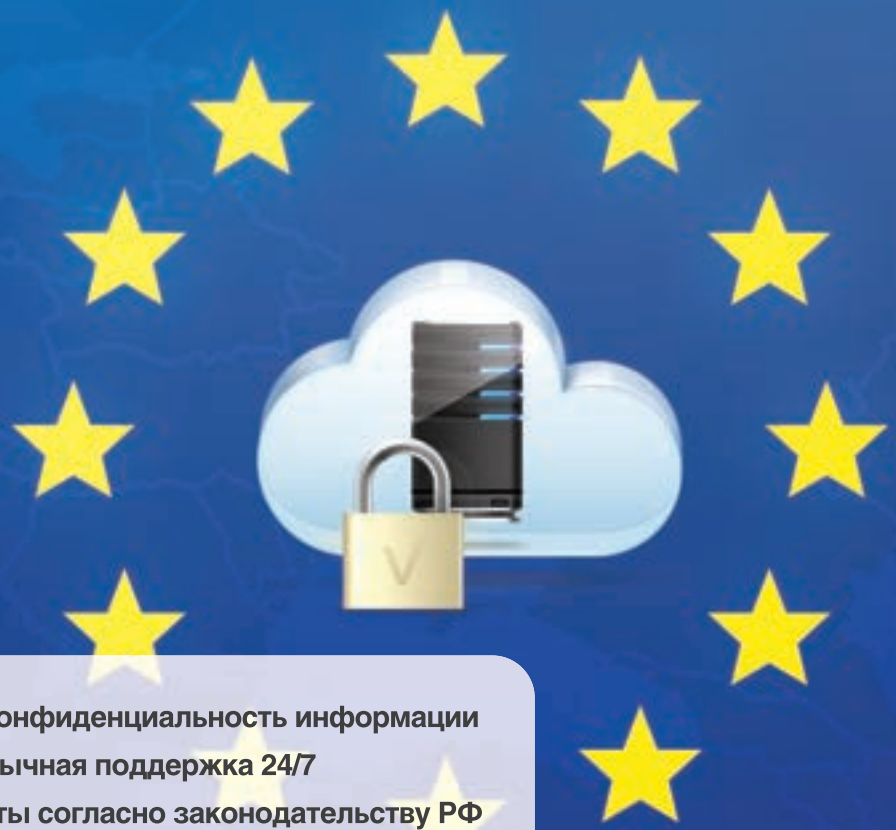
softline®

cloud.softline.ru, cloud@softline.ru
+7 (495) 232-00-23, 8-800-100-00-23
(звонок по России бесплатный)

Active CLOUD

by softline

«Облако» ActiveCloud в Европе



Полная конфиденциальность информации
Русскоязычная поддержка 24/7
Документы согласно законодательству РФ

- **Размещение ресурсов в дата-центрах Европы**

  Современные дата-центры, оборудованные по последнему слову техники. Размещение возможно в Литве, Нидерландах, Беларуси.

- **Защита конфиденциальной информации**

  Мы гарантируем защиту конфиденциальной информации клиента, а также защиту от физического изъятия.

- **Возможность организации канала «точка-точка»**

  По запросу возможно построение канала «точка-точка», что обеспечит дополнительную скорость отклика сервера и отказоустойчивость.

- **Оформление всех документов по российскому законодательству**

  Мы придерживаемся прозрачных отношений с клиентом со стороны законодательства и бухгалтерского учета. Все закрывающие бухгалтерские документы будут подготовлены во время и по стандартам учета.

- **Автоматизация, удобный интерфейс управления услугой**

  Удобный и понятный интерфейс ориентирован на клиента, все ресурсы автоматизированы.

- **Русскоязычная поддержка 24/7**

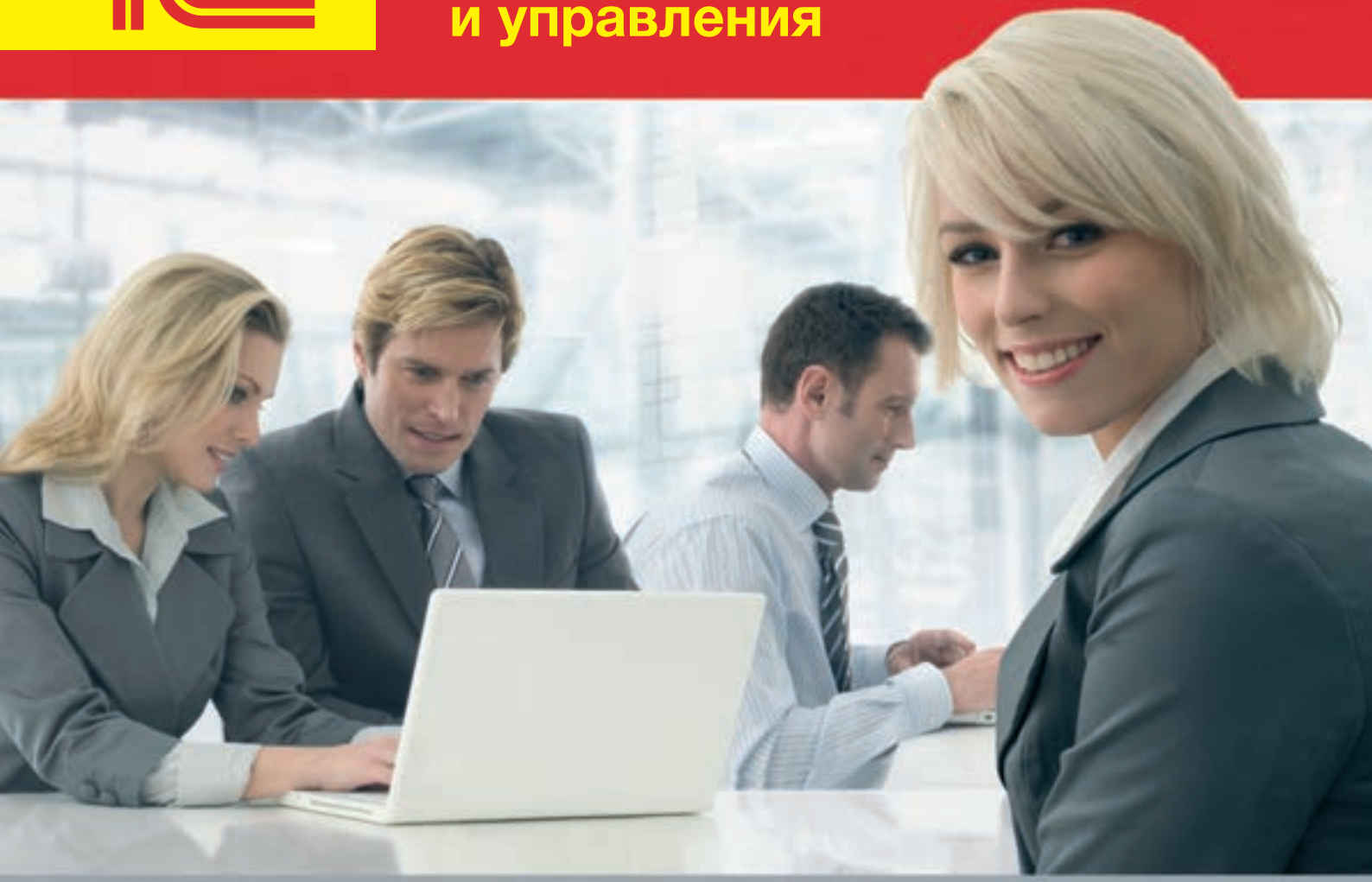
  Русскоязычная поддержка в онлайн режиме 24/7, которая готова ответить на все вопросы по эксплуатации, настройке, а также предложить полный пакет администрирования. Доступность сервиса до 99,95% с финансовой гарантией.

+7 495 988-22-62
8 800 100-22-50

ООО «АктивХост РУ». Дербеневская набережная, д. 7, стр. 9, деловой квартал «Новоспасский Двор», Москва, 115114

www.activecloud.ru эл. почта: **sld@activecloud.ru**

Комплекс решений для учета и управления



Все продукты 1С и сервис:

- **Базовые и новые программы 1С**
- **Отраслевые и специализированные решения**
- **Поддержка и обновления (ИТС)**
- **Аренда программного обеспечения**
- **Хостинг 1С - защищенная ИТ инфраструктура**

  Услуга позволит вынести корпоративную базу данных и приложения 1С на удаленный сервер и обеспечить безопасный доступ из любой точки, где есть интернет. Решение обеспечивает шифрование и конфиденциальность данных и защиту их от физического вмешательства и изъятия.

- **Выгодные пакетные предложения**

  1С + Microsoft Windows Server

  1С + Microsoft SQL Server

  1С + Microsoft Office 2010

by softline

Active CLOUD

По любым вопросам данного предложения обращайтесь к вашему персональному менеджеру в Softline или по 1C@activecloud.ru

8 800 100-22-50

WOLFRAM

В октябре в Россию приедут представители компании Wolfram Research и проведут ряд бесплатных семинаров совместно с компанией Softline.
Приглашаем вас принять участие!

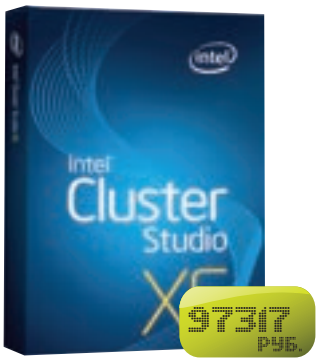
2 октября — семинар в Москве,
4 октября — семинар в Екатеринбурге,
8 октября — семинар в Казани,
9 октября — семинар в Новосибирске,
11 октября — семинар в Томске.

Основанная в 1987 году компания Wolfram Research является одной из наиболее авторитетных современных компаний по производству программного обеспечения в мире, а также активным инноватором в области научных и технических разработок. Главным продуктом компании является система *Mathematica*, стоявшая у истоков современных технических вычислений. Это постоянно совершенствующееся приложение, фактически ставшее универсальной вычислительной системой

Для участия в семинаре необходима предварительная регистрация на сайте http://seminars.softline.ru/recent-events/seminars

Дополнительную информацию о Wolfram Research вы можете получить на сайтах www.softline.ru и www.wolfram.com

Ждем вас на наших семинарах!



Intel Cluster Studio XE 2013

Пакет Intel Cluster Studio XE обеспечивает исчерпывающий набор стандартных средств параллельного программирования на языках Fortran и C/C++, а также программных моделей, которые позволяют разработчикам эффективно разрабатывать, анализировать и оптимизировать высокопроизводительные приложения для горизонтального и вертикального масштабирования и увеличения производительности для процессоров, совместимых с архитектурой Intel, в том числе сопроцессора Intel Xeon Phi.

Самое эффективное и современное масштабирование

Эволюция высокопроизводительных вычислительных архитектур, направленная на увеличение количества ядер и расширение векторов, ставит разработчиков перед необходимостью создания приложений, которые полностью используют потенциал этих инноваций и при этом удовлетворяют жестким временным срокам. Intel Cluster Studio XE содержит инструменты разработки ПО следующего поколения:

- Intel MPI Library — хорошо масштабируемая, производительная и независимая от межкомпонентных соединений библиотека MPI (интерфейса передачи сообщений);
- Intel Trace Analyzer and Collector — профилировщик производительности для коммуникаций MPI;
- Компиляторы Intel C, C++ и Fortran — лучшие компиляторы в отрасли;
- Intel MKL и Intel IPP — библиотеки оптимизированных процедур для математики и задач мультимедиа;
- Intel Threading Building Blocks и Intel Cilk Plus — модели параллельного программирования, основанные на потоках;
- Intel Advisor XE — Инструмент для потоковой обработки приложений C/C++, C# и Fortran с использованием потоковой параллелизации на главном узле кластера;
- Intel VTune Amplifier XE — профилировщик производительности и потоков, который можно активировать на каждом узле с помощью MPI;
- Intel Inspector XE — инструмент для проверки ошибок памяти и многопоточности;
- Static Analysis — средство для выявления труднонаходимых ошибок;
- Intel MPI Benchmarks — пакет исследования производительности кластеров и функций передачи сообщений.

Сравнение версий

Существует несколько пакетов, сочетающих функции компилирования, настройки и отладки приложений. Доступны однопользовательские и многопользовательские лицензии, а также скидки для корпораций, образовательных учреждений и студентов.

Ключевые особенности

Интегрированный набор инструментов для разработки высокопроизводительных приложений

Не имеющие аналогов компиляторы, параллельные модели и библиотеки с продвинутыми функциями оптимизации, обеспечивающие великолепную производительность приложений с общим доступом, распределенных и гибридных приложений для многоядерных и мультиядерных процессоров сегодняшнего и завтрашнего дня.

Высокопроизводительная библиотека MPI

Библиотека Intel MPI открывает новые горизонты в производительности, гибкости и масштабируемости для приложений, выполняемых на кластерах платформ Intel.

Компиляторы C++ и Fortran, а также мощные параллельные модели

Intel Trace Analyzer and Collector — мощный инструмент для анализа правильности функционирования и производительности MPI-приложений.

- Визуализация и анализ поведения параллельных приложений
- Предоставление статистики профилировки и балансировки нагрузок

Инструменты проверки и профилировки для ПО с общим доступом, распределенных и гибридных приложений

Компиляторы Intel C/C++ и Fortran содержат встроенные технологии оптимизации и поддержку многопоточности, которая позволяет разрабатывать код, лучше всего работающий на новейших много- и мультиядерных архитектурах Intel.

	ПАКЕТЫ	Cluster Studio XE	Parallel Studio XE	C++ Studio XE	Fortran Studio XE	Composer XE	C++ Composer XE	Fortran Composer XE
КОМПОНЕНТЫ	Intel C / C++ Compiler	•	•	•		•	•	
	Intel Fortran Compiler	•	•		•	•		•
	Intel Integrated Performance Primitives	•	•	•		•	•	
	Intel Math Kernel Library	•	•	•	•	•	•	•
	Intel Cilk Plus	•	•	•		•	•	
	Intel Threading Building Blocks	•	•	•		•	•	
	Intel Inspector XE	•	•	•	•			
	Intel VTune Amplifier XE	•	•	•	•			
	Static Analysis	•	•	•	•			
	Intel MPI Library	•						
	Intel Trace Analyzer & Collector	•						
	Rogue Wave IMSL Library							•
	Операционная система	W, L	W, L	W, L	W, L	W, L	W, L, M	W, L, M

Примечание: W — Windows, L — Linux, M — Macintosh.

Intel Parallel Studio XE 2013

Обеспечьте максимальную производительность приложений при минимальных затратах на разработку, настройку и тестирование. Intel Parallel Studio XE предоставляет разработчикам на C/C++ и Fortran инновационные компиляторы и библиотеки, проверенные модели параллельного программирования, а также совместимые и взаимодополняемые инструменты анализа.

Ведущее средство для оптимизации производительности

Intel Parallel Studio XE 2013 бесшовно интегрируется с Visual Studio и инструментарием GNU, обеспечивая высокую продуктивность при сохранении инвестиций в среду разработки. Intel Parallel Studio XE содержит следующие инструменты разработки ПО нового поколения:

- Компиляторы Intel C, C++ и Fortran — лучшие компиляторы в отрасли;
- Intel MKL и Intel IPP — библиотеки оптимизированных процедур для математики и мультимедиа;
- Intel Threading Building Blocks и Intel Cilk Plus — модели параллельного программирования, основанные на потоках;
- Intel Advisor XE — инструмент для потоковой обработки приложений C/C++, C# и Fortran;
- Intel VTune Amplifier XE — профилировщик производительности и потоков;
- Intel Inspector XE — инструмент для проверки ошибок памяти и многопоточности;
- Static Analysis — средство для выявления труднонаходимых ошибок.

Выше производительность — меньше усилий

Оптимизируйте приложения с помощью последних версий получивших заслуженное признание средств разработки Intel. Для того чтобы приложения, для которых скорость работы является критичной, максимально использовали возможности новейших Intel-совместимых процессоров, достаточно просто перекомпилировать их с новыми компиляторами Intel и перекомпоновать библиотеки.

Ключевые возможности

Популярнейшие библиотеки и компиляторы C++ и Fortran

Intel Composer XE — это ориентированный на оптимизацию инструмент разработки, включающий компиляторы Intel C++ и Fortran, а также библиотеки для математики, мультимедиа, работы с потоками и обработки сигналов.

- Компиляторы C++ и Fortran значительно быстрее аналогов и совместимы с Microsoft Visual C++ и gcc.
- Параллельные модели Intel Cilk Plus и Intel Threading Building Blocks упрощают использование преимуществ высокопроизводительных сейчас и в будущем.
- Ведущие в отрасли библиотеки Intel Math Kernel Library и Intel Integrated Performance Primitives содержат множество процедур для оптимизации и сокращения времени разработки.

Новейший инструмент работы с потоками для Linux и Windows

Intel® Advisor XE представляет собой инструмент работы с потоками для разработчиков на C, C++, C# и Fortran. Он находит сегменты кода с наибольшим потенциалом для параллелизации и выявляет критичные проблемы синхронизации.

- Сравните возможные варианты перед инвестированием во внедрение.
- Оцените прирост производительности.
- Проверьте правильность функционирования.
- Выберите вариант, обеспечивающий скорейший возврат инвестиций.

Оптимизация последовательного и параллельного кода.

Intel VTune Amplifier XE — самый высококачественный профилировщик потоков и производительности, позволяющий настроить скорость работы приложений.

- Анализируйте скорость работы на C, C++, C#, Fortran, Ассемблере и Java.
- Получайте полную информацию о производительности в «узких местах», потоках, задержках и времени ожидания, пропускной способности, взаимодействии с DirectX и многом другом.

Новые возможности

Поддержка последних версий процессоров. Intel предлагает первый набор инструментов, позволяющий максимально использовать возможности нового аппаратного обеспечения от Intel, сохраняя совместимость с более старыми версиями процессоров. Набор поддерживает такие новые процессоры, как Intel AVX2, TSX и FMA3.

Получение повторяемых результатов. Обретите уверенность в возможности повторения результатов. Увеличьте надежность вычислений с плавающей точкой с помощью библиотеки Intel Math Kernel, специальной поддержки OpenMP и Intel Threading Building Blocks.

Руководство по оптимизации на C++. Если вы не являетесь экспертом в области оптимизации, то это руководство вам очень пригодится. Оптимизируйте приложения с помощью простого и быстрого процесса, состоящего из 5 шагов.

Поддержка стандартов Fortran и C++ — Intel Fortran поддерживает популярные возможности стандарта F2003, а также ключевые элементы стандарта 2008, в том числе секционированные массивы. Этот релиз также поддерживает стандарт C++11.

Находите и устраняйте больше ошибок с помощью Intel Inspector XE. Этот инструмент предоставляет эффективные методы для обеспечения надежности и производительности приложений C, C++, C#, Fortran, Java и MPI. Новая функция анализа роста кучи предлагает новые способы обнаружения утечек памяти.

Дополнительные данные профилировки, более легкие для использования. Intel® VTune™ Amplifier XE стал удобнее и предоставляет дополнительные данные. Его большая пропускная способность и функции анализа доступа к памяти позволяют тратить меньше времени, пытаясь разобраться в запутанной статистике производительности, и уделять больше времени разработке.

Программно проверяемые указатели. Этот новый инструмент диагностики, основанный на компиляторе, позволяет выявлять код, который обращается к адресам памяти, находящимся за пределами выделенной области. Тем самым программное обеспечение становится более устойчивым, и становится проще обнаружить ошибки, связанные с нарушением целостности оперативной памяти.

Контакты

За дополнительной информацией обращайтесь к менеджеру компании Softline Анне Курьяновой.

Пишите: AnnaKuri@softline.ru

Звоните: +7 (473) 250-20-23, доб. 3266

Переводчик для небольших компаний

PROMT SMB — новое решение по переводу в интранет-сетях небольших компаний. Новейшие информационные технологии по доступной цене!

Зачем малому бизнесу решение по переводу?

В современном мире даже у небольших компаний есть потребность в работе с текстами на иностранных языках. Например, менеджерам нужно переписываться с зарубежными клиентами или поставщиками, юристу — ориентироваться в законодательстве других стран, секретарю — выбирать гостиницу и покупать билеты для командировок и т. д. Если они будут переводить всю необходимую информацию вручную, даже используя электронный словарь или обращаясь к online-сервису, процесс будет слишком медленным, неудобным, без гарантии качества. В таких случаях снимает проблему развертывание бюджетного решения по переводу в компании и предоставление доступа к корпоративному переводчику всем ключевым сотрудникам.

Увеличиваем эффективность

Численность малых и средних предприятий в России — около полутора миллионов. Для многих из них использование информационных технологий становится существенным фактором повышения эффективности бизнеса. Однако, по причине ограниченности ресурсов, таким компаниям необходимы недорогие и простые IT-решения, в том числе по переводу.

Специально для них было разработано решение PROMT SMB. Это привлекательное по цене и простое в использовании серверное решение позволяет подключить до 10 рабочих мест с возможностью одновременной работы для 5 человек.

Возможности

PROMT SMB полностью отвечает запросам клиентов по работе с документами и сайтами на иностранном языке, существенно облегчает переписку с зарубежными партнерами, клиентами и поставщиками. Для успешной работы компании всегда необходимо иметь самую свежую, достоверную и полную информацию, анализ которой позволяет оперативно реагировать на изменения рынка. Решение PROMT SMB предоставляет возможность небольшим предприятиям решать текущие бизнес-задачи оперативно и с минимальными затратами, а также дает компаниям дополнительное конкурентное преимущество. Сочетание этих качеств обеспечивает компании рост бизнеса без слишком больших инвестиций.

Решение позволяет быстро и качественно переводить:

- входящую и исходящую корреспонденцию;
- документы внутри корпоративной сети;
- информацию на интернет-сайтах.

Интеграция в другие приложения

- Встраивание с помощью плагинов функций перевода непосредственно в приложения Microsoft Office 2000-2010 (Outlook, Word, Excel, PowerPoint, FrontPage), а также перевод PDF-документов и файлов в формате OpenOffice (Org.writer).
- Перевод web-страниц в окне браузера с помощью встроенных кнопок для Microsoft Internet Explorer, Mozilla Firefox, Opera и Google Chrome.
- Перевод текстов с помощью комбинации «горячих» клавиш в любом Windows-приложении.

Преимущества:

- **быстрота развертывания,**
- **простота использования и легкость в обучении,**
- **защита корпоративных данных от утечки к третьим лицам,**
- **удаленный доступ: автоматическим переводом сотрудники могут пользоваться как в центральном офисе, так и в филиалах,**
- **а главное — быстрый и качественный перевод документов.**

Акция!

При заказе решения до 30 ноября 2012 года по ключевому слову «Softline, сентябрь» вы получаете скидку 30 %.

Подробности — у менеджеров Softline и PROMT.

Моментальный грамотный перевод: оперативно и с минимальными затратами

Поддерживаемые языки (на выбор покупателя):

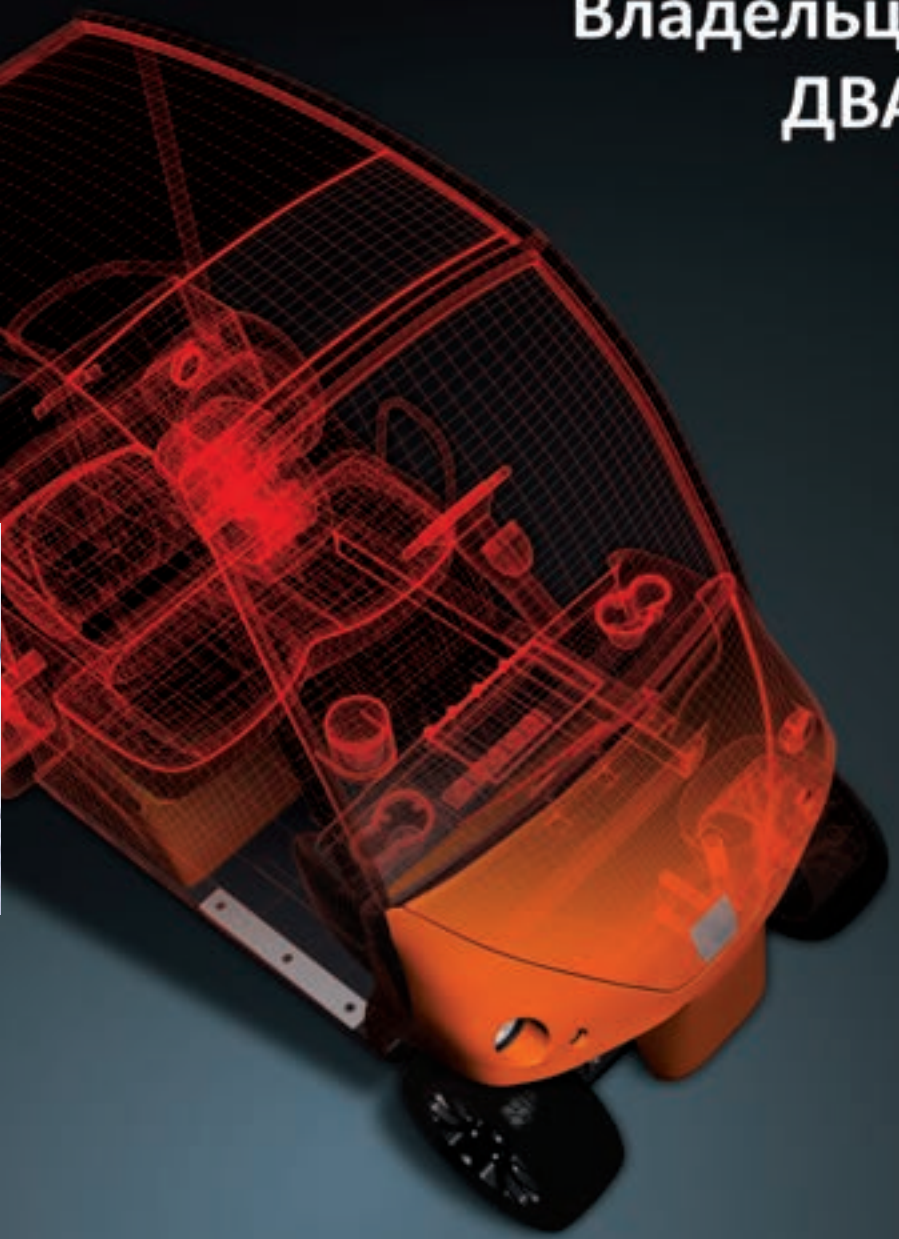
- **английский,**
- **русский,**
- **немецкий,**
- **французский,**
- **испанский,**
- **итальянский,**
- **португальский,**
- **болгарский,**
- **турецкий,**
- **украинский,**
- **латышский,**
- **казахский,**
- **польский,**
- **китайский (упрощенный, традиционный).**

CorelCAD

powered by ARES®

COREL

Владельцам CorelDRAW в ДВА раза дешевле!

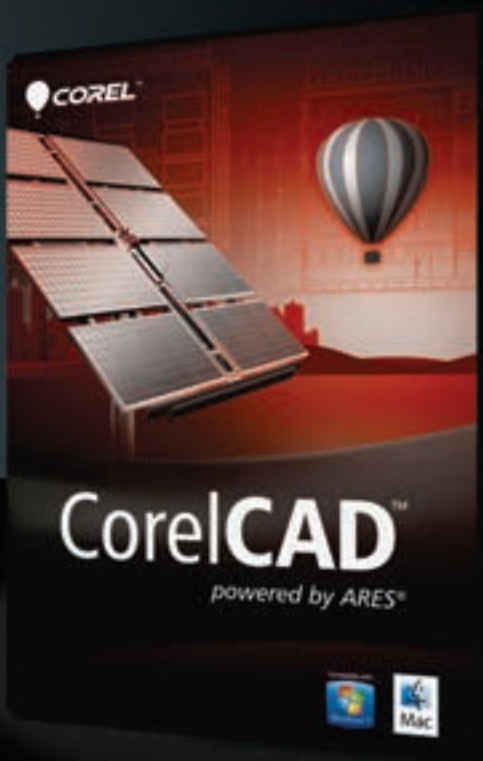


Только до 29 октября
вы можете приобрести:

CorelDRAW X6 + CorelCAD за **26900 ₽**
экономия до 30%*

Лицензии Upgrade CorelCAD за **9500 ₽**
экономия до 50%*

Всем, кто приобретет CorelCAD, новая версия **2.0 в подарок!****



Уже сейчас все легальные пользователи CorelDRAW версий X4 и выше могут воспользоваться правом на покупку CorelCAD по цене апгрейда, экономя при этом более 50% от цены полной коммерческой версии!

Если у нас нет программы CorelDRAW, предлагаем воспользоваться специальным предложением и приобрести обе программы, экономя при этом более 30%

* Указаны ориентировочные розничные цены.
** Участие в данной акции предоставляет право на бесплатный переход на версию CorelCAD 2.0

Семейство Adobe Acrobat XI

Работать с PDF-файлами стало еще проще: приложения семейства Adobe Acrobat XI позволяют создавать, редактировать и подписывать PDF-документы и формы. Программное обеспечение Acrobat XI доступно в двух версиях: Acrobat XI Pro и Acrobat XI Standard.

Лучшие функции

1. Интеграция с Microsoft. Используйте все возможности, которые перед вами открывает поддержка Microsoft Windows 7 и 8, применяйте функции Acrobat, доступные непосредственно на ленте команд Acrobat в приложениях Office, и повышайте эффективность работы с SharePoint и Office 365 в операционных системах Windows и Mac OS.
2. Упрощенное управление ПО. Упрощайте развертывание и обновление при помощи кумулятивных пакетов исправлений согласно прогнозируемому графику. Развертывание и управление может осуществляться при помощи Microsoft SCCM/SCUP, GPO и Apple Remote Desktop.
3. Безопасность. Снижайте вероятность атак через PDF-файлы благодаря множеству встроенных средств защиты и обеспечения безопасности, включая изолирование программной среды.
4. Защита документов. Защищайте корпоративную информацию при помощи настроек защиты документов по умолчанию или автоматизированных действий — задач безопасности, которые будут безо всякого труда применяться всеми пользователями при работе с PDF-файлами.
5. Упрощенные рабочие процессы. Работайте эффективнее, предоставляя конечным пользователям интуитивно понятные средства редактирования PDF-файлов, преобразования PDF в форматы Office, создания форм и портфолио PDF. Acrobat XI — это комплексное решение для работы с PDF-документами и формами, которое делает развертывание и обслуживание ПО проще.

Очевидная экономия средств

Приложение Acrobat XI содержит функции, которые устраняют необходимость установки других программ и повышают продуктивность.

- Экономия за счет корпоративного лицензирования. Adobe предлагает несколько вариантов корпоративного лицензирования, которые снижают не только затраты на закупку, но и расходы на развертывание ПО и управление лицензиями.
- Минимизация эксплуатационных затрат. Упрощенное развертывание и прогнозируемый график выпуска обновлений помогают снизить внутренние расходы.
- Повышение продуктивности. Ускоренное рецензирование и электронное подписание документов, а также усовершенствованные средства создания форм помогают работать более эффективно.
- Возможность отказаться от ненужных программ. Широкая функциональность программного обеспечения Acrobat позволяет использовать его вместо множества разных приложений, включая системы распознавания текста, совместной работы, создания пакетов файлов, работы с формами и архивации.

Adobe Acrobat XI Standard

С программным обеспечением Adobe Acrobat XI Standard пользователи получают надежные комплексные средства для создания, редактирования и подписания PDF-документов, а IT-специалисты — надежные инструменты, которые помогают совершенствовать безопасность и упрощают управление ПО. Простота развертывания обеспечивается благодаря поддержке Microsoft SCCM/SCUP. Используйте все возможности, которые перед вами открывает поддержка Microsoft Windows 7 и 8, а также интеграция с Microsoft Office и SharePoint.

- Преобразование файлов PDF. Установите панель инструментов Acrobat для популярных приложений Microsoft и браузеров. Это позволит быстро преобразовывать документы и web-страницы в высококачественные файлы PDF, а также создавать документы PDF из любого настольного приложения, поддерживающего печать.
- Экспорт файлов PDF. Преобразуйте файлы PDF в документы Microsoft Word и Excel с сохранением форматирования.
- Редактирование файлов PDF. Исправляйте и перекомпоновывайте текст или обновляйте изображения при помощи нового удобного интерфейса — вносите изменения прямо в файлы PDF.
- Слияние файлов в один документ PDF. Просматривайте документы, а затем объединяйте их в один файл.
- Электронное подписание документов. С легкостью подписывайте документы и передавайте их на подпись другим пользователям.

Adobe Acrobat XI Pro

Adobe Acrobat XI Pro — это комплексное решение для работы с PDF-документами и формами для пользователей и упрощенное развертывание и управление для IT-специалистов. Улучшенная защита приложений, поддержка автоматизированных средств развертывания, а также прогнозируемый график выпуска обновлений с кумулятивными пакетами исправлений — все это помогает снизить затраты и объем работ на управление ПО для работы с PDF. Новые инструменты редактирования PDF, расширенные функции экспорта в PDF и тесная интеграция с Microsoft Office помогают пользователям работать более продуктивно.

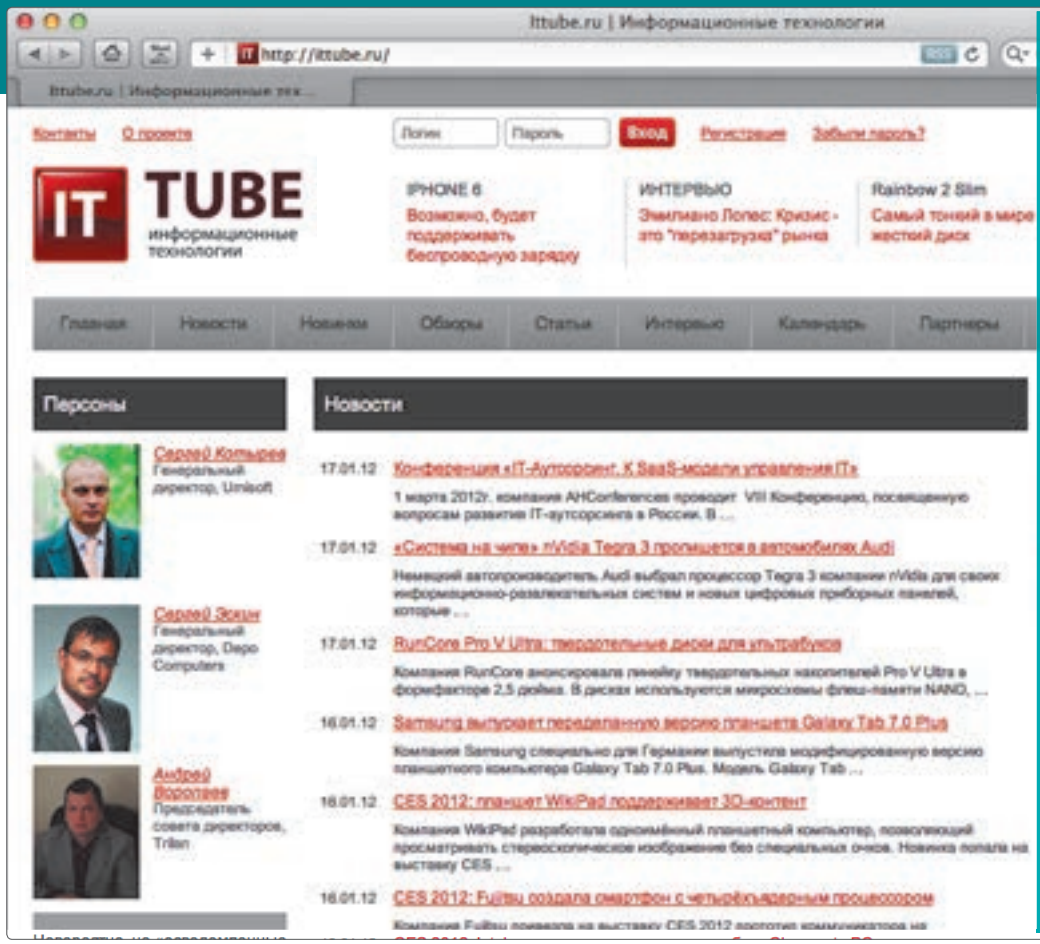
CERTIFIED RESELLER Gold

CERTIFIED RESELLER Education Gold

Центр компетенций Adobe: adobe@softline.ru

Наш сайт: http://adobe.softline.ru

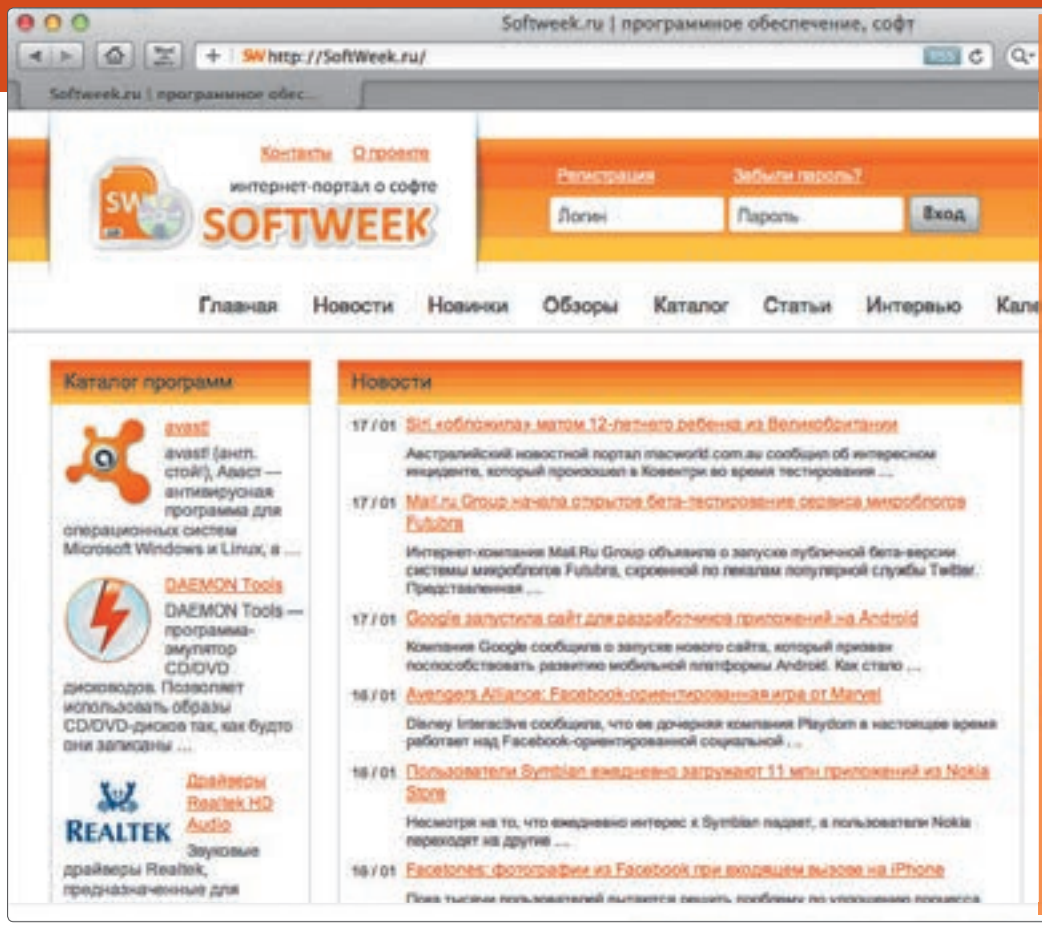
Интернет-портал гаджетов ittube.ru



- Новые гаджеты
- Освещение ключевых событий
- Интервью с экспертами
- Рекомендации
- Каталог производителей и устройств
- Календарь событий

Email: info@ittube.ru
Тел.: +7 (495) 565-33-65
125373, Москва, ул. Героев Панфиловцев, д. 42, к. 2

Интернет-портал о софте SoftWeek.ru



- Свежие релизы
- Сравнительный анализ ПО
- Персоналии
- Обзоры
- Конференции
- IT-словарь

Email: info@ittube.ru
Тел.: +7 (495) 565-33-65
125373, Москва, ул. Героев Панфиловцев, д. 42, к. 2

Radmin 3.4

Radmin — одна из лучших и самых известных программ удаленного управления компьютерами для платформы Windows. Вы можете подключаться к удаленным компьютерам как по локальной сети, так и через Интернет из любой точки мира. Radmin позволяет полноценно работать на удаленном компьютере в режиме реального времени, как будто вы сидите непосредственно перед его экраном и используете его клавиатуру и мышь.

Решаемые задачи

Поддержка пользователей и системное администрирование

Сотрудники компании могут оперативно получать необходимую техническую помощь, что сокращает время их простоя. С помощью Radmin можно снизить издержки и повысить эффективность не только IT.отдела, но и всей компании.

Удаленная работа

С Radmin вы можете управлять домашним или офисным компьютером удаленно из любой точки мира, где есть доступ в Интернет, будь то отель или интернет.кафе.

Техническая поддержка клиентов

Сотрудники службы технической поддержки могут удаленно решать проблемы и настраивать программное обеспечение на компьютерах клиентов.

Дистанционное обучение и проведение вебинаров

Radmin позволяет организовать дистанционное обучение сотрудников компании, студентов или учеников, а также проводить вебинары и online.демонстрации.

Наименование	Код Softline	Цена, руб
Radmin 3.4 Стандартная лицензия (на 1 компьютер)	1113F.. AMATECHSL .	1250
Radmin 3.4 Пакет из 50 лицензий (на 50 компьютеров)	1114F.. AMATECHSL .	38000
Radmin 3.4 Пакет из 100 лицензий (на 100 компьютеров)	1115F.. AMATECHSL .	63500

Режимы соединения

Управление. Полное управление удаленным компьютером: пользователь видит его экран и может управлять его клавиатурой и мышью.

Просмотр. Наблюдение за происходящим на экране удаленного компьютера.

Telnet. Управление компьютером в режиме командной строки.

Передача файлов. Копирование файлов на удаленный компьютер с локального и наоборот. Поддерживается докачка файлов при прерванном копировании.

Выключение. Выключение и перезагрузка удаленного компьютера.

Intel AMT. Включение и выключение удаленного компьютера, управление его BIOS, управление загрузкой операционной системы и др.

Текстовый и голосовой чат. Общение с другими пользователями.

Система безопасности

- Защита всех передаваемых данных.
- Индивидуальные права доступа для каждого пользователя.
- Поддержка протоколов аутентификации Windows NTLMv2/Kerberos и службы каталогов Active Directory.
- IPфиль.трация.
- Надежная защита от подбора пароля.

Надежность

Radmin не дает сбоев, даже если работает непрерывно в течение года. Это подтверждают как результаты тестирования, так и отзывы пользователей.

Совместимо с Windows 7.

SCAD SOFT
www.scadsoft.com

ИНТЕГРИРОВАННАЯ СИСТЕМА **АНАЛИЗА КОНСТРУКЦИЙ «SCAD Office»**

СОСТАВ СИСТЕМЫ

SCAD — расчетная система конечно-элементного анализа конструкций, ориентированная на решение задач проектирования зданий и сооружений достаточно сложной структуры, где основные трудности представляет определение напряженно-деформированного состояния конструкции.

ФОРУМ — препроцессор, служащий для формирования укрупненных моделей и импорта данных из архитектурных систем.

КРИСТАЛЛ — расчет и проверка элементов стальных конструкций по СНиП II-23-81*, СП 53-102-2004, СП 16.13330.2011, ДБН В.2.6-163:2010

АРБАТ — подбор арматуры и экспертиза элементов железобетонных конструкций по СНиП 52-01-2003, СП 52-101-2003, СНиП 2.01.07-85.

КАМИН — экспертиза элементов каменных и армокаменных конструкций по СНиП II-22-81, СНиП 2.01.07-85.

МОНОЛИТ — проектирование монолитных ребристых железобетонных перекрытий.

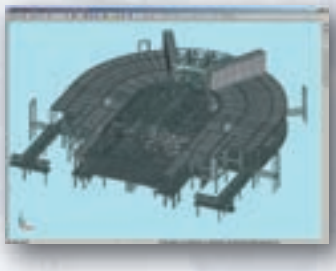
КОМЕТА — расчет и конструирование узлов стальных конструкций.

КРОСС — расчет коэффициентов постели фундаментных плит на упругом основании.

ВЕСТ — расчет нагрузок по СНиП и ДБН «Нагрузки и воздействия».

КОНСТРУКТОР СЕЧЕНИЙ — формирование произвольных сечений из стальных прокатных профилей и листов.

КОНСУЛ — формирование сечений, исходя из теории сплошных стержней.



ТОНУС — формирование сечений, исходя из теории тонкостенных стержней.

СЕЗАМ — поиск сечения типа «коробка», «двутавр» или «швеллер», близкого по характеру заданному.

ЗАПРОС — расчет элементов оснований и фундаментов по СНиП 2.02.01-83*, СП 50-101-2004, СП 22.13330.2011, ДБН В.2.1-10- 2009

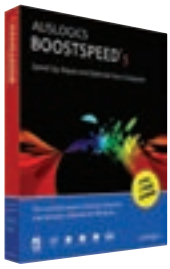
ДЕКОР — расчет и проверка элементов деревянных конструкций по СНиП II-25-80, СП 64.13330.2011

ОТКОС — определение коэффициента запаса устойчивости откосов и склонов.

КОКОН — электронный справочник для определения коэффициентов концентрации напряжений.

КУСТ — электронный расчетно-теоретический справочник инженера-проектировщика.

Группа компаний «SCAD Soft»
Телефоны: +7 (499) 267-40-76, +38 (044) 249-71-91. www.scadsoft.ru www.scadhelp.com



Auslogics BoostSpeed 5

Пакет утилит, предоставляющий мощные и эффективные средства для детальной настройки системного реестра, ускорения работы интернетсо.единений, оптимизации и профилактических действий в Microsoft Windows.

Новые возможности

Удобная навигация. Новый интерфейс упрощает работу с программой. Основные задачи — очистка дисков, исправление ошибок в реестре, а также дефрагментация файлов — решаются очень быстро.

Восстановление файлов и поиск ошибок. Программа восстанавливает любые файлы, удаленные с жесткого диска, USB.накопителя или карты памяти цифровой камеры. Функция предварительного просмотра помогает быстро найти и «вернуть к жизни» именно то, что нужно. Утилита Disk Doctor проверяет жесткий диск на наличие ошибок в файловой системе, контролируя состояние винчестера и предотвращая потерю данных.

Обзор дисков. Функция Disk Explorer помогает контролировать использование дискового пространства, подсказывая, какие папки, файлы и типы файлов занимают больше всего места на жестком диске. Список «Top.100 файлов» отображает самые крупные документы на ПК.

Основные достоинства

- Легкая очистка дисков, удаление временных файлов и дубликатов.
- Удобная дефрагментация жестких дисков.
- Быстрое включение и выключение компьютера.
- Восстановление случайно удаленных файлов.
- Надежное удаление информации с жесткого диска без возможности восстановления.
- Возможность управлять запущенными процессами и деинсталлировать установленное ПО.

Ключевые функции

Продукт включает порядка 20 утилит для оптимизации производительности компьютера. Лицензия позволяет устанавливать BoostSpeed на трех компьютерах одновременно.

Работа с дисками. Для освобождения пространства на диске программа очищает компьютер от дубликатов файлов и ненужных программ. Новая версия популярного дефрагментатора Auslogics Disk Defrag 3 позволяет сделать процесс обновления и оптимизации логической структуры диска более эффективным.

Полезные советы по настройке. Благодаря функции под названием «Советчик» BoostSpeed 5 анализирует состояние компьютера и дает рекомендации по повышению производительности и безопасности. Программа включает утилиту с более чем 280 различными опциями для быстрой и удобной настройки Windows согласно нуждам и предпочтениям пользователя.

Оптимизация интернетсо .единения. Встроенный Internet Optimizer увеличивает скорость закачки файлов и загрузки сайтов.

Защита личной информации. Благодаря утилите Track Eraser никто не узнает, какие сайты пользователь просматривал на своем ПК, какие файлы открывал и какие приложения запускал. Программа скрывает историю работы с сайтами, предотвращая возможность утечки конфиденциальной информации.

Системные требования

- Windows 7/ 2008/ Vista/ 2003/ XP (32 .и 64бит ные версии);
- 50 МБ на жестком диске;
- 256 МБ RAM.

Тираж: 20 000. Объем – до 100 полос

Ежемесячный деловой журнал **«ВРЕМЯ ИННОВАЦИЙ»**

посвящен вопросам развития инновационной деятельности в сегментах экономики страны.

Главное назначение журнала Редакция видит в оказании информационной поддержки всем участникам инновационных процессов, идущих в России.

Редакция ведет переговоры о проведении на информационных площадках Москвы и регионов большого числа мероприятий: «круглых столов», конференций, выставок с целью поддержки рекламодателей журнала и расширения их возможностей для налаживания прямых деловых контактов.

Распространение журнала: подписка, адресная рассылка (адресная база Москвы и 69 регионов), адресная доставка (Ассоциации, Союзы, крупные строительные, производственные и транспортные компании, бизнес-центры, научные организации, архитекторы и дизайнеры Москвы, бюджетные организации), активное распространение на Московских и региональных выставках, форумах, конгрессах, конференциях, и других мероприятиях с присутствием целевой аудитории.

Учредители журнала:
ОАО «Московский ИМЭТ»
Редакция.

Русская версия MapBasic 11

MapBasic для Windows 2000/ XP/Vista/7 — язык программирования геоинформационной системы MapInfo Professional. MapBasic позволяет разрабатывать приложения, расширяющие стандартные возможности MapInfo. Возможность вызова DLL и других программ позволяет создавать сложные специализированные приложения с использованием языков программирования высокого уровня. MapBasic содержит около 400 операторов и функций. Имеется возможность разработки приложений на языках VB.NET, C# и других языках платформы .NET. Для тиражирования приложений можно использовать MapInfo RunTime.

MapInfo Professional 11

MapInfo Professional для Windows 2000/XP/Vista/7 — полнофункциональная геоинформационная система (профессиональное средство для создания, редактирования и анализа картографической и пространственной информации). Интегрируется в качестве клиента в распределенные информационные системы на базе серверов: Microsoft SQL, Oracle, Informix, DB2, Sybase и другие. Для разработки специализированных приложений используется язык программирования MapBasic. ГИС MapInfo Professional полностью русифицирована.

Сферы применения. Земельный, лесной кадастр и кадастр недвижимости, градостроительство и архитектура, телекоммуникации, добыча и транспортировка нефти и газа, электрические сети, экология, геология и геофизика, железнодорожный и автомобильный транспорт, банковское дело, образование, управление.

Работа с данными в форматах AutoCAD (DXF, DWG); ESRI (E00, SHP); Intergraph/ MicroStation Design (DGN); EMF; WMF. Растровые изображения в форматах BMP, ECW, EMF, GIF, GRC, JPEG, JPEG2000, MrSID, PCX, PNG, PSD, TGA, TIF, GeoTIFF и др.

Подключение внешних баз данных — прямой доступ к пространственным данным СУБД Oracle, Microsoft SQL 2008, PostGIS, а также работа со всеми СУБД через ODBC.

MapInfo MapXtreme

Программное обеспечение MapInfo MapXtreme 7.0 и MapInfo MapXtreme Java предназначено для создания настольных ГИС%приложений и геоинформационных систем в Интернете/интранете. Серверы пространственных данных, разработанные с помощью MapInfo MapXtreme 7.0/Java, обеспечивают обслуживание неограниченного количества сетевых пользователей.

Единая платформа для разработки настольных, а также Интернет/интранет.приложений — одно из основных достоинств MapXtreme 7.0, существенно упрощающее разработку и сопровождение программного продукта.

Программное обеспечение MapXtreme включает в себя SDK — инструментарий разработчика и готовые web.сервисы пространственных данных, работающие по стандартным протоколам WMS/WFS.

Единый инструментарий разработки MapXtreme 7.0 предоставляет возможность совместного использования разработанных библиотек как в настольных, так и в сетевых приложениях.

MapXtreme 7.0 SDK спроектирован на основе платформы Microsoft .NET и позволяет использовать все языки программирования, совместимые с .NET Framework. Высокая скорость и качество разработки приложений достигается за счет полной интеграции MapXtreme SDK со средой Visual Studio .NET.

Используя MapXtreme 7.0 и возможности платформы .NET Framework, можно создавать картографические web.сервисы и интегрировать их в распределенную архитектуру своей системы. Для работы с пространственными данными MapXtreme 7.0 содержит web.сервисы, взаимодействующие по протоколам WMS/ WFS. MapXtreme 7.0 обеспечивает генерацию тайлов, работу с картами Google и Bing. Применение стандартных протоколов позволяет существенно сократить затраты на внедрение и интеграцию приложений, разработанных на основе MapXtreme 7.0, в существующую ITи.нфраструктуру компании.

MapInfo MapXtreme Java 4.8.2

MapXtreme Java предназначен для создания геоинформационных систем в Интернете/интранете под управлением различных ОС. Работает со всеми промышленными СУБД. Обеспечивает непосредственный доступ к пространственной информации, хранящейся в Oracle 9i и выше. Совместим с web.серверами, поддерживающими J2EE.сервлет.контейнерную спецификацию (Apache Tomcat, Bea WebLogic, IBM WebSphere, Sun One, JRun и другие). Имеет развитый механизм тематического картографирования. Предоставляет большой выбор базовых шаблонов и апплетов.

MapXtreme 7.0 предоставляет разработчику все основные функции современных геоинформационных систем. Особый интерес представляют развитые средства тематического картографирования, пространственные запросы, а также прямой доступ к пространственным данным в Oracle и Microsoft SQL Server 2008.

Соответствие MapXtreme 7.0 ITстан дартам. Программное обеспечение MapXtreme отвечает требованиям стандартов OpenLS, GML, WMS, WFS, Microsoft.NET, ASP.NET, ADO.NET, SQL3 .и др.

Эффективный доступ к данным. MapXtreme 7.0 поддерживает работу с широким набором атрибутивных и пространственных источников данных, в качестве которых могут выступать СУБД и файлы различных форматов (например, MapInfo TAB, ESRI Shapefiles).

Совместимость

Базы данных: Oracle; SQL Server 2008; поддержка протоколов ADO.NET, ODBC.

Средства разработки: Microsoft .NET Framework 2.0 и выше; Visual Studio.NET 2005.

Поддержка стандартов: WMS/WFS,GML; Microsoft .NET; SQL3..

Операционные системы: Windows 2000, XP, 2003.

Особенности MapInfo MapXtreme Java

- работает под управлением операционных систем UNIX, Linux, FreeBSD, Microsoft Windows;
- готовый, легко настраиваемый и управляемый WMScep вис;
- генерация карт в любых растровых форматах, в том числе WBMP и SVG.

Компания ЭСТИ МАП

Официальный представитель Pitney Bowes Software Inc. в России и СНГ

ЭСТИ МАП

Тел.: +7 (495) 6277637, ..
+7 (495) 6277649..

Email: . sales@mapinfo.ru
estim@mapinfo.ru;.
http://www.mapinfo.ru

Журнал
не только про атом...

www.proatom.ru

Подписка принимается с любого месяца!

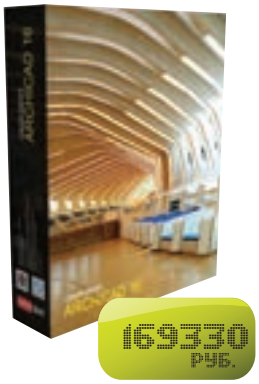
E-mail: info@proatom.ru, pr@proatom.ru, dir@proatom.ru.
Тел.: (812) 764-3712, 438-3277, 958-9004. **Тел./факс** (812) 764-3712

PROATOM

атомная стратегия XXI

Graphisoft ArchiCAD 16

BIM-компоненты на кончиках ваших пальцев



Одна из популярнейших систем автоматизированного архитектурно-строительного проектирования, реализующая технологию информационного моделирования зданий (BIM). Работая с объемной моделью здания, проектировщики детально прорабатывают проектное решение и сводят число ошибок к нулю. В любой момент можно получить согласованные между собой чертежи поэтажных планов, разрезы, фасады, точные спецификации по проекту, презентационные материалы, подготовить задания в смежные отделы. ArchiCAD — это современные технологии, работающие на вас.

Новые возможности

Анализируя функционал ArchiCAD 16, вы, без сомнения, обратите внимание на новейший инструмент Морф (Morph) для объемного концептуального проектирования и на уникальную систему по созданию и поиску пользовательских объектов (BIM-компонентов), а также по обмену ими. А новые встроенные возможности анализа энергетической эффективности проекта превращают ArchiCAD в одно из лучших решений на рынке САПР для создания экологических BIM-проектов.

Свободные формы

Архитектура всегда идет рука об руку с развитием строительных технологий, опираясь на три закона Витрувия: прочность, польза, красота. Эти три принципа можно обнаружить в любом значимом архитектурном объекте: и в классических сводах исторических зданий, и в современных органических формах. В ArchiCAD 15/16 существенно расширены проектные возможности BIM-инструментов: новые инструменты Оболочка (Shell) и Морф (Morph) позволяют моделировать широкий спектр архитектурных объемов свободных форм как для исторических, так и для современных зданий!

FC-интерфейс и принципы открытого взаимодействия с инженерами, поддержка 64-битных операционных систем (в первую очередь Mac OS) и улучшение параметрических библиотек объектов — все это вы найдете в новой версии.

Ключевые преимущества ArchiCAD

Мультиплатформенное решение

ArchiCAD поддерживает как распространенную платформу Windows, так и популярную среди творческих людей платформу Mac OS. Вы просто выбираете наиболее удобное для вас решение, а ArchiCAD всегда будет с вами.

Информационное моделирование зданий (BIM)

Все данные по проекту собираются в единой согласованной базе, из которой затем исходит согласованная и взаимосвязанная информация: чертежи, спецификации, визуализация и задания смежникам.

Сложные архитектурные формы

Теперь никаких ограничений в формообразовании — новые инструменты Оболочка (Shell) и Морф (Morph) позволяют моделировать широкий спектр архитектурных объемов свободных форм как для исторических, так и для современных зданий!

Уникальные открытые технологии взаимодействия проектировщиков

ArchiCAD позволяет группе проектировщиков одновременно работать с одной моделью здания (используя ArchiCAD как единое решение), а также поддерживает открытый формат IFC для динамической связи BIM-модели ArchiCAD с другими современными системами проектирования: Tekla Structures, Revit Structure и MEP, ETABS, Green Building Studio, ECOTECT и другими. Это в разы ускоряет процесс создания и согласования проектного решения.

Сервисный контракт

Позволяет работать на самых современных версиях ArchiCAD и страхует ключ защиты от краж, поломок и прочих непредвиденных случаев. Это наиболее выгодное вложение денег в лицензионное программное обеспечение.

Altium Designer

Altium Designer представляет собой систему сквозного автоматизированного проектирования электронных средств на базе печатных плат и ПЛИС. Принцип сквозного проектирования подразумевает передачу результатов одного этапа проектирования на следующий в единой проектной среде (Altium Designer использует интегрированную платформу Design Explorer).

Altium Designer состоит из нескольких структурных модулей и охватывает основные этапы проектирования РЭС: разработку электрических схем, проектирование печатных плат, разработку встроенного программного обеспечения, смешанное аналогово-цифровое моделирование, анализ целостности сигналов, технологическую подготовку производства, проектирование и отладку систем на базе ПЛИС с использованием макетной платы Altium NanoBoard.

AltiumLive представляет собой профессиональную online-среду с развитыми возможностями загрузки и обмена контента, так или иначе связанного с проектированием электронного изделия. В разделе Content Store можно расширить функционал Altium Designer и получить новый контент, библиотеки, готовые проектные шаблоны.

Перенос проекта электронного изделия из одной среды проектирования в другую всегда является одной из сложнейших задач. Встроенный Мастер импорта (Import Wizard) позволяет импортировать схемы, платы, библиотеки, выполненные с помощью систем P-CAD, Protel, OrCAD, PADs, DxDesigner, Allegro PCB, и преобразует их в проекты Altium Designer.

3D-визуализация позволяет получать реалистичные изображения платы, обеспечивает поддержку машиностроительных САПР, прямую связь с моделями в формате STEP, оперативную проверку зазоров и расстояний и многое другое.

NanoBoard — плата отладки и макетирования систем на основе ПЛИС

Для отладки системы на базе ПЛИС компания Altium предлагает проектировщикам свою уникальную реконфигурируемую аппаратную платформу NanoBoard. Это решение позволяет протестировать созданный проект внутри реальной ПЛИС уже на этапе моделирования и получить прототип задолго до изготовления печатной платы.

При наличии NanoBoard разработчики электроники, даже не имея опыта работы с FPGA, могут конструировать сложные системы, базирующиеся на программных процессорах. Для этого им не требуется предварительной подготовки в области программных языков VHDL или Verilog. Компания Altium предлагает две модели NanoBoard:

- NanoBoard NB2 — универсальная плата, которая поддерживает работу с ПЛИС различных производителей благодаря сменным дочерним платам (Xilinx, Altera и Lattice). Каждая дочерняя плата содержит ту или иную ПЛИС и устанавливается в разъемы NanoBoard. Замена дочерней платы позволяет разработчику быстро и просто переориентировать проект на другого производителя ПЛИС, причем без изменения самого проекта. В комплекте с NanoBoard NB2 поставляется одна дочерняя плата на выбор.
- NanoBoard 3000 обеспечивает работу с ПЛИС только одного производителя и выпускается в трех видах: NB3000XN-01 (Xilinx), NB3000AL-01 (Altera), NB3000LC-01 (Lattice).

В комплекте с платой NanoBoard поставляется специальная годовая лицензия Altium Designer Soft Design.

nanoCAD — отечественная САПР

Платформа nanoCAD — новейшая альтернативная САПР, на основе которой объединены решения для выполнения проектных работ инженерами различных специальностей. Прямая поддержка формата DWG обеспечивает возможность легко обмениваться данными между различными проектами. Простой классический интерфейс не требует переобучения специалистов, позволяя сразу включить программу в технологический цикл проектирования.

САПР на базе nanoCAD

nanoCAD является одновременно и базовой платформой для специализированных решений, обладающих всеми необходимыми инструментами автоматизации проектной деятельности, и недорогим самостоятельным решением, предлагающим «классическое» 2D-черчение и выпуск документации ручным способом. Такая схема позволяет выстроить экономичные решения для заказчиков любого уровня: нетребовательные пользователи могут использовать в коммерческой деятельности предыдущие версии nanoCAD бесплатно, а профессиональные пользователи — приобрести самые современные инструменты по цене от 5 000 руб за рабочее место.

Профессиональные специализированные решения

На базе nanoCAD выстроены 12 решений, которые существенно повышают производительность ручных методов проектирования и автоматизируют каждодневную рутину. В качестве специализированных решений первого уровня можно выделить программные продукты nanoCAD СПДС, Механика и Схемы, которые предназначены для автоматизации работ в области оформления рабочей документации в строгом соответствии с российскими стандартами. Они могут использоваться и как дополнение к любой системе 3D-моделирования (для оформления проекций чертежей), и в качестве самостоятельных продуктов, обеспечивающих решение всего комплекса задач 2D-проектирования и выпуска документации.

nanoCAD — открытая для разработки система. Это означает, что вы сможете разработать (на языках .NET, C++, JS, VBS, LISP и DCL) собственное приложение под бесплатную платформу и использовать такое решение в своей работе.

- **nanoCAD Электро** — автоматизированное выполнение проектов в части силового электрооборудования (ЭМ) и внутреннего электроосвещения (ЭО) промышленных и гражданских объектов строительства.
- **nanoCAD СКС** — автоматизированное проектирование структурированных кабельных систем (СКС) зданий и сооружений различного назначения, кабеленесущих систем.
- **nanoCAD Геоника** — автоматизация проектно-изыскательских работ. Предназначена для специалистов отделов изысканий и генплана. Включает модули «Топоплан», «Генплан», «Сети».
- **nanoCAD Стройплощадка** — оформление чертежей по разделам «Проект организации строительства» (ПОС) и «Проект производства работ» (ППР). Программа включает в себя весь функционал nanoCAD СПДС и является независимым приложением.
- **nanoCAD Конструкции** — предназначена для конструкторов, разрабатывающих комплекты рабочих чертежей марок КЖ и КЖИ в строгом соответствии с отечественными нормами и стандартами.
- **nanoCAD Фундаменты** — предназначена для подготовки схем расположения и чертежей столбчатых фундаментов на свайном и естественном основании, включая расчет основания по деформациям для фундаментов колонн промышленных и гражданских зданий, расчет свайного куста на прочность по несущей способности сваи и расчет монолитных ленточных фундаментов.
- **nanoCAD ЛЭП** — автоматизация проектирования, расчета и выпуска полного комплекта документов при проектировании воздушных линий электропередач.

Model Studio CS —

решения для проектирования промышленных объектов

Эта линейка программных комплексов разработана специально для российской инженерной школы. Model Studio CS — это передовые решения в области IT и САПР, ориентация на российскую технологию проектирования, зарубежный опыт, база данных оборудования, изделий и материалов, применяемых в России и за рубежом, техническая поддержка, сертификаты соответствия российским нормам проектирования.

Исследования в области эргономики и интерактивных технологий позволили максимально сократить сроки освоения этих программ. Приступать к работе проектировщик может сразу же после краткого знакомства с интерфейсом. В состав каждого из программных продуктов включены средства автоматического формирования спецификаций и экспликаций, а также инструменты автоматического снятия размеров, простановки позиций и надписывания.

Основные возможности:

- трехмерное проектирование;
- готовая база данных оборудования, изделий и материалов для работы в России и за рубежом;
- расчеты в среде проектирования с автоматической генерацией документов;
- соответствие российским нормативным документам (ПУЭ, ГОСТ, СНиП);
- проверка инженерных решений.

Рабочее место, где установлена программа, уже оснащено всем необходимым для проектирования: средствами трехмерного моделирования, проверки на предмет коллизий, подготовки расчетной модели. В состав продуктов Model Studio CS включены средства автоматического формирования спецификаций и экспликаций.

Model Studio CS ЛЭП — программный комплекс, предназначенный для расчета и выпуска полного комплекта документов при проектировании воздушных линий электропередач всех классов напряжений (0,4-750 кВ) и ВОЛС.

Model Studio CS Молниезащита — программный комплекс для расчета и трехмерного интерактивного проектирования молниезащиты зданий, сооружений и открытых территорий промышленного и гражданского назначения.

Model Studio CS Открытые распределительные устройства — программный комплекс, предназначенный для разработки компоновочных решений в трехмерном пространстве открытых распределительных устройств, выполнения расчетов гибкой ошиновки, выпуска проектной и рабочей документации (чертежей, спецификаций и т.д.).

Model Studio CS Трубопроводы — программный комплекс, предназначенный для трехмерного проектирования внутриплощадочных, внутрицеховых и межцеховых систем трубопроводов, в том числе технологических трубопроводов, трубопроводов пара и горячей воды, систем водо- и газоснабжения, отопления, канализации и других.

Model Studio CS Кабельное хозяйство — программный комплекс, предназначенный для трехмерной компоновки кабельных конструкций любой сложности и автоматической трехмерной раскладки кабелей.

CADLib Модель и Архив — специализированное программное обеспечение для работы с информационными трехмерными моделями, полученными в процессе проектирования.

Model Studio CS Компоновщик щитов предназначен для трехмерного проектирования общих видов щитов (пультов).

КОМПАС-3D V13.
Машиностроительное проектирование

Система КОМПАС-3D предоставляет специалистам современные технологии проектирования в полном соответствии с отечественными стандартами. С ее помощью инженер может осуществить полный спектр необходимых работ — от первоначальной трехмерной проработки идеи по созданию или модернизации изделия, проверки полученной конструкции на прочность до получения комплекта конструкторской документации и передачи ее в производство.

Станок буровой, ООО «УГМК-Рудгормаш-Воронеж»

Пульт управления, ОАО Завод «Фиолент», г. Симферополь

Маяк проблесковый светодиодный, ОАО «Сарапульский электрогенераторный завод»

Основные компоненты КОМПАС-3D:

- система трехмерного моделирования;
- универсальная система автоматизированного проектирования КОМПАС-График;
- инженерный текстовый редактор;
- модуль проектирования спецификаций.

Специализированные приложения КОМПАС-3D для машиностроительного и приборостроительного проектирования помогают эффективнее решать самые различные задачи за счет автоматизации процесса разработки.

Машиностроительная конфигурация включает в себя приложения, обеспечивающие автоматизацию типовых задач конструктора-машиностроителя:

- Библиотека «Стандартные изделия» содержит большую базу элементов, которая затрагивает практически все области проектирования;
- Модули КОМПАС-Shaft и КОМПАС-Spring позволяют максимально эффективно выполнять расчет и построение распространенных деталей машин: конструктору достаточно указать исходные данные, все остальное система сделает сама;
- Специализированные приложения Трубопроводы 3D, Металлоконструкции 3D, Пресс-формы 3D автоматизируют создание наиболее сложных пространственных конструкций, повышая производительность работы;
- Встроенная система прочностного анализа APM FEM, Универсальный механизм и Библиотека анимации позволяют произвести расчет прочностных и динамических характеристик изделия и моделировать поведение изделия в реальной среде, сокращая количество натурных испытаний.

Приборостроительная конфигурация объединяет приложения для проектирования радиоэлектронной аппаратуры, приборов и электрооборудования:

- КОМПАС-Электрик автоматизирует проектирование и выпуск комплекта документов (схем и отчетов к ним) на электрооборудование.
- КОМПАС-Электрик Express предназначен для пользователей, которые занимаются разработкой принципиальных электрических схем и перечней элементов к ним.
- Кабели и жгуты 3D автоматизирует процесс трехмерного моделирования электрических кабелей и жгутов, а также выпуск конструкторской документации на эти изделия.
- Конвертер 3D-моделей печатных плат (формат IDF) и текстовой КД из электронных САПР позволяет получить трехмерную модель печатной платы, разработанной в ECAD-системах.
- Библиотека поддержки формата PDF (P-CAD) обеспечивает передачу в КОМПАС-График чертежей узлов печатного монтажа, разработанных в ECAD-системах и сохраненных в формате PDF.

В декабре 2011 года с выходом сервис-пака SP1 КОМПАС-3D V13 приобрел новые качества, существенно влияющие на мощность и скорость работы системы.

Разработана версия КОМПАС-3D для 64-разрядных операционных систем. При использовании современного компьютера, оснащенного процессором с несколькими ядрами и достаточным количеством оперативной памяти (от 8 ГБ), создание и перестроение ассоциативных видов происходит в несколько раз быстрее за счет их параллельной обработки.

Компас-3D V13, система трехмерного моделирования, лицензия	219-64-11-ASCON-SL	93 000 руб.
Компас-График V13, универсальная система автоматизированного проектирования, лицензия	219-64-12-ASCON-SL	49 500 руб.
Компас-3D V13 с Пакетом обновлений до V14, лицензия	219-64-14-ASCON-SL	107 500 руб.

Расписание курсов в Учебном центре Softline

Вендор	Код	Город	Название курса	Начало	Окончание
Microsoft	10175	Екатеринбург	Разработка приложений Microsoft SharePoint 2010	01.10.2012	05.10.2012
VMware	VI5 ICM	Челябинск	VMware vSphere: Install, Configure, Manage	01.10.2012	05.10.2012
Oracle	11gNFA	Мирный(НСК)	Oracle Database 11g: New Features for Administrators	01.10.2012	05.10.2012
Oracle	11gDG	Новосибирск	Oracle Database 11g: Администрирование Data Guard	01.10.2012	04.10.2012
Cisco	BGP	Новосибирск	Конфигурирование BGP на маршрутизаторах Cisco	01.10.2012	05.10.2012
Microsoft	10751	Новосибирск	Настройка и развертывание частного «облака» с использованием System Center 2012	01.10.2012	05.10.2012
Cisco	ICND1	Нижний Новгород	Interconnecting Cisco Networking Devices v.1.1 Part 1	01.10.2012	05.10.2012
Microsoft	10174	Нижний Новгород	Настройка и управление Microsoft SharePoint 2010	01.10.2012	05.10.2012
Microsoft	10267	Дзержинск(НН)	Введение в web-разработку с помощью Visual Studio 2010	01.10.2012	05.10.2012
Citrix	CXA-206I	Саратов (Самара)	Citrix XenApp 6.5 Administration (Администрирование Citrix XenApp 6.5)	01.10.2012	05.10.2012
Microsoft	50357	Ростов-на-Дону	Внедрение Forefront Threat Management Gateway 2010	01.10.2012	02.10.2012
«Лаборатория Касперского»	KL-002.98-дист	дистанционно	Kaspersky Endpoint Security для Windows. Базовый курс	01.10.2012	03.10.2012
«Лаборатория Касперского»	KL-302.98-дист	дистанционно	Kaspersky Endpoint Security для Windows. Расширенный курс	04.10.2012	06.10.2012
Microsoft	10748	Москва	Внедрение System Center 2012 Configuration Manager	01.10.2012	03.10.2012
Microsoft	10774	Москва	Создание запросов в SQL Server 2012	01.10.2012	05.10.2012
Microsoft	6421	Москва	Конфигурирование и устранение неполадок сетевой инфраструктуры Windows Server 2008	01.10.2012	05.10.2012
Symantec	DP0157	Москва	Symantec Backup Exec 2012: Администрирование	01.10.2012	05.10.2012
VMware	VI5 ICM	Москва	VMware vSphere: Install, Configure, Manage	01.10.2012	05.10.2012
Microsoft	10325	Москва	Автоматизация администрирования при помощи Windows PowerShell 2.0	01.10.2012	05.10.2012
Microsoft	10135	Москва	Конфигурация, управление и устранение неисправностей работы организации Microsoft Exchange Server 2010	01.10.2012	05.10.2012
Битрикс 1С	BIT06	Москва	Интеграция дизайна в Bitrix Framework	01.10.2012	03.10.2012
Битрикс 1С	BIT07	Москва	Разработчик Bitrix Framework	04.10.2012	06.10.2012
Microsoft	50468	Москва	SharePoint 2010 для конечных пользователей, уровень 1	01.10.2012	03.10.2012
Microsoft	50469	Москва	SharePoint 2010 для конечных пользователей, уровень 2	04.10.2012	05.10.2012
Трубопровод	Тр-3	Москва	ПС «СТАРТ»	02.10.2012	04.10.2012
Oracle	11gPLSQL	Москва	Oracle Database 11g: PL/SQL Fundamentals	01.10.2012	02.10.2012
Oracle	11gDPU	Москва	Oracle Database 11g: Develop PL/SQL Program Units	03.10.2012	05.10.2012
Cisco	ROUTE	Москва	Маршрутизация с использованием оборудования Cisco	01.10.2012	05.10.2012
Citrix	CXA-301I	Саратов (Самара)	Citrix XenApp 6.5 Advanced Administration	08.10.2012	13.10.2012
Microsoft	10175	Казань	Разработка приложений Microsoft SharePoint 2010	08.10.2012	19.10.2012
Microsoft	6419	Новосибирск	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	08.10.2012	12.10.2012
Oracle	11gAPLS	Новосибирск	Oracle Database 11g: Advanced PL/SQL	08.10.2012	10.10.2012
Oracle	11gTSQL	Новосибирск	Oracle Database 11g: SQL Tuning Workshop	11.10.2012	13.10.2012
Oracle	11gRAC	Мирный(НСК)	Oracle 11g: RAC and Grid Infrastructure Administration Accelerated	08.10.2012	13.10.2012
Microsoft	10175	Нижний Новгород	Разработка приложений Microsoft SharePoint 2010	08.10.2012	12.10.2012
Microsoft	50400	Нижний Новгород	Проектирование, оптимизация и поддержка решений в области администрирования Microsoft SQL Server 2008	08.10.2012	12.10.2012
Microsoft	10774	Хабаровск	Создание запросов в SQL Server 2012	08.10.2012	12.10.2012
Microsoft	10135	Хабаровск	Настройка, управление и диагностика Microsoft Exchange Server 2010	08.10.2012	12.10.2012
Microsoft	10262	Томск	Разработка клиентских приложений	08.10.2012	12.10.2012
Microsoft	6425	Уфа	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	08.10.2012	12.10.2012

JOURNALS for PROFESSIONALS

JOURNALS for PROFESSIONALS

JOURNALS for PROFESSIONALS

Подписка на журналы www.ITbook.ru

Журналы

для ИТ-специалистов

[... и не только]

Журнал	Подписной индекс Агентства «Роспечать»
MSDN MAGAZINE/РУССКАЯ РЕДАКЦИЯ Ведущий журнал для разработчиков программного обеспечения	81240
MSDN MAGAZINE/РУССКАЯ РЕДАКЦИЯ на DVD Полный электронный архив журнала: июль 2002 – декабрь 2011	20460
TECHNET MAGAZINE/РУССКАЯ РЕДАКЦИЯ Администрирование и эксплуатация сетевых коммуникаций и информационных систем	18197
АДМИНИСТРИРОВАНИЕ СЕТЕЙ WINDOWS И LINUX (+CD) Актуальные сведения и готовые приложения из зарубежных и отечественных источников	84243
ИСПОЛЬЗОВАНИЕ VISUAL STUDIO Актуальная практическая информация для программистов и ИТ-специалистов	82843
ПРОГРАММИРОВАНИЕ НА C# Разработчикам приложений и компонентов для .NET	82845
ПРОГРАММИРОВАНИЕ НА C/C++ Статьи, примеры и готовые приложения зарубежных и отечественных авторов	82690
WEB-РАЗРАБОТКА: ASP, WEB-СЕРВИСЫ, XML Практические сведения из зарубежных и отечественных источников	82692
WEB-ДИЗАЙН ДЛЯ ПРОФЕССИОНАЛОВ Дизайн, программирование, юзабилити и поисковая оптимизация контента	83606
СИСТЕМНОМУ АДМИНИСТРАТОРУ: ПОЛЕЗНЫЕ УТИЛИТЫ (+CD) ПО для администрирования, настройки, тестирования, проектирования, автоматизации и защиты сетей	46361
БЕЗОПАСНОСТЬ ИТ-ИНФРАСТРУКТУРЫ Теория, практика и средства обеспечения безопасности ИТ-среды предприятия	36728
КОРПОРАТИВНЫЕ СУБД Независимое издание для специалистов по современным СУБД корпоративного уровня	18199
SQL SERVER ДЛЯ ПРОФЕССИОНАЛОВ (+CD) Разработка приложений, приемы эффективной работы	79947
SQL SERVER ДЛЯ АДМИНИСТРАТОРОВ Приемы администрирования, сценарии автоматизации	20838
КОНТРОЛЬ, РЕВИЗИЯ, ПРОВЕРКА (в финансово-хозяйственной деятельности) Бухгалтерский, налоговый и управленческий учет — организация и проведение контроля	46365
ЦИФРОВЫЕ ТЕХНОЛОГИИ ADOBE ДЛЯ ПРОФЕССИОНАЛОВ НОВИНКА Профессиональное издание, посвященное секретам и тонкостям создания проектов в Adobe Creative Suite	84890
ПОЛЯНА НОВИНКА Произведения современных писателей	84959

Журнал	Подписной индекс Агентства «Пресса России»
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В БИЗНЕСЕ Практический опыт и рекомендации по внедрению и эксплуатации систем на базе 1С, Microsoft Dynamics, SAP, Oracle и др.	82867
УПРАВЛЕНИЕ БИЗНЕС-ПРОЦЕССАМИ Профессиональное издание, посвященное технологиям управления бизнес-процессами, стратегическому управлению и вопросам успешной реализации проектов	82883
TECHNET MAGAZINE/РУССКАЯ РЕДАКЦИЯ на CD Полный электронный архив журнала: январь 2005 – декабрь 2011	82855
MICROSOFT ARCHITECTS JOURNAL/РУССКАЯ РЕДАКЦИЯ на CD Полный электронный архив журнала: январь 2005 – декабрь 2011	82557

Предлагаемые журналы распространяются по подписке и в розничную торговлю не поступают.

Вендор	Код	Город	Название курса	Начало	Окончание
Microsoft	10747	Екатеринбург	Администрирование System Center 2012 Configuration Manager	08.10.2012	12.10.2012
Cisco	ICND1	Санкт-Петербург	Interconnecting Cisco Networking Devices v.1.1 Part 1	08.10.2012	12.10.2012
Cisco	ICND1	Ростов-на-Дону	Interconnecting Cisco Networking Devices v.1.1 Part 1	08.10.2012	12.10.2012
Linux	LL-103-дист	дистанционно	Сетевое администрирование Linux	08.10.2012	11.10.2012
ITIL	SERV_DESK	Москва	Организация работы службы Service Desk. Управление инцидентами и проблемами (основные элементы подхода)	08.10.2012	10.10.2012
Oracle	11gAPLS	Москва	Oracle Database 11g: Advanced PL/SQL	08.10.2012	10.10.2012
Microsoft	10533	Москва	Развертывание, настройка и администрирование Microsoft Lync Server 2010	08.10.2012	12.10.2012
Microsoft	10174	Москва	Настройка и управление Microsoft SharePoint 2010	08.10.2012	12.10.2012
VMware	VS5 OS	Москва	VMware vSphere: Оптимизация и масштабирование	08.10.2012	12.10.2012
Microsoft	10233	Москва	Проектирование и внедрение решений на базе организации Microsoft Exchange Server 2010	08.10.2012	12.10.2012
Symantec	DP1383	Москва	Symantec Backup Exec 2010: Administration	08.10.2012	12.10.2012
Microsoft	10215	Москва	Внедрение и сопровождение платформы виртуализации на базе Microsoft Server	08.10.2012	12.10.2012
Microsoft	6419	Москва	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	08.10.2012	12.10.2012
Cisco	SWITCH	Москва	Создание коммутируемых сетей Cisco	08.10.2012	12.10.2012
Citrix	CXA-206I	Алматы	Citrix XenApp 6.5 Administration (Администрирование Citrix XenApp 6.5)	15.10.2012	19.10.2012
Oracle	11gDBA1	Самара	Oracle Database 11g: Administration Workshop I	15.10.2012	19.10.2012
Cisco	CVOICE	Самара	Технологии Cisco для передачи голоса по сетям IP	15.10.2012	19.10.2012
Autodesk	AC 15	Многовершинное (Хаб)	AutoCAD 2012/2013: уровень 2 (Intermediate)	17.10.2012	24.10.2012
Microsoft	10775	Хабаровск	Администрирование баз данных Microsoft SQL Server	15.10.2012	19.10.2012
Red Hat	RH-134	Новосибирск	Red Hat — Системное администрирование II	15.10.2012	18.10.2012
Red Hat	EX-300	Новосибирск	Экзамен RHCE	15.10.2012	15.10.2012
Cisco	IPS	Новосибирск	Внедрение системы предотвращения вторжений Cisco	15.10.2012	19.10.2012
Microsoft	6425	Нижний Новгород	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	15.10.2012	19.10.2012
Oracle	11gDBA2	Нижний Новгород	Oracle Database 11g: Administration Workshop II	15.10.2012	19.10.2012
Cisco	ICND2	Нижний Новгород	Interconnecting Cisco Networking Devices v.1.1 Part 2	15.10.2012	19.10.2012
Oracle	11gDWS	Нижний Новгород	Oracle Fusion Middleware 11g: Build Web Services	15.10.2012	18.10.2012
Cisco	ICND2	Санкт-Петербург	Interconnecting Cisco Networking Devices v.1.1 Part 2	15.10.2012	19.10.2012
Cisco	ICND2	Ростов-на-Дону	Interconnecting Cisco Networking Devices v.1.1 Part 2	15.10.2012	19.10.2012
Microsoft	10711	Миасс(ЧЛК)	Настройка, управление и диагностика Microsoft Exchange Server 2010 (русскоязычная версия курса 10135)	15.10.2012	20.10.2012
ITIL	ITILv3	Москва	ITIL — введение и основы управления IT-сервисами	15.10.2012	17.10.2012
Microsoft	10262	Москва	Разработка клиентских приложений	15.10.2012	19.10.2012
Microsoft	6451	Москва	Планирование, внедрение и управление Systems Center Configuration Manager	15.10.2012	19.10.2012
Microsoft	10534	Москва	Планирование и проектирование решения Lync Server 2010	15.10.2012	19.10.2012
Citrix	CXD-202I	Москва	Администрирование Citrix XenDesktop 5	15.10.2012	19.10.2012
Symantec	DP1380	Москва	Symantec NetBackup 7.0 for Windows, Administration	15.10.2012	19.10.2012
Microsoft	6425	Москва	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	15.10.2012	19.10.2012
Microsoft	10175	Москва	Разработка приложений Microsoft SharePoint 2010	15.10.2012	19.10.2012
Microsoft	10325	Екатеринбург	Автоматизация администрирования при помощи Windows PowerShell 2.0	22.10.2012	26.10.2012
Microsoft	6419	Миасс(ЧЛК)	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	22.10.2012	27.10.2012
ITIL	ITILv3	Нижний Новгород	ITIL — введение и основы управления IT-сервисами	22.10.2012	24.10.2012
Microsoft	6433	Нижний Новгород	Планирование и внедрение Windows Server 2008	22.10.2012	26.10.2012
Autodesk	AC 15	Многовершинное (Хаб)	AutoCAD 2012/2013: уровень 2 (Intermediate)	24.10.2012	31.10.2012

Вендор	Код	Город	Название курса	Начало	Окончание
Microsoft	10777	Хабаровск	Реализация хранилищ данных в Microsoft SQL Server 2012.	22.10.2012	26.10.2012
Oracle	11gDBA2	Самара	Oracle Database 11g: Administration Workshop II	22.10.2012	26.10.2012
Microsoft	10325	Новосибирск	Автоматизация администрирования при помощи Windows PowerShell 2.0	22.10.2012	26.10.2012
RedHat	RH-255	Новосибирск	Red Hat — Системное администрирование III и экзамены RHCSA и RHCE	22.10.2012	26.10.2012
RedHat	RH-254	Новосибирск	Red Hat — Системное администрирование III	22.10.2012	25.10.2012
RedHat	EX-200	Новосибирск	Экзамен RHCSA	26.10.2012	27.10.2012
RedHat	EX-300	Новосибирск	Экзамен RHCE	26.10.2012	27.10.2012
Microsoft	50322-дист	дистанционно	Конфигурирование и администрирование	22.10.2012	26.10.2012
VMware	VI5 ICM	дистанционно	Vmware vSphere: Install, Configure, Manage	22.10.2012	26.10.2012
Microsoft	50028	Москва	Управление System Center Operations Manager 2007 R2	22.10.2012	26.10.2012
Microsoft	10267	Москва	Введение в web-разработку с помощью Visual Studio 2010	22.10.2012	26.10.2012
Microsoft	10231	Москва	Планирование и развертывание Microsoft SharePoint 2010	22.10.2012	26.10.2012
Citrix	CXS-203I	Москва	Citrix XenServer Enterprise Edition 6.0: Администрирование	22.10.2012	26.10.2012
Cisco	TSHOOT	Москва	Поиск и решение проблем в IP сетях на базе оборудования Cisco	22.10.2012	26.10.2012
Citrix	CXA-201I	Москва	Implementing Citrix XenApp 5.0 for Windows Server 2008 (Внедрение Citrix XenApp 5.0 для Windows Server 2008)	22.10.2012	26.10.2012
Microsoft	6425	Миасс(ЧЛК)	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	29.10.2012	03.11.2012
Microsoft	6428	Нижний Новгород	Конфигурирование и устранение неполадок служб терминалов Windows Server 2008	29.10.2012	30.10.2012
Microsoft	6427	Нижний Новгород	Конфигурирование и устранение неполадок служб IIS в Windows Server 2008	31.10.2012	02.11.2012
VMware	VI5 ICM	Нижний Новгород	VMware vSphere: Install, Configure, Manage	29.10.2012	02.11.2012
Microsoft	6421	Нижний Новгород	Конфигурирование и устранение неполадок сетевой инфраструктуры Windows Server 2008	29.10.2012	02.11.2012
Microsoft	10263	Москва	Разработка приложений WCF с помощью Visual Studio 2010	29.10.2012	31.10.2012
VMware	VI4 ADFT	Москва	Advanced Fast Track	29.10.2012	02.11.2012
Microsoft	10747	Москва	Администрирование System Center 2012 Configuration Manager	29.10.2012	02.11.2012
Microsoft	50331	Москва	Техническая поддержка Windows 7 в корпоративной среде	29.10.2012	02.11.2012
Symantec	SC1439	Москва	Symantec Endpoint Protection 12.1: Administration	29.10.2012	02.11.2012
Microsoft	10232	Москва	Проектирование и разработка приложений Microsoft SharePoint Server 2010	29.10.2012	02.11.2012
Cisco	QOS	Москва	Поддержка технологии QOS	29.10.2012	02.11.2012
Red Hat	RH-300	Москва	Ускоренная подготовка к сертификации RHCE (включает экзамены RHCSA и RHCE)	29.10.2012	02.11.2012
Red Hat	RH-299	Москва	Ускоренная подготовка к сертификации RHCE	29.10.2012	01.11.2012
Citrix	CXA-300I	Москва	Advanced Administration for Citrix XenApp 5.0 for Windows Server 2008 (Расширенное администрирование Citrix XenApp 5.0 for Windows Server 2008)	29.10.2012	02.11.2012

Ульяновск, знакомься — «Лаборатория Касперского»

25 июля 2012 года в Ульяновске на территории Управления Федеральной службы судебных приставов (УФССП) по Ульяновской области состоялся круглый стол, организованный Учебным центром Softline для специалистов, отвечающих за IT-инфраструктуру в системе УФССП по Ульяновской области, с целью ознакомления с возможностями продуктов «Лаборатории Касперского» при повседневном использовании.

Вступительное слово произнес руководитель Учебного центра Softline в Самаре, который рассказал о компании Softline Education. Далее, согласно программе мероприятия, инженер компании Softline выступил с презентацией по новым антивирусным продуктам «Лаборатории Касперского». Он рассказал о различных комплексах продуктов Kaspersky класса Space Security, предназначенных для защиты от современных компьютерных угроз. Особое внимание в докладе было уделено теме виртуальных машин Kaspersky Endpoint Security 8. По завершению информационного блока был организован семинар для участников круглого стола.

«Благодаря профессиональной работе сотрудников Учебного центра Softline наши специалисты в ходе семинара получили исчерпывающую информацию о современных возможностях программных продуктов «Лаборатории Касперского», — отмечает Андрей Козленко, начальник отдела информатизации и обеспечения информационной безопасности УФССП России по Ульяновской области. — Мы довольны результатами встречи и заинтересованы в дальнейшей работе по организации совместных учебных мероприятий. Благодарим сотрудников Учебного центра Softline за ответственность и профессионализм».

«Совместный круглый стол с УФССП России по Ульяновской области стал первым в линейке подобных мероприятий, которые мы планируем организовывать с представителями других силовых федеральных структур в городе Ульяновске, — рассказывает Юлия Меркурьева, руководитель Учебного центра Softline в Самаре. — Семинары по данным тематикам главным образом направлены на выявление потенциальных потребностей в области обучения персонала заказчика и являются важным элементом нашей стратегии по формированию портфеля услуг для органов государственной власти».

Центр подготовки и повышения квалификации it-специалистов
“АйТи-Подготовка” (www.it-podgotovka.ru)

18-22 июня, г. Москва

«Моделирование, анализ, спецификация телекоммуникационных систем средствами UML. Моделирование и анализ сетевых протоколов»

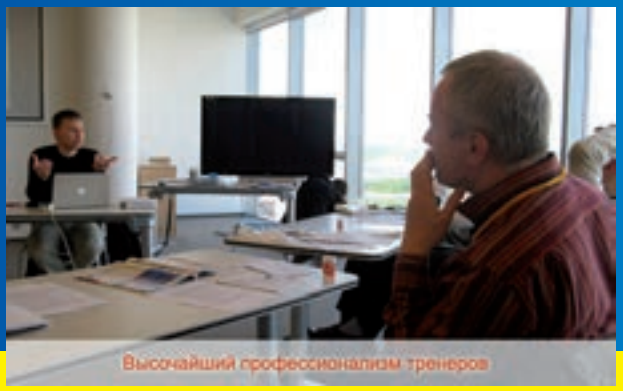
Подробности на сайте www. it-podgotovka.ru

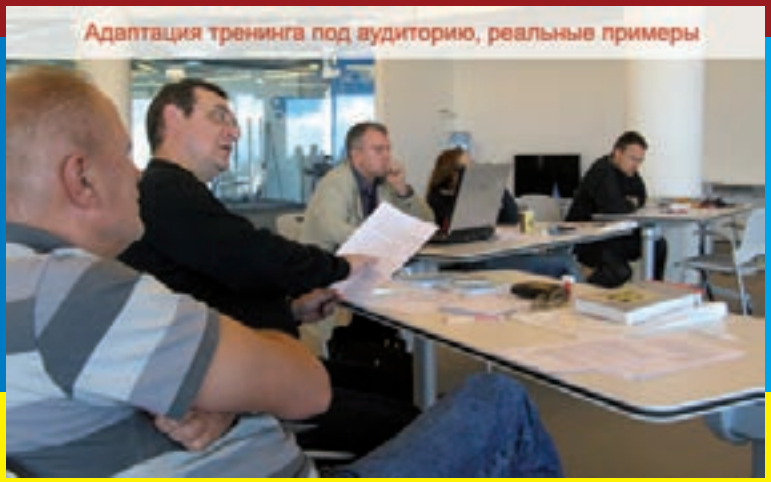
ТАКЖЕ в ЦЕНТРЕ “АйТи-Подготовка ” ВЫ НАЙДЕТЕ БОЛЬШОЕ КОЛИЧЕСТВО УЧЕБНЫХ КУРСОВ, ТРЕНИНГОВ и МАСТЕР-КЛАССОВ ОТ ЛУЧШИХ СПЕЦИАЛИСТОВ В СВОИХ ОБЛАСТЯХ

Например:

1. Профессиональная разработка пользовательских интерфейсов.
2. Двухдневный экспресс-курс “Моделирование на UML. Экспресс”.
3. Четырехдневный практический мастер-курс “Моделирование на UML”.
4. QDD – разработка программных систем, направляемая вопросами или как при плохом (неполном, неточном) техническом задании сделать хороший продукт.
5. Повышение качества программного продукта и эффективности его разработки путем использования моделей.
6. Разработка приложений в специализированных областях (в сложных предметных областях).
7. Управление и контроль качества в разработке программных систем.
8. Спецификация программных систем.
9. Повышение эффективности разработки программных систем. Системный подход и примеры практической реализации.
10. UML для аналитиков.
11. RUP — методология разработки программного обеспечения, созданная компанией Rational Software (IBM). Теория, практика, опыт.

И многое другое!!!





Полный перечень курсов, расписание и подробности на сайте www. it-podgotovka.ru

ПОДПИШИСЬ НА LINUX FORMAT И ВЫИГРАЙ СУПЕРПРИЗ!

Lenovo ThinkPad X220
Разыгрывается 5 ноутбуков

Дистрибутив Ubuntu 12.04
Разыгрывается 50 дисков

Сумка Java Days 2012
Разыгрывается 3 сумки

Плюс бонусы!
Каждому редакционному подписчику печатной версии Linux Format на 2013 год

- DVD с архивом журнала Linux Format 2005–2012
- Подписка на PDF-версию журнала Linux Format
- Объемная наклейка на системный блок

Оформи подписку на 2013 год на печатную версию журнала Linux Format и участвуй в розыгрыше призов!

Для участия в розыгрыше необходимо до 31 октября 2012 года оформить и оплатить подписку на печатную версию журнала Linux Format на сайте shop.linuxformat.ru и пройти процедуру регистрации по адресу www.linuxformat.ru/priz/

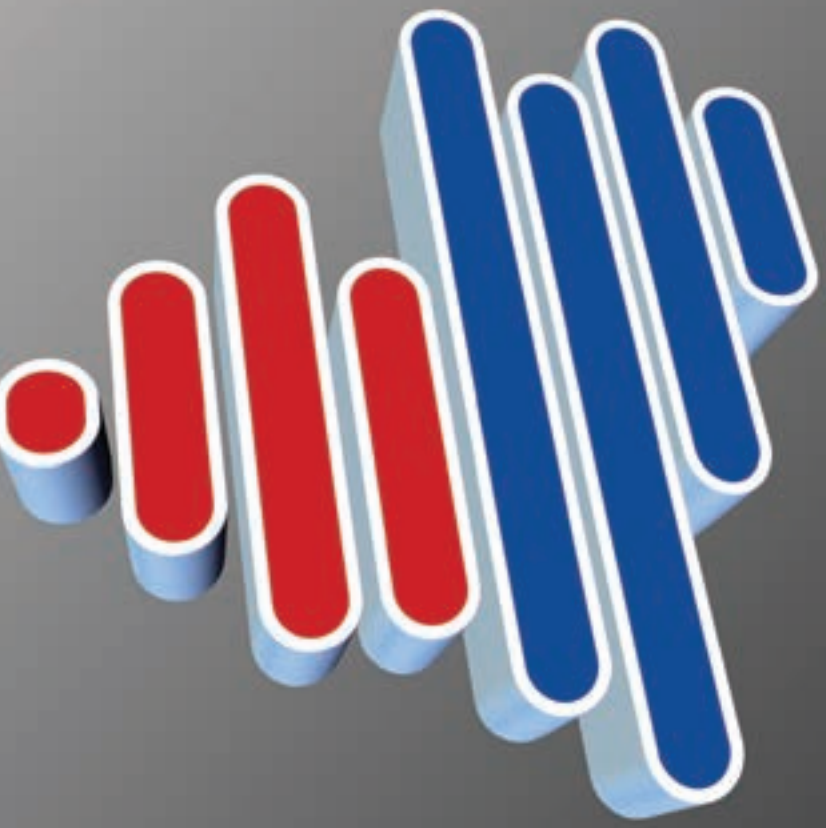
Стоимость годовой подписки на печатную версию журнала Linux Format — 2190 руб. (без учета стоимости доставки).

shop.linuxformat.ru

первый ИТ-портал самарского региона

СамараTECH

Портал СамараTECH - это первый региональный информационно-аналитический Интернет ресурс о развитии информационных технологий в Самарском регионе.



- все ИТ-новости региона
- репортажи с мероприятий
- обзоры новинок рынка
- ИТ-календарь
- клуб ИТ-специалистов
- форум для общения
- твиттер-вещание

Развивайте Ваш бизнес вместе с нами

приглашаем к сотрудничеству ИТ-компании, уже работающие на Самарском рынке или стремящиеся на него выходить.

WWW.SAMARA-TECH.RU

NewScientist RU

навигатор в науке и инновационном бизнесе

United Kingdom, USA, Canada, Australia, New Zealand

теперь и в РОССИИ

Тел.: +7(495) 930-87-07, 930-88-50

www.newscientist.ru info@newscientist.ru

@Astera

Новости ИТ-бизнеса для Профессионалов

Информационно-деловой канал @ASTERA является ведущим поставщиком деловой информации для нужд профессиональных участников российского рынка ИТ.

Ежедневно канал @ASTERA предоставляет актуальную информацию о людях и бизнесе, технологиях и компаниях, событиях и мероприятиях, продуктах и услугах. Ежемесячно сайт www.astera.ru посещают свыше 150 000 человек.

Редакция канала тщательно следит за всеми основными событиями, происходящими на ИТ-рынке, существующими тенденциями и проблемами. Кроме того, внимание уделяется событиям в жизни страны и за рубежом, прямо или косвенно влияющим на бизнес. Для публикации отбирается информация более чем из 1000 источников. Основные принципы – актуальность, широта охвата различных сегментов рынка и соответствие профессиональным интересам аудитории канала.

Начиная с 2003 года канал @ASTERA проводит регулярную исследовательскую работу, направленную на изучение структуры российского ИТ-рынка. Результаты исследований публикуются в виде отчетов: «Рейтинг ИТ-компаний в России», «Лучшие дистрибьюторы», «Лучшие производители», «Рейтинг ИТ-брендов».

Информационно-деловой канал @ASTERA основан в 1999 году.

www.astera.ru

подробнее на **www.astera.ru**

Mandriva
www.mandriva.ru

Mandriva Linux — один из самых популярных дистрибутивов GNU/Linux в мире. Главные преимущества Mandriva — дружелюбный интерфейс, простота настройки, возможность быстрой адаптации пользователей, ранее не знакомых с этой ОС, совместимость с широким спектром программного и аппаратного обеспечения.

Корпоративные продукты Mandriva Linux

Mandriva 2011 Powerpack

Дистрибутив Mandriva 2011 Powerpack включает набор офисных и серверных приложений, и подходит для установки на офисной или домашней рабочей станции и на сервере. Дружелюбный интерфейс, простота настройки Mandriva Powerpack, совместимость с широким спектром аппаратного обеспечения и совместимость с «1С:Предприятие» обеспечивают корпоративным пользователям возможность легкого перехода с Windows на GNU/Linux.

Mandriva Enterprise Server 5

Mandriva Enterprise Server 5 (MES 5) — это надежный и производительный дистрибутив GNU/Linux для корпоративного сервера. MES 5 поможет вам снизить текущие расходы и упростить инфраструктуру. В MES 5 интегрированы серверные разработки программистов Mandriva, в том числе сервер каталогов пользователей Mandriva Directory Server, а также ведущие свободные серверные приложения, которые помогут вам с минимумом затрат времени и энергии настроить и поддерживать необходимые вам серверы. Срок поддержки дистрибутива — 5 лет.

Сертифицировано ФСТЭК

Дистрибутивы Mandriva Linux **сертифицированы по требованиям ФСТЭК по 5 классу для СВТ и 4 уровню контроля НДВ**, что дает возможность использовать их для обработки конфиденциальной информации в автоматизированных системах класса до 1Г включительно и обработки персональных данных в информационных системах класса до К2 включительно.

- **Mandriva 2008 Spring Powerpack** — дистрибутив для рабочей станции или небольшого сервера.
- **Mandriva Corporate Server 4 Update 3** — дистрибутив для создания корпоративного сервера.
- **Mandriva Flash** — дистрибутив GNU/Linux, загружающийся и работающий прямо с USB-носителя.

EduMandriva — свободное ПО для образования

- Создано с участием российских преподавателей и методистов.
- Все ПО, необходимое для преподавания информатики.
- Методические материалы.

Наименование	Стоимость, руб.
Корпоративные продукты Mandriva	
Mandriva Linux 2011 Powerpack (DVD-box)	1 500
Услуга подписки на Mandriva Enterprise Server 5 на 1 год, базовый уровень (с физическим носителем)	13 300
Услуга подписки на Mandriva Enterprise Server 5 на 3 года, базовый уровень (с физическим носителем)	34 800
Продукты Mandriva для образования	
Комплект программного обеспечения Mandriva Linux и EduMandriva для школ	3 500
Сертифицированные ФСТЭК продукты Mandriva	
Сертифицированный ФСТЭК Mandriva 2008 Spring Powerpack на 10 рабочих мест	28 500
Сертифицированный ФСТЭК Mandriva 2008 Spring Powerpack на 5 рабочих мест	14 500
Сертифицированный ФСТЭК Mandriva 2008 Spring Powerpack на 1 рабочее место	4 990
Сертифицированный ФСТЭК Mandriva Corporate Server 4.0 Update 3	10 050

MANDRIVA УЖЕ ИСПОЛЬЗУЮТ: МВД РФ, Минздравсоцразвития РФ, Минфин республики Саха (Якутия), Правительство Московской области, администрация Черниговского района Приморского края, ОАО «Морион», сеть магазинов «Компьютер-центр «КЕЙ», группа компаний «ИМАГ», компания «Азбука мебели», и многие другие.

С вопросами по продуктам Mandriva обращайтесь в Softline!

Москва +7 (495) 232-00-23

Санкт-Петербург +7 (812) 777-44-46

12NEWS

НОВОСТИ ТЕХНОЛОГИЙ АВТОМАТИЗАЦИИ

ЭВОЛЮЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Издание для корпораций, маленьких компаний, и их сотрудников

WWW.12NEWS.RU

Технологии настоящего для вас!

Актуально.
Просто.
Доступно.

Вся информация,
необходимая
для внедрения СЭД
и работы с документами,
в одном журнале.

Выгодная подписка в редакции по тел.: (495) 937-9082 или на сайте www.shop.mcfr.ru

ISSN 2072-8735 (Print) ISSN 2072-8743 (Online)

T•Comm

Телекоммуникации и транспорт

Периодичность — 6 номеров в год.

Объём — от 64 полос. Формат 215 x 285 мм.

Тираж 5 000 экз.

Интернет-версия на русском и английском языках.

Журнал "T-Comm" рекомендован УМО по образованию в области телекоммуникаций в качестве дополнительного учебного материала для студентов высших учебных заведений по специальностям телекоммуникации и экономика.

Издание включено:

- **в перечень ВАК** (публикации в нём учитываются при защите кандидатских и докторских диссертаций);
- **в реферативный журнал и базу данных ВИНИТИ РАН** (сведения о нем публикуются в справочной системе по периодическим и продолжающимся изданиям Ulrich's Periodicals Directory);
- **в систему Российского индекса научного цитирования** (РИНЦ): eLIBRARY.RU.

Специальные выпуски журнала

"Информационные технологии на транспорте"

"Измерительное оборудование"

"Информационная безопасность"

"Радиочастотная идентификация"

"Цифровое телерадиовещание"

"Системы спутниковой навигации"

КАТАЛОГ

ведущих российских и зарубежных производителей навигационного обрудования и программного обеспечения

ИЗДАТЕЛЬСКИЙ ДОМ
МЕДИА ПАБЛИШЕР
+7 (495) 957-77-43

WWW.MEDIA-PUBLISHER.RU

федеральный деловой журнал

ТСР

тренды. события. рынки

Пять лет на рынке деловой прессы России!

ТСР только важные события

- Связь
- Нефть и газ
- Транспорт России
- Профильные вузы
- Химия, нефтехимия
- Агропромышленный комплекс
- Машиностроение и металлургия
- Топливно-энергетический комплекс
- Банки, страхование, финансовый сектор
- Дорожное и промышленное строительство

В каждом номере ТСР

новые проекты
передовые идеи и технологии
все важные события и мероприятия
ведущие компании и лидеры бизнеса

Уникальная система
целевого распространения
(direct-mail руководителям
ведущих предприятий России,
а также главам субъектов федерации)

www.tsr-media.ru

Подшивка на

PFM. Недвижимость: УПРАВЛЕНИЕ И ЭКСПЛУАТАЦИЯ

– пособие для управляющего

publishing house
IMPRESSMEDIA

+7 (495) 926-45-75
subscribe@impressmedia.ru

Журнал IDO Business - это:

Научно - практическое, информационно - аналитическое и образовательное полноцветное издание об инновациях, их применении в развитии различных отраслей экономики и об аутсорсинге

Рубрики издания:

- Новости
- Эксперт номера
- Иновации
- Развитие
- Аутсорсинг
- Биржа идей
- Мониторинг и законодательство
- Иновационные мероприятия
- Об иновациях - легко

Контакты:

www.ido.ru

по вопросам информационного и рекламного сотрудничества
телефон: +7 (495) 4117987 **e-mail: dsereda@ido.ru**

Распространение:

подписка на печатную и электронную версии, целевая рассылка, участие в крупных московских и региональных отраслевых выставках и форумах в области иноваций и развития информационного общества

IDO: всё об информационных инновациях и аутсорсинге!

Подписка на журнал:

каталог "Пресса России"
http://www.pressa-rf.ru/
индекс 90943

Периодичность - шесть номеров год
Объем - 80 - 96 полос
Тираж - 3000 экз

Журнал издается Некоммерческим Партнерством "Центр Развития Современных Образовательных технологий" при поддержке Евразийского Открытого Институт (ЕАОИ) и Московского Государственного Университета Экономики, Статистики и Информатики (МЭСИ)

XXII

Международная

КОНФЕРЕНЦИЯ

ВЫСТАВКА

ИТО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

2012

Место проведения:

Москва

Ленинские горы

Московский государственный университет имени М. В. Ломоносова

2-й учебный корпус

д. 1, стр. 52

7–9 ноября

Оператор конференции:

ООО НПП «БИТ про», тел.: +7 499 408-55-86

http://ito.su email: info@ito.su

Конференция проходит при поддержке:

ГРУППА КОМПАНИЙ АВЕРС

НАУЧНЫЙ.РУ

ОБРАЗОВАНИЕ электронная система

ИНФО

МЦФЭР ресурсы образования

OFERNIO.RU

GUIR

Вестник Образования России

it-world.ru

it-weekly.ru

LINUX FORMAT

МГУ имени М.В. Ломоносова 1755

elc разработка электронных курсов

ОСНОВА

ОТКРЫТОЕ ОБРАЗОВАНИЕ

МГУ ВМК

АУПИ

softline

УРОК

VII специализированная выставка

ПРОМЭНЕРГО

ПРОМЭНЕРГО 2012

II специализированная выставка

УПРАВЛЕНИЕ ОТХОДАМИ. ЭКОЛОГИЯ

УПРАВЛЕНИЕ ОТХОДАМИ. ЭКОЛОГИЯ 2012

21 - 23 НОЯБРЯ 2012

РАЗДЕЛЫ ВЫСТАВКИ:

- Машиностроение
- Станкостроение
- Металлообработка
- Сварка и тепловая резка технологии и оборудование
- Энергоэффективные и ресурсосберегающие технологии, оборудование и материалы в промышленности и энергетике
- Модернизированное и восстановленное оборудование
- Информационные технологии в промышленности
- Средства и системы автоматизации технологических процессов
- Средства измерения, метрологическое оборудование
- Светотехническое оборудование и источники света
- Оборудование для систем тепло-, газо-, и водоснабжения
- Стройиндустрия
- Лизинговые компании и финансовые группы
- Общественные объединения, учебные заведения

- Сбор, хранение, транспортировка, переработка отходов
- Переработка промышленных отходов и использование вторичных ресурсов
- Сбор и переработка бытовых отходов и отходов жилищно-коммунального хозяйства
- Сбор и переработка отходов сельского хозяйства и перерабатывающей промышленности
- Воды и сточные воды
- Технологии и оборудование для переработки отходов
- Рекуперация энергии, возобновляемые источники
- Рециклинг (механические, физико-химические, биологические, термические, комбинированные методы)
- Системы и технологии очистки воды
- Безопасность и защита от шума
- Техника и технологии ликвидации аварийных разливов нефти и нефтепродуктов
- Санитарная очистка города, экологическая реабилитация природных объектов, благоустройство и озеленение

ОАО «УралЭкспо»
(3532) 950-250,
67-11-01, 560-560

г. Оренбург
С-КК «ОРЕНБУРЖЬЕ»
пр-т Гагарина 21/1

uralexpo@yandex.ru,
www.uralexpo.ru

ORENFON

56 WEB STUDIO

НЕФТЬ. ГАЗ. ХИМИЯ.

Волгоград

Дворец Спорта профсоюзов

12-14 декабря 2012

ВЫСТАВКА

ОБОРУДОВАНИЕ - НЕФТЬ. ГАЗ. ХИМИЯ.

ВЫСТАВКА-КОНФЕРЕНЦИЯ

15-я специализированная выставка оборудования, материалов, технологий для нефтяной, газовой промышленности, нефтеперерабатывающего комплекса.

БИОХИМИЧЕСКИЕ ТЕХНОЛОГИИ

ЭКО-ПЕРЕРАБОТКА И УТИЛИЗАЦИЯ ОТХОДОВ ПРОМЫШЛЕННОГО ПРОИЗВОДСТВА

ГЕНЕРАЛЬНЫЙ ПАРТНЕР:

Нефтегазовая вертикаль

ТЭР NEFTEGAZ

Территория Нефтегаз

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА:

Нефть. Газ. Новации

Нефть России 15 лет

Газовая промышленность

Издательство ГАЗОИЛ ПРЕСС

Neftegaz.RU

Эксплуатация Нефть Газ

Нефть России

ХТ

КГП

Информационно-аналитическое издание ПРОМЫШЛЕННОЕ ОБОРУДОВАНИЕ

13 выпусков в год с 2001 года

Публикации. Новости. Компании

Научно-практический образовательный журнал ПРОФЕССИОНАЛ

ЭкспоМаркет

Волгоградский Выставочный Центр "Регион"
400007, Волгоград, а/я 3400
тел/факс: (8442) 26-61-70, 24-26-02, 26-51-86
e-mail: ngch@regionex.ru www.regionex.ru

ВВЦ РЕГИОН

14-я международная специализированная выставка

ЭНЕРГЕТИКА РЕСУРСОСБЕРЕЖЕНИЕ

XIII МЕЖДУНАРОДНЫЙ СИМПОЗИУМ «Энергоресурсоэффективность и энергосбережение»

5-7 декабря КАЗАНЬ, 2012

ОРГАНИЗАТОРЫ:
Министерство промышленности и торговли РТ,
Центр энергосберегающих технологий РТ
при Кабинете Министров РТ,
Мэрия г. Казани,
ОАО «Казанская ярмарка»
при поддержке Президента и Правительства РТ

В ПРОГРАММЕ:
Заседание Правительства РТ
о реализации целевой программы
«Энергосбережение и повышение
энергетической эффективности в
Республике Татарстан на 2010 – 2015 годы
и на перспективу до 2020 года».

XIII международный симпозиум
«Энергоресурсоэффективность
и энергосбережение».

Конкурс энергоэффективного
оборудования и технологий

www.expoenergo.ru

Генеральный Интернет-спонсор: elec.ru

Генеральный Информационный спонсор: ЭНЕРГО INFO

ОАО "КАЗАНСКАЯ ЯРМАРКА",
420059, г. Казань, Оренбургский тракт,8
тел.: (843) 570-51-06, 570-51-11 (круглосуточно),
факс: 570-51-23
E-mail: 5705106@expokazan.ru,
kazanexpo@telebit.ru

ИНФОРМАЦИОННАЯ СЛУЖБА СИМПОЗИУМА:
ГАУ «Центр энергосберегающих технологий
Республики Татарстан
при Кабинете Министров Республики Татарстан»
тел. (843) 272-99-43, 272-19-21, 272-19-31,
e-mail: cetrt@mail.ru,
сайт: cet.tatarstan.ru


III ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 23 НОЯБРЯ 2012, МОСКВА
ПРЯМОЕ И ВЕНЧУРНОЕ ИНВЕСТРОВАНИЕ В РОССИИ
ОРГАНИЗАТОР
Российский Бизнес Форум
МЕДИА ПАРТНЕРЫ
softline
ОСНОВНЫЕ ТЕМЫ ФОРУМА
Определить какие сектора будут в лидерах роста в 2013 г.
Узнать о новых механизмах инвестирования и стратегиях выхода
Встретить отечественных и иностранных LPs инвестирующих в Россию
Услышать о факторах успеха стоявших за крупнейшими сделками 2011 года
Получить детальный анализ возможностей для венчурных инвесторов
Познакомиться с ведущими игроками российской индустрии PE & VC
СРЕДИ ВЫСТУПАЮЩИХ
Айдар Калиев
Руководитель венчурного бизнеса, ВТБ Капитал
Райнхард Кольайк
Управляющий Партнер, Квадрига Капитал Россия
Александр Аболмасов
Управляющий партнер, инвестиционный фонд, отношения с инвесторами, NRG
Юрий Машинцев
Директор, Russia Partners
Александр Лупанов
Руководитель инвестиционной службы, Фонд Сколково
Николай Дмитриев
Директор по инвестициям, Prostor Capital
Джек Барбанел
Управляющий Директор, Strategic Investment Group
Роланд Нэш
Старший партнер, Vermo Capital
Константин Рыжков
Директор, Russian Direct Investment Fund
Тимоти Эннекинг
Председатель, Altima Asset Management
Мартин Шведлер
Генеральный директор российского офиса, Raiffeisen Investment Ltd.
и другие ...
Простые способы регистрации: по телефону +44 207 1837 103, факсом +44 207 1837 191, по эл.почте registrations@ros.biz
III ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 23 НОЯБРЯ 2012, МОСКВА


ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 17 ОКТЯБРЯ 2012, МОСКВА
КОРПОРАТИВНОЕ УПРАВЛЕНИЕ
ОРГАНИЗАТОР
Российский Бизнес Форум
СПОНСОР КОНФЕРЕНЦИИ
DOWJONES
МЕДИА-ПАРТНЕР
softline
ОСНОВНЫЕ ТЕМЫ ФОРУМА
Пути развития корпоративного управления в отечественных компаниях
Особенности российской практики корпоративного управления
Инструменты оценки качества корпоратив - ного управления
Как обеспечить необходимый уровень независимости совета директоров?
Судебная практика по защите миноритариев
Разрешение корпоративных конфликтов
Страхование ответственности директоров
Выплаты вознаграждений и критерии измерения корпоративного успеха
СРЕДИ ВЫСТУПАЮЩИХ
Дмитрий Дудов
Судья Высший Арбитражный Суд Российской Федерации
Станислав Коптяков
Директор по корпоративному управлению ОАО Энергетические Системы Востока
Руслан Ибрагимов
Вице-президент по корпоративным и правовым вопросам "Мобильные ТелеСистемы"
Александр Дюжиков
Заместитель Начальника Департамента корпоративного управления ФСК ЕЭС
Вера Крупова
Заместитель по корпоративной работе СУЭК
Владимир Гусаков
Член Совета директоров ОАО "РЖД"
Юрий Пермяков
Директор Департамента корпоративного управления «НАК «Азот»
Игорь Петров
Корпоративный секретарь АФК "Система"
Марина Баронина
Главный специалист отдела корпоративного управления «Автоинфинетехзолото»
Иван Родионов
Председатель Совета директоров ОАО «Ростелеком»
Константин Коптяков
Советник президента Сбербанк
и другие ...
Простые способы регистрации: по телефону +44 207 1837 103, факсом +44 207 1837 191, по эл.почте registrations@ros.biz
ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 17 ОКТЯБРЯ 2012, МОСКВА

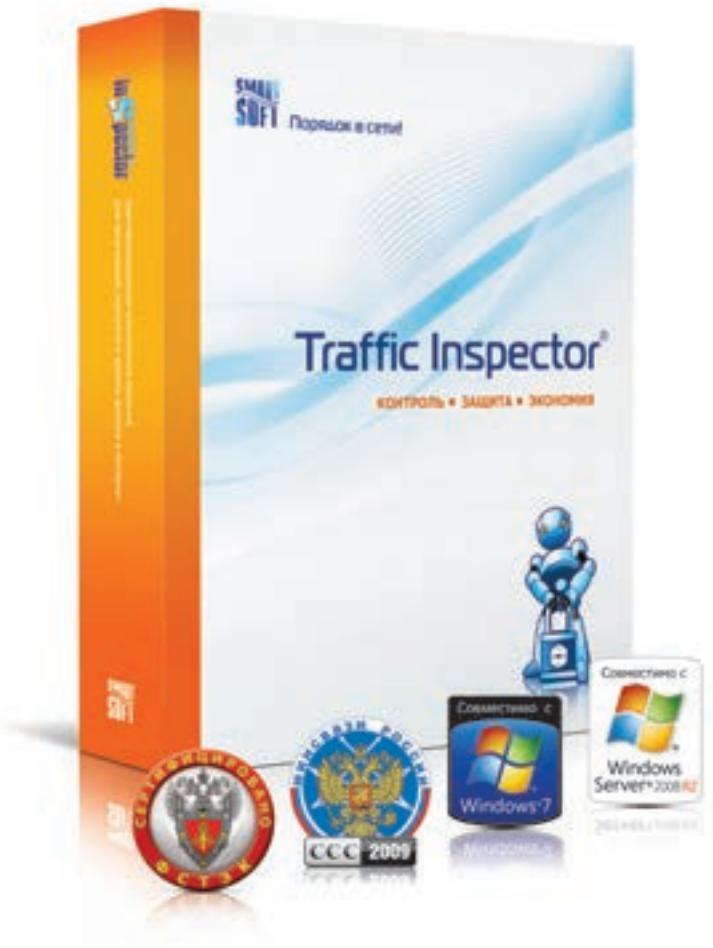

II ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 19 ОКТЯБРЯ 2012, МОСКВА
УПРАВЛЕНИЕ АКТИВАМИ
ОРГАНИЗАТОР
Российский Бизнес Форум
МЕДИА ПАРТНЕРЫ
softline
ЭКСПЕРТ РА
ОСНОВНЫЕ ТЕМЫ ФОРУМА
Законодательные изменения в лицензировании и регулировании деятельности УК и паевых фондов
Перспективы развития российских УК
Развитие розничного направления: Повышение эффективности стратегии привлечения средств
Управление активами государственного и негосударственных пенсионных фондов
Использование производных финансовых инструментов
Риск менеджмент в новых условиях. Хеджирование рисков
СРЕДИ ВЫСТУПАЮЩИХ
Дмитрий Александров Президент Национальная Лига Управляющих
Дмитрий Благов Генеральный Директор УК "ТРИНФИКО"
Ирина Крикошина Генеральный Директор УК «Альфа-капитал»
Роман Соколов Управляющий Директор УК «Открытие»
Павел Санаев Заместитель Генерального Директора «Эксперт РА»
Александр Попов Директор департамента доверительного управления Внешэкономбанк
Андрей Шульга Генеральный Директор, УК «ФИНАМ Менеджмент»
Владимир Потапов CFA, Руководитель бизнеса Портфельных Инвестиций, ВТБ Капитал Управление Активами
Ольга Буланцева Исполнительный Директор НПФ «Промагрофонд»
Роман Шеменков Генеральный директор, УК Капиталъ ПИФ
Виктор Четвериков Генеральный директор Национальное рейтинговое агентство
и другие ...
Простые способы регистрации: по телефону +44 207 1837 103, факсом +44 207 1837 191, по эл.почте registrations@ros.biz
II ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 19 ОКТЯБРЯ 2012, МОСКВА


ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 30 НОЯБРЯ 2012, МОСКВА
УПРАВЛЕНИЕ ЮРИДИЧЕСКИМИ РИСКАМИ КОМПАНИЙ
ОРГАНИЗАТОР
Российский Бизнес Форум
МЕДИА ПАРТНЕРЫ
softline
ОСНОВНЫЕ ТЕМЫ ФОРУМА
Построение комплексной системы управления юридическими рисками
Эффективные механизмы реализации юридической стратегии компании
Модели управления регуляторными рисками и отношения с государственными органами
Комплаенс как одна из технологий управления юридическими рисками
Построение договорной работы сквозь призму управления юр. рисками
Правовые механизмы разрешения корпоративных конфликтов
СРЕДИ ВЫСТУПАЮЩИХ
Александр Виноградов Заместитель начальника юридического департамента, Газпром-Медиа
Ирина Холина Директор юридического департамента, АЭРОФЛОТ
Григорий Сипяков Глава департамента комплаенс контроля, ВТБ Капитал Управление Активами
Ольга Войтович Директор Юридического департамента, ИНТЕРРОС
Елена Чугунова Заместитель директора по правовым вопросам, ЗАО "ЮКОС"
Павел Баранов Директор юридического департамента, РУССКИЕ ФОНДЫ
Елена Габдуллаева Руководитель юридического департамента, METRO Cash & Carry
Татьяна Одабашян Директор по правовым вопросам, ОБЪЕДИНЁННЫЕ ПИВОВАРНИ ХЕЙНЕКЕН
Александр Арсеньев Старший вице-президент по правовым вопросам, ЮИТ
Павел Капков Руководитель рабочей группы
Елена Сидорова Руководитель юридического департамента, АШАН
и другие ...
Простые способы регистрации: по телефону +44 207 1837 103, факсом +44 207 1837 191, по эл.почте registrations@ros.biz
ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ, 30 НОЯБРЯ 2012, МОСКВА

allsoft.ru®

представляет программу для организации, контроля и защиты интернет-доступа

TRAFFIC inSpector



Возможности

- Организация доступа в Интернет. NAT, прокси-сервер, VPN, AD.
- Сертифицированная защита сети. Межсетевой экран и антивирусы.
- Контроль интернет-доступа. Мониторинг, отчеты и статистика.
- Блокировка сайтов и контентная фильтрация. Правила по типам, группам и категориям.
- Экономия трафика, времени и денег. Кэширование, блокировка рекламы.
- Управление скоростью интернет-доступа. Динамический шейпер, приоритеты.
- Настройка и управление маршрутизацией. Перенаправление трафика, публикация служб, Advanced Routing, резервные каналы.
- Сертифицированный учет трафика (система биллинга). Подсчет, лимиты, автоматизация.
- Удаленное администрирование. Консоль и доступ через веб-сервер.

8-800-200-22-33
(бесплатно по России)

www.allsoft.ru

sales@allsoft.ru

Мы продаем продукцию более 1000 мировых производителей программного обеспечения, и эта цифра постоянно растет. Если вы не нашли в списке нужную компанию, отправьте запрос на info@softline.ru — вдруг она уже появилась?

1С.: 1С, 4D, ABBYY, ACD Systems, Acronis, ActFax, ActiveXperts, AdAstra, Adiscon, Adobe, AdRem, AEC, Agnitum, Ahead, Aist, AKComputers, AlachiSoft, Aladdin, Alias, Alloy, AllRoundAutomations, Altiris, ALTLinux, Altova, Aptech, Araxis, Ascon, ASPLinux, Astaro, Autodesk, BakBone, BeaSystems, BitDefender, Borland, BridgeITSolutions, Burstek, BusinessObjects, c360, CambridgeSoft, CastleRock, CAUnicenter, ChaosGroup, CheckPoint, Cimaware, Cisco, Citrix, Clearswift, CognitiveTech, CommontimeLimited, CommuniGatePro, Compaq, ComponentOne, ComputerAssociates, CompuwareNumega, Comsol, ConsistentSoftware, Contentkeeper, Context, Corel, CredantTechnologies, CryptoPro...

Наименование	цена, руб.

ACRONIS

Acronis Backup & Recovery 11 Advanced Server incl. AAP ESD	48 965
Acronis Backup & Recovery 11 Advanced Server Bundle with Universal Restore incl. AAP ESD	58 625
Acronis Backup & Recovery 11 Advanced Server Bundle with Universal Restore and Deduplication incl. AAP ESD	65 450
Acronis Backup & Recovery 11 Advanced Server SBS Edition with Universal Restore incl. AAP ESD	17 465
Acronis Backup & Recovery 11 Virtual Edition with Universal Restore incl. AAP ESD	62 965
Acronis Backup & Recovery 11 Virtual Edition with Universal Restore incl. AAP ESD (only Bundled with VMware)	44 076
Acronis Backup & Recovery 11 Virtual Edition with Univ. Restore and Dedup. incl. AAP ESD	75 565
Acronis Backup & Recovery 11 Virtual Edition with Univ. Restore and Dedup. incl. AAP ESD (only Bundled with VMware)	52 896
Acronis Backup & Recovery 11 Advanced Workstation incl. AAP ESD	3 465
Acronis Backup & Recovery 11 Advanced Workstation Bundle with Universal Restore incl. AAP ESD	3 815
Acronis Backup & Recovery 11 Advanced Workstation Bundle with Universal Restore and Deduplication incl. AAP ESD	4 690
Acronis Backup & Recovery 11 Deduplication for Advanced Server incl. AAP ESD	8 750
Acronis Backup & Recovery 11 Deduplication for Advanced Server SBS Edition incl. AAP ESD	3 465
Acronis Backup & Recovery 11 Deduplication for Virtual Edition incl. AAP ESD	18 865
Acronis Backup & Recovery 11 Deduplication for Advanced Workstation incl. AAP ESD	980
Acronis Backup & Recovery 11 Server for Windows incl. AAP ESD	29 855
Acronis Backup & Recovery 11 Server for Windows Bundle with Universal Restore incl. AAP ESD	40 495
Acronis Backup & Recovery 11 Universal Restore for Advanced Server incl. AAP ESD	12 775
Acronis Backup & Recovery 11 Universal Restore for Advanced Workstation incl. AAP ESD	1 295
Acronis Backup & Recovery 11 Universal Restore for Server for Windows incl. AAP ESD	12 775
Acronis Backup & Recovery 11 Universal Restore for Workstation incl. AAP ESD	1 295
Acronis Backup & Recovery 11 Workstation incl. AAP ESD.	2 590
Acronis Backup & Recovery 11 Workstation Bundle with Universal Restore incl. AAP ESD	3 115
Acronis Recovery for Microsoft Exchange SBS Edition incl. AAP ESD	17 465
Acronis Recovery for Microsoft Exchange Server incl. AAP ESD	42 665
Acronis Recovery for Microsoft SQL Server incl. AAP ESD	21 315
Acronis Snap Deploy 4 for Server incl. AAP ESD	4 235
Acronis Snap Deploy 4 for PC incl. AAP ESD	875
Acronis Universal Deploy 4 for Server incl. AAP ESD	1 295
Acronis Universal Deploy 4 for PC incl. AAP ESD	437
Acronis vmProtect 7 incl. AAP ESD	20 965
Acronis vmProtect – 1 TB per year ESD	24 739
Acronis Disk Director 11 Advanced Server incl. AAP ESD	21 315
Acronis Disk Director 11 Advanced Workstation incl. AAP ESD	2 800
Acronis Backup & Recovery Online Backup for Server - 1 TB per year ESD	20 609
Acronis Backup & Recovery Online Backup for Virtual Machines – 2 TB per year ESD	49 519
Acronis Backup & Recovery Online Backup for Workstation - 250 GB per year ESD	2 065
Acronis Drive Cleanser 6.0 incl. AAP ESD	2 135
Acronis Drive Cleanser 6.0 incl. AAS ESD	2 065
Acronis Backup & Recovery Online – Initial Seeding ESD	4 130
Acronis Backup & Recovery Online – Large Scale Recovery ESD	11 564
Acronis Disk Director 11 Home	1 015
Acronis True Image Home 2012	1 015
Acronis True Image Home 2012 - Family Pack	1 748
Acronis True Image Home 2012 Plus Pack	609

AGNITUM

Outpost Firewall Pro Персональная (Single)	899
Outpost Firewall Pro Домашняя (Personal Pack)	1 149
Outpost Firewall Pro Семейная (Family)	1 349
Outpost Security Suite Pro Персональная (Single)	1 299
Outpost Security Suite Pro Домашняя (Personal Pack)	1 399
Outpost Security Suite Pro Семейная (Family)	2 799
Outpost Antivirus Pro Персональная (Single)	699
Outpost Antivirus Pro Домашняя (Personal Pack)	949
Outpost Antivirus Pro Семейная (Family)	1 199
Outpost Firewall Pro Business 1-9 лицензий в пакете 12 месяцев первая подписка (за лицензию)	899
Outpost Security Suite Pro Business 1-9 лицензий в пакете 12 месяцев первая подписка (за лицензию)	1 399
Outpost Antivirus Pro Business 1-9 лицензий в пакете 12 месяцев первая подписка (за лицензию)	699
Outpost Network Security Business 7 лицензий в пакете 12 месяцев первая подписка (за пакет)	9 310

ALADDIN

Лицензия на использование Secret Disk 4. Базовый комплект с USB-ключом.	4 240
Лицензия на использование Secret Disk 4 Workgroup Edition. Базовый комплект с USB-ключом.	12 440
Лицензия на использование сертифицированной версии Secret Disk 4. Базовый комплект с USB-ключом.	4 400
Лицензия на использование сертифицированной версии Secret Disk 4 Workgroup Edition. Базовый комплект с USB-ключом.	14 150
Лицензия на использование Secret Disk 4. 1-50 (за единицу)	2 800
Лицензия на использование сертифицированной версии Secret Disk 4. 1-50 (за единицу).	2 900
Лицензия на использование ПО Secret Disk Enterprise на одном сервере в одном домене Microsoft Active Directory.	150 000
Лицензия на использование ПО Secret Disk Enterprise на одном рабочем месте. 1-250 (за единицу).	1 200
Лицензия на использование ПО Secret Disk Enterprise для малого бизнеса. Базовый комплект на 10 рабочих мест.	34 800
Лицензия на использование ПО Secret Disk Enterprise для малого бизнеса. Полный комплект на 10 рабочих мест.	44 500
Лицензия на использование ПО Secret Disk Enterprise. Базовый комплект на 25 рабочих мест.	68 500
Лицензия на использование ПО Secret Disk Enterprise. Полный комплект на 25 рабочих мест.	91 050
Лицензия на использование ПО Secret Disk Enterprise на одно рабочее место (только для лицензиатов Secret Disk 4).	480
Лицензия на использование Secret Disk Server NG для файлового сервера на N пользователей (одновременных подключений). Базовый комплект. N = 5 (за единицу)	18 000
Лицензия на использование Secret Disk Server NG для сервера приложений. Базовый комплект.	38 000
Лицензия на использование комбинированного решения: Secret Disk Server NG для сервера приложений и файлового сервера на N пользователей (одновременных подключений). Базовый комплект. N=10 (за единицу)	63 250
Лицензия на использование сертифицированной версии Secret Disk Server NG 3.2 для файлового сервера на N пользователей (одновременных подключений). Базовый комплект. N = 5 (за единицу)	22 000
Лицензия администратора Secret Disk Server NG. 1-10 (за единицу)	1 900
Лицензия администратора Secret Disk Server NG на USB-ключе eToken.	2 810
Лицензия на использование eToken Network Logon. Базовый комплект.	1 985
SAM Лицензия на использование SafeNet Authentication Manager - лицензия на 1 пользователя на 1 год 1–100 (за единицу)	1 400

ALT N

ActiveSync for MDeamon	4 950
MDaemon Standard 6 User	4 290
MDaemon Professional 6 User	12 540
SecurityPlus 6 User License	4 125
RelayFax Professional 6 User	6 765
eLearning for MDaemon	2 310
Outlook Connector Professional 6 User License	3 960
GroupWare Professional 6 User License	4 290
SecurityGateway 10 User	9 801
ProtectionPlus 10 User	6 270

ALTX

Базовый пакет для сертифицированной версии ОС Windows 7 Профессиональная/Professional для использования на 1 АРМ от 1 шт. (за ед.)	972
Базовый пакет для сертифицированной версии ОС Windows 7 Максимальная/Ult для использования на 1 АРМ от 1 шт. (за ед.)	1 263
Базовый пакет для сертифицированной версии ОС Windows 7 Корпоративная/Ent для использования на 1 АРМ от 1 шт. (за ед.)	1 263
Базовый пакет для сертифицированной версии ПО Office 2010 ProPlus для использования на 1 АРМ от 1 шт. (за ед.).	2 295
Базовый пакет для сертифицированной версии ОС Windows Server 2008 Standard Edition для использования на 1 АРМ от 1 шт. (за ед.)	4 500
Базовый пакет для сертифицированной версии ОС Windows Server 2008 Enterprise Edition для использования на 1 АРМ от 1 шт. (за ед.)	14 784
Полный пакет для сертифицированной версии ОС Windows Server 2008 Enterprise Edition для использования на 1 АРМ от 1 шт. (за ед.)	16 184

APPSECINC

DbProtect - Activity Monitoring - 1 Uup	81 774
DbProtect - Vulnerability Management - 1 Uup	58 410
DbProtect - Rights Management - 1 Uup	58 410
DbProtect - Vulnerability Management for DB2 OS/390 or z/OS - 1 Uup.	973 500
DbProtect - RiskView	973 500
AppDetectivePro - Subscription - 1 Uut	77 880
AppDetectivePro - Vulnerability Assessment - 1 Uut	40 887
AppDetectivePro - User Rights Review - 1 Uut	35 046
AppDetectivePro - Perpetual - 1 Uut	233 640

AVAST

avast! Endpoint Protection 1-4 лицензии	899
avast! Endpoint Protection Plus 1-4 лицензии	1 199
avast! Endpoint Protection Suite 5-19 лицензий	999
avast! Endpoint Protection SuitePlus 5-19 лицензий	1 299
avast! File Server Security 1 лицензия	11 419
avast! Email Server Security 1 лицензия	7 139
avast! for Linux 10-19 лицензий	400
avast! Rescue Disc 1 лицензия unlimited	300
avast! Internet Security 1 лицензия	1 200
avast! Pro Antivirus 1 лицензия	900

AVG

Стандарт лицензия AVG Anti-Virus 2012 1 ПК	990
Стандарт лицензия AVG Internet Security 2012 1 ПК	1 550
Стандарт лицензия AVG Mobilation Anti-Virus 1 device	150
Стандарт лицензия AVG PC Tuneup 1 ПК	820
Стандарт лицензия AVG Anti-Virus Business Edition 2012 2 ПК	2 790
Стандарт лицензия AVG eMail Server Edition 2012 5 почтовых ящиков	4 321

Если вам не понравилось, как с вами общался наш менеджер, консультант, курьер или вы хотите посоветовать, как можно сделать обслуживание еще лучше, напишите об этом Председателю совета директоров Softline **Игорю Боровикову** (igorb@softline.ru)

ESET NOD32 Smart Security 5

Интеллектуальное комплексное решение для обеспечения безопасности домашнего ПК

1 790 руб.

АСКОН Компас-3D V13

Система трехмерного моделирования и оформления конструкторской документации

93 000 руб.

DeviceLock 7 DLP Suite

Высочайший уровень предотвращения информационных утечек при минимальных затратах

4200 руб.
(за 1 шт., от 5 шт.)

Mandriva 2008 Spring Powerpack

Удобный и простой дистрибутив Linux, сертифицированный ФСТЭК

Звоните!

Dr. Web Бастион Pro 7

Всесторонняя защита от интернет-угроз и криптограф

2 290 руб.

Intel Cluster Studio 2011

Разработка, анализ и оптимизация высокопроизводительных приложений

65 568 руб.

Microsoft Office Professional 2010

Многофункциональный пакет офисного ПО и поддержки, помогающий в развитии бизнеса

17 602 руб.

Autodesk 3ds Max Design 2013

Лидер рынка программного обеспечения для трехмерного моделирования, анимации и визуализации

99 120 руб.

CorelCAD

Новая 2D . и 3DСАПР . от Corel, экономичная и интуитивно понятная.

28 645 руб.

Serif PagePlus X6

Мощная профессиональная настольная система для издательской верстки и публикации

Звоните!

Panda Internet Security 2012

Защита от вирусов, шпионов, руткитов, хакеров, сетевого мошенничества

1 600 руб.

TrustPort Antivirus 2013

Мощный многосканерный антивирус, способный противостоять разнообразным угрозам

726 руб.

Adobe Photoshop CS6 Extended

Все возможности Photoshop CS6, а также работа с 3D-объектами и анализ изображений

43 200 руб.

MapleSoft Maple 15

Математическая система для аналитических и численных расчетов, включающая более трех тысяч встроенных функций

Звоните!

Мы продаем продукцию более 1000 мировых производителей программного обеспечения, и эта цифра постоянно растет. Если вы не нашли в списке нужную компанию, отправьте запрос на info@softline.ru — вдруг она уже появилась?

CI.: CrystalBall, CrystalGraphics, CSOdessa, Daffodil, DameWare, DataDirect, Datawatch, Deerfield, DesignScience, DeveloperExpress, DigitalSecurity, DocsVision, DrWeb, Dundas, eEye, ejTechnologies, ElectronicsWorkbench, Embarcadero, Enfocus, eRain, Eset, ESRI, ЭСТИ МАП , Eurosoft, eXcsoftware, ExecutiveSoftware, Extensis, Famatech, FileMaker, FinePrint, Flowerfire, Forecast, FriskSoftware, FSecure, Funk, G6FTPServer, GarantPark, GEARSoftware, GFI, Glasspalace, GlobalScape, GlobeSoft, GoldenSoftware, Gupta, HewlettPackard, Hummingbird, Hyena, HyperMethod, IBM, Incache, InfoPower, Informatic, Infostrider...

Наименование	цена, руб.
Стандарт лицензия AVG File Server Edition 2012 2 ПК	1 148
Стандарт лицензия AVG Internet Security Business Edition 2012 2 ПК	3 227

AVIRA

Avira Managed Email Security 12 месяцев 1 узлов сети	886
Avira Business Security Suitee 12 месяцев 3 узлов сети	6 578
Avira AntiVir Exchange 12 месяцев 3 узлов сети	3 078
Avira AntiVir Gateway Bundle 12 месяцев 3 узлов сети	3 864
Avira Internet Security 2012 12 месяцев 1 узлов сети	1 458
Avira AntiVir MailGate 12 месяцев 3 узлов сети.	3 078Avira MailGate Suite +
Avira WebGate 12 месяцев 3 узлов сети	8 107
Avira MailGate Suite 12 месяцев 3 узлов сети	6 290
Avira Endpoint Security 12 месяцев 3 узлов сети	4 264
Avira Antivirus Premium 2012 12 месяцев 1 узлов сети	728
Avira Server Security 12 месяцев 3 узлов сети	2 978
Avira AntiVir SharePoint 12 месяцев 3 узлов сети	2 413
Avira Small Business Security Suite 12 месяцев 3 узлов сети.	5 913
Avira AntiVir WebGate 12 месяцев 3 узлов сети.	2 459
Avira WebGate Suite 12 месяцев 3 узлов сети	4 031
Avira Professional Security 12 месяцев 1 узлов сети.	970
Avira Small Business Security 2012 24 месяцев 5 узлов сети.	5 000
Avira Endpoint & Email Security 12 месяцев 3 узлов сети.	4 684

BARRACUDA

Barracuda Spam & Virus Firewall 100 6 Months EU	11 643
Barracuda Spam & Virus Firewall 100 1 Year EU	21 378
Barracuda Web Filter 210 1 Year EU.	21 378
Barracuda Link Balancer 230 1 Year EU	13 590
Barracuda Load Balancer 240 1 Year EU	13 590
Barracuda Message Archiver 150 1 Year EU	27 219
Barracuda Web App Firewall 360 1 Year EU.	73 947
Barracuda SSL-VPN 180 1 Year EU	11 643
Barracuda Backup Server 190 1 Year EU	11 643
Barracuda Control Server 665 1 Year EU	147 933
Yosemite Desktop/Laptop Backup Enterprise.	2 103
Yosemite Server Backup.	15 537
Yosemite Server Backup SBS/EBS	21 378
Yosemite Server Backup Plus.	38 901
Yosemite Server Backup Unlimited.	81 735

BITDEFENDER

Bitdefender Clent Security на 5-24 рабочих станций 1 год	1 318
Bitdefender Antivirus for mac - buisness edition на 5-24 рабочих станций 1 год	988
Bitdefender Antivirus Scaner на 5-24 рабочих станций 1 год	619
Bitdefender Security for Fle Servers на 5-24 рабочих станций 1 год	823
Bitdefender Security for Samba на 5-24 рабочих станций 1 год.	823
Bitdefender Security for SharePoint на 5-24 рабочих станций 1 год	594
Bitdefender Security for Exchange на 5-24 рабочих станций 1 год	988
Bitdefender Security for Mail Servers на 5-24 рабочих станций 1 год	988
Bitdefender Security for Isa Servers на 5-24 рабочих станций 1 год	594
Bitdefender Small Office Security на 5-24 рабочих станций 1 год	1 483
Bitdefender Buisness Security на 5-24 рабочих станций 1 год	1 647
Bitdefender Sbs Security на 5-24 рабочих станций 1 год	1 978
Bitdefender Corporate Security на 5-24 рабочих станций 1 год	2 206
Cloud Security for Endpoints by Bitdefender на 5-24 рабочих станций 1 год	1 351

Наименование	цена, руб.

CA

CA ARCserve Backup r16 for Windows	17 057
CA ARCserve Central Virtual Standby r16 per Host Licence.	20 759
CA ARCserve Backup r16 for Windows Advanced eMail Module	37 391
CA ARCserve Backup r16 for Windows Enterprise Application Module.	39 892
CA ARCserve Backup r16 for Windows Standard Database Module	34 890
CA ARCserve D2D r16 for Windows Server Advanced Edition	19 233
CA ARCserve D2D r16 for Windows Small Business Server Edition	12 005
CA ARCserve D2D r16 for Windows Workstation Edition - 25 Pack	39 662
ARCserve Replication and High Availability r16 Assured Recovery Option for Windows	14 306
CA ARCserve High Availability r16 for Windows Cluster Resource Group with Assured Recovery	110 557
CA ARCserve Replication r16 for Windows Cluster Resource Group with Assured Recovery	52 045
CA ARCserve Replication r16 for Windows Standard OS with Assured Recovery.	41 631
CA ARCserve Content Distribution r16 for Windows 1-50 Server Band	42 918

CBI

Программа фиксации и контроля исходного состояния программного комплекса ФИКС (версия 2.0.1) Лицензия (право на использование) на 1 год	2 220
Средство создания модели системы разграничения доступа Ревизор -1 XP Лицензия (право на использование) на 1 год	750
Программа контроля полномочий доступа к информационным ресурсам Ревизор– 2 XP Лицензия (право на использование) на 1 год	7 050
Средство автоматизированного моделирования СРД АРМ Ревизор - 1 для Linux Лицензия на 1 год	1 200
Средство проверки настроек СРД Ревизор – 2 для Linux Лицензия (право на использование) на 1 год	10 200
Программа фиксации и контроля целостности информации ФИКС-DOS 1.0 Лицензия (право на использование) на 1 год	600
Система анализа программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер Ревизор Сети версия 2.0) 1 – 5 IP-адресов Лицензия (право на использование) на 1 год.	5 000
Программа фиксации и контроля исходного состояния программного комплекса ФИКС (версия 2.0.2) Лицензия (право на использование) на 1 год	2 850
Программа исследования программного обеспечения EMU Лицензия (право на использование) на 1 год	299 300
Анализатор исходных текстов АИСТ-С Лицензия (право на использование) на 1 год	299 300
Программа расчета показателей защищенности конфиденциальной информации ГРОЗА-К версия 1.0 для Windows 9x/NT/2000/XP Лицензия (право на использование) на 1 год	6 800
Программа расчета показателей защищенности ПЭМИН-2005 Лицензия (право на использование) на 1 год	39 420
Агент инвентаризации Лицензия (право на использование) на 1 год	1 300
Астра 1.0 Лицензия (право на использование) на 1 год	2 700

CLEARSWIFT

MIMEsweeper for SMTP Standard 50 Users	69 409
MIMEsweeper for SMTP Advanced 50 Users.	100 663
MIMEsweeper for SMTP Enterprise 50 Users	183 918
EXCHANGE manager 50 Users	17 364
IMAGE manager 50 Users.	17 364
MIMEsweeper for SMTP Standard 50 Users Clearswift Support 24x7 1 Year	18 085

Наименование	цена, руб.
Clearswift MIMEsweeper SSS SecureIT Standard One Year Subscripion 50 Users	28 909
Clearswift MIMEsweeper SSS SecureIT Advanced One Year Subscripion 50 Users	41 943
Clearswift MIMEsweeper SSS SecureIT Enterprise One Year Subscripion 50 Users	76 625

CRYPTOPRO

СКЗИ КриптоПро CSP версии 3.6 на одном рабочем месте MS Windows	1 800
СКЗИ КриптоПро CSP версии 3.6 на сервере MS Windows	20 000
СКЗИ КриптоПро JCP на одном рабочем месте	800
СКЗИ КриптоПро eToken CSP с USB-ключом	2 200
СКЗИ КриптоПро Рутокен CSP.	2 100
ПО КриптоПро OCSP Server из состава ПАК Службы УЦ версии 1.5 на одном сервере.	100 000
ПО КриптоПро TSP Server из состава ПАК Службы УЦ 1.5 на одном сервере	100 000
ПО КриптоПро OCSP Client на одном рабочем месте	900
ПО КриптоПро TSP Client на одном рабочем месте.	900
ПО КриптоПро Revocation Provider на одном рабочем месте	900
ПО КриптоПро OCSP Client на одном рабочем месте	900
одной компоненты Центр Регистрации ПАК КриптоПро УЦ версии 1.5 класс КС3	234 000
ПО КриптоПро NET на одном рабочем месте	600
ПО КриптоПро NET на одном сервере.	10 000
ПО КриптоПро Office Signature.	600
КриптоПро EFS на одном рабочем месте	1 000
КриптоПро PDF на одном рабочем месте	15 000
ЭЦП-процессор в одной прикладной системе	16 200
КриптоПро Winlogon на одном рабочем месте.	900
КриптоПро Winlogon-KDC на одном сервере	20 000
Secure Pack Rus for Server версия 1.0 на одном сервере	9 300
Secure Pack Rus версия 1.0 на одном рабочем месте	3 150

DIGT

КриптоАРМ Стандарт	1 200
модуля TSP для КриптоАРМ Стандарт (включая лицензию на право использования КриптоПро TSP Client)	650
модуля OCSP для КриптоАРМ Стандарт (включая лицензию на право использования КриптоПро OCSP Client.	650
модуля Клиент УЦ.	360
КриптоАРМ СтандартPRO.	2 500
ПО Trusted Java for Windows Client 2.0	600
ПО Trusted Java for Windows Server 2.0.	9 000
ПО Trusted Java for IBM AIX Server 2.0.	60 000
ПО Trusted TLS for Windows 2.2.	16 000
ПО Trusted TLS for IBM AIX 2.2.	80 000
ПО Trusted TLS for CheckPoint Connectra R66.	30 000
ПО Trusted TLS for 1C-Bitrix 2.2	20 000
ПО Trusted TLS for Oracle 2.2	120 000
ПО Trusted Bitrix Login (версии 8.5, 9.5, 10.0).	7 200
ПО Trusted Bitrix Documents (версии 8.5, 9.5, 10.0)	10 800
ПО Trusted Login Kerberos версии 1.0 (сервер).	160 000
ПО Trusted Login Kerberos версии 1.0 (клиент).	600
ПО Trusted Login CA (УЦ) (сервер).	160 000
ПО Trusted Login CA (УЦ) (клиент).	600
ПО Trusted Records (сервер).	180 000
ПО Trusted Records (клиент).	500

DR. WEB

Dr.Web Security Space Pro 2 ПК/1 год	1 990
Антивирус Dr.Web Pro 2 ПК/1 год	1 290
Dr.Web Бастион Pro 2 ПК/1 год	2 290
Dr.Web Малый бизнес 5 ПК/1 сервер/ 5 пользователей почты.	4 990

ENTENSYS

UserGate Proxy & Firewall 5.X до 5 сессий.	4 500

Если вам не понравилось, как с вами общался наш менеджер, консультант, курьер или вы хотите посоветовать, как можно сделать обслуживание еще лучше, напишите об этом Председателю совета директоров Softline **Игорю Боровикову** (igorb@softline.ru)

Мы продаем продукцию более 1000 мировых производителей программного обеспечения, и эта цифра постоянно растет. Если вы не нашли в списке нужную компанию, отправьте запрос на info@softline.ru — вдруг она уже появилась?

IN.: Infotecs, Infragistics, InstallShield, Intel, InterAct, Intuit, Ipswitch, Irislink, iSleuthHound, ISS, ITNets, Jalasoft, JetBrains, JetInfosystems, JNetDirect, Jproductivity, Kaspersky, Kerio, KiwiEnterprises, Lahey, Legato, LinuxCenter, LiraServis, Loftware, Lumigent, LWP, Mackichan, Macromedia, Manakoa, MapleSoft, Markzware, MathSoft, Mathworks, McAfee, MDaemon, MediaHouse, MediaLingva, Megaputer, Merant, Microsoft, MicrosoftEA, MicrosoftEAS, MindJet, MKS, Mobiliti, MSAcademic, MSEmbedded, MySQL, NetIQ, NetManage, NetOp, NetSarang, NetSupport, net-Viz...

Наименование	цена, руб.
UserGate Proxy & Firewall 5.X с модулем фильтрации сайтов Entensys URL Filtering до 5 сессий	6 214
UserGate Proxy & Firewall 5.X + Антивирус Касперского до 5 сессий	7 170
Антивирус Касперского для UserGate Proxy & Firewall 5.X до 5 сессий	2 670
UserGate Proxy & Firewall 5.X + Panda Antivirus до 5 сессий	7 536
Panda Antivirus для UserGate Proxy & Firewall 5.X до 5 сессий	3 036
UserGate Proxy & Firewall 5.X + Антивирус Касперского + Panda Antivirus до 5 сессий	10 206
Антивирус Касперского + Panda Antivirus для UserGate Proxy & Firewall 5.X до 5 сессий	5 706
Модуль фильтрации сайтов по категориям (1 год) для UserGate Proxy & Firewall 5.X до 5 сессий	1 714
УКС UserGate Proxy & Firewall 5.X с 5 до 10 сессий	3 500
УКС UserGate Proxy & Firewall 5.X с 10 до 15 сессий	2 400

ESET

ESET NOD32 Антивирус + Vocabulary - на 1 год на 3ПК.	1 250
ESET NOD32 Антивирус + Bonus - лицензия на 1 год на 3ПК.	1 250
ESET NOD32 Антивирус - лицензия на 1 год на 3ПК	1 250
ESET NOD32 Антивирус Platinum Edition - лицензия на 2 года на 1ПК.	1 620
ESET NOD32 Антивирус - лицензия на 2 года на 1ПК.	1 620
ESET NOD32 Smart Security + Vocabulary - лицензия на 1 год на 3ПК.	1 790
ESET NOD32 Smart Security + Bonus - лицензия на 1 год на 3ПК.	1 790
ESET NOD32 Smart Security - лицензия на 1 год на 3ПК.	1 790
ESET NOD32 Smart Security Platinum Edition - лицензия на 2 года на 1ПК.	2 535
ESET NOD32 Smart Security - лицензия на 2 года на 1ПК	2 535
ESET NOD32 Mobile Security - лицензия на 1 год.	790
ESET NOD32 Mobile Security - лицензия на 2 года	1 185
ESET NOD32 Mobile Security - лицензия на 1 год на 1 мобильное устройство	790
ESET NOD32 Cybersecurity for MAC - лицензия на 1 год.	1 250
ESET NOD32 TITAN - лицензия на 1 ПК	2 250
Антивирус ESET NOD32 SMALL Business Pack newsale for 5 User	5 500
Антивирус ESET NOD32 Business Edition newsale for 5 User	9 340
ESET NOD32 Smart Security Business Edition newsale for 5 User	8 000
Антивирус NOD32 Exchange Mail Server newsale for 25 mailboxes	11 135
ESET NOD32 for KCT 20 users	7 036
ESET NOD32 for KCL 10 users	5 097

F-SECURE

F-Secure Anti-Virus for Workstations License for 1 Year (1-24)	1 096
F-Secure Client Security License for 1 Year (1-24)	1 316
F-Secure Email and Server Security License for 1 Year (1-24).	655
F-Secure Business Suite License for 1 Year (1-24)	2 122
F-Secure Mobile Security for Business License for 1 Year (1-24).	1 403
Protection Service for Business, Advanced Workstation Security License for 1 Year (1-24)	1 490
Protection Service for Business, Advanced Server Security License for 1 Year (1-24)	1 490
Protection Service for Business, Advanced E-mail and Server Security License for 1 Year (1-24)	406
Protection Service for Business, Advanced Mobile Security License for 1 Year (1-24)	1 403
Protection Service for Business, Standard Workstation Security License for 1 Year (1-24)	1 490
Protection Service for Business, Standard Server Security License for 1 Year (1-24)	1 490
Protection Service for Business, Standard E-mail and Server Security License for 1 Year (1-24)	406
Protection Service for Business, Standard Mobile Security License for 1 Year (1-24)	1 403
Protection Service for Email License for 1 Year (1-24)	1 161
Protection Service for Email with Encryption License for 1 Year (1-24),	1 626
F-Secure Messaging Security Gateway, Inbound Protection License for 1 Year (25-99)	1 376
F-Secure Messaging Security Gateway, Protection Bundle License for 1 Year (25-99)	1 912
F-Secure Messaging Security Gateway, Email Encryption License for 1 Year (25-99)	1 376
F-Secure Anti-Virus for Workstations subscription for 1 month (1-24)	100
F-Secure Client Security subscription for 1 month (1-24)	119
F-Secure Email and Server Security subscription for 1 month (1-24)	60
F-Secure Business Suite subscription for 1 month (1-24)	193
F-Secure Mobile Security for Business subscription for 1 month (1-24)	128
Protection Service for Business, Advanced Workstation Security subscription for 1 month (1-24),	194
Protection Service for Business, Advanced Server Security subscription for 1 month (1-24),	194
Protection Service for Business, Advanced E-mail and Server Security subscription for 1 month (1-24),	53
Protection Service for Business, Advanced Mobile Security subscription for 1 month (1-24),	128
Protection Service for Email subscription for 1 month (1-24)	105
Protection Service for Email with Encryption subscription for 1 month (1-24),	148
F-Secure Messaging Security Gateway, Inbound Protection subscription for 1 month (25-99)	125
F-Secure Messaging Security Gateway, Protection Bundle subscription for 1 month (25-99)	174
F-Secure Messaging Security Gateway, Email Encryption subscription for 1 month (25-99)	125

GFI

GFI FAXmaker including 1 year SMA from 5 to 9 Users (per User)	5 175
GFI FAXmaker - Options 2 Additional Lines including 1 year SMA	41 355
GFI MailArchiver including 1 year SMA from 10 to 24 Mailboxes (per Mailboxe)	1 440
GFI MailEssentials - Anti-Spam Edition - including 1 year SMA and SpamRazer updates from 10 to 24 Mailboxes (per Mailboxe)	1 013
GFI MailEssentials - EmailSecurity Edition - including 1 year SMA / VIPRE / BitDefender Updates from 10 to 24 Mailboxes (per Mailboxe)	765
GFI MailEssentials - UnifiedProtection Edition - including 1 year SMA / SpamRazer / VIPRE & BitDefender Updates from 10 to 24 Mailboxes (per Mailboxe)	1 373
Norman Anti-Virus Updates for GFI MailEssentials from 10 to 24 Mailboxes (per Mailboxe)	668
Kaspersky Anti-Virus Updates for GFI MailEssentials from 10 to 24 Mailboxes (per Mailboxe)	716
McAfee Anti-Virus Updates for GFI MailEssentials from 10 to 24 Mailboxes (per Mailboxe).	763
GFI EmailProtection Suite including 1 year SMA from 10 to 24 Mailboxes (per Mailboxe)	1 913
GFI WebMonitor for ISA/TMG - UnifiedProtection 1 year from 10 to 49 Seats (per Seat)	1 395
GFI WebMonitor for ISA/TMG - WebFilter 1 year from 10 to 49 Seats (per Seat).	810
GFI WebMonitor for ISA/TMG - WebSecurity 1 year from 10 to 49 Seats (per Seat).	720
GFI WebMonitor - UnifiedProtection for 1 year from 10 to 49 Seats (per Seat).	1 395
GFI WebMonitor - WebFilter for 1 year from 10 to 49 Seats (per Seat).	810
GFI WebMonitor - WebSecurity for 1 year from 10 to 49 Seats (per Seat).	720
GFI LanGuard including 1 year SMA and updates from 10 to 24 IPs (per IPs).	1 440
GFI EventsManager for Servers including 1 year SMA from 1 to 9 Servers (per Server)	12 555
GFI EventsManager for Workstations including 1 year SMA from 10 to 24 Workstations (per Workstation).	1 305
GFI EndPointSecurity including 1 year SMA from 10 to 24 Computers (per Computer)	1 181
GFI Network Server Monitor including 1 year SMA from 10 to 24 IPs (per IPs).	4 455
GFI VIPRE - Business Standard (1 year SMA including Content updates) 5 Users (per User)	908
GFI VIPRE - Business Premium (1 year SMA including Content update) 5 Users (per User).	1 125
GFI VIPRE - Email Security for Exchange (1 year SMA including Content update) 5 Users (per User)	1 294
GFI MailEssentials Online for 1 year from 1 to 9 Users (per User)	428

INFOWATCH

EgoSecure Access Control 1 Year	400
EgoSecure Audit 1 Year	400
EgoSecure Removable Device Encryption 1 Year	400
EgoSecure Application Control 1 Year.	400
EgoSecure Power Management 1 Year	400
EgoSecure Endpoint Total Solution 1 Year	1 500
EgoSecure Endpoint Base Solution 1 Year	900

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Anti-Virus 2013 Russian Edition. 2-Desktop 1 year Base Box	1 200
Kaspersky Internet Security 2013 Russian Edition. 2-Desktop 1 year Base Box	1 600
Kaspersky CRYSTAL 2.0 Russian Edition. 2-Desktop 1 year Base Box	2 200
Kaspersky Anti-Virus 2012 Russian Edition. 2-Desktop 1 year Base Box	1 200
Kaspersky Internet Security 2012 Russian Edition. 2-Desktop 1 year Base Box	1 600
Kaspersky Small Office Security 2 for Personal Computers Russian Edition. 5-Workstation 1 year Base License Pack.	4 900
Kaspersky Small Office Security 2 for Personal Computers and File Servers Russian Edition. 5-Workstation + 1-FileServer 1 year Renewal License Pack.	3 540
Kaspersky Security for Virtualization, Desktop Russian Edition. 10-14 VirtualWorkstation 1 year Base License.	880
Kaspersky Anti-Virus for Storage Russian Edition. 10-14 Node 1 year Base License	737
Kaspersky Security for Virtualization, Server Russian Edition. 1-VirtualServer 1 year Base License.	3 230
Kaspersky Security for Mail Server Russian Edition. 10-14 User 1 year Base License.	1 065
Kaspersky Security for Collaboration Russian Edition. 10-14 User 1 year Base License.	765
Kaspersky Security for Internet Gateway Russian Edition. 10-14 User 1 year Base License.	574
Kaspersky DDoS Prevention, Basic Level Russian Edition. 1-Resource 1 year Base License	653 400
Kaspersky DDoS Prevention, Standard Level Russian Edition. 1-Resource 1 year Base License	1 009 800
Kaspersky DDoS Prevention, Advanced Level Russian Edition. 1-Resource 1 year Base License	1 425 600
Kaspersky DDoS Prevention, Ultimate Level Russian Edition. 1-Resource 1 year Base License	2 138 400
Kaspersky DDoS Prevention, Reports Option Russian Edition. 1-Resource 1 year Base License	300 000
Kaspersky DDoS Prevention, Logs Option Russian Edition. 1-Resource 1 year Base License	300 000
Kaspersky Anti-Spam for Linux Russian Edition. 10-14 User 1 year Base License.	378
Kaspersky WorkSpace Security Russian Edition. 10-14 User 1 year Base License.	1 144
Kaspersky BusinessSpace Security Russian Edition.	

Если вам не понравилось, как с вами общался наш менеджер, консультант, курьер или вы хотите посоветовать, как можно сделать обслуживание еще лучше, напишите об этом Председателю совета директоров Softline **Игорю Боровикову** (igorb@softline.ru)

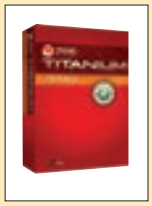
Microsoft SQL Server Standard Edition 2012

Надежная, эффективная и интеллектуальная платформа управления данными

123 382 руб.

Trend Micro Titanium Antivirus 2012

Надежный антивирус и антишпион, способный защищать ПК в реальном времени



1 099 руб.

Citrix XenApp 6.0

Стандарт дефакто в области потоковой доставки и виртуализации Windows приложений

10 976 руб.

MathCAD 15 Professional

ПО для решения самых сложных инженерных и математических задач

Звоните!

Autodesk AutoCAD 2013

Система проектирования, для построения чертежей и внесения в них изменений

122 720 руб.

Norton Internet Security 2012

Интегрированный набор средств сетевой безопасности для комплексной защиты ПК

1 172 руб.

Microsoft Exchange Server Standard

Интегрированное корпоративное решение для обмена сообщениями и совместной работы

50 101 руб.

ESET NOD32 Антивирус 5

Простое и надежное антивирусное ПО для базовой защиты домашнего компьютера.

1 080 руб.

Embarcadero RAD Studio XE 2

Комплексное решение для быстрой разработки Windows . и .NETприложений.

44 768 руб.

Symantec Norton 360 v 5.0

Защита по всем направлениям: web, почта, IMсистемы, . P2Pсети . и мобильные рабочие станции

1 612 руб.

Adobe Acrobat X

Современное средство подготовки и распространения документов PDF

12 256 руб.

Oracle Database Standard Edition One

Доступная и многофункциональная база данных для СМБ

от 5 760 руб.

Kaspersky Internet Security 2012

Оптимальное решение для борьбы с вирусами и интернет. угрозами.

1 600 руб.

Famatech Radmin 3.4

Быстрое и надежное решение для удаленного управления ПК

1 250 руб.

Мы продаем продукцию более 1000 мировых производителей программного обеспечения, и эта цифра постоянно растет. Если вы не нашли в списке нужную компанию, отправьте запрос на info@softline.ru — вдруг она уже появилась?

NS.: NetwokAutomation, NetworkInstruments, Nevron, NewDisk, Novalumen, Novell, Nsoftware, NTPSoftware, Ontrack, OOsoftware, Optima, Oracle, Paessler, Panda, Panorama, Paragon, Paratype, Pervasive, PGP, PhotoAlto, PhotoDisc, PixMaker, Pixtal, Portlock, ProInvest, ProjectViewer, ProLAN, Promt, Pytheas, QuantitativeMicro, Quark, Quest, RARSoft, Rational, RealNetworks, RedHat, RightFax, Rodnik, Roxio, RSASecurity, Ruscard, Sakrament, SCAD Soft, SCO, SeagulScientific, Seapine, SecurIT, SecurStar, Serif, Shavlik, SIM, Skywire, SmartDraw, SmartLine, SoftExport, SoftTreeTech, SolarWinds, SonicWall, Sophos, SparxSystems, StarForce, StarNet, Stata, StatSoft...

KERIO

Наименование	цена, руб.
10-14 User 1 year Base License	1 581
Kaspersky EnterpriseSpace Security Russian Edition. 10-14 User 1 year Base License	2 415
Kaspersky TotalSpace Security Russian Edition. 10-14 User 1 year Base License	4 715
Kerio Connect 7 Server 5 users License	17 999
Kerio Control Server 5 users License	10 257
Kerio Operator Server 5 users License	5 806
Kerio Workspace Server 5 users License	5 806
Пакет Kerio Connect с а/в Sophos + Kerio Workspace Server с а/в Sophos (включают лицензии на оба продукта для 5 пользователей) License	21 484
Kerio Connect + Kerio Control (Standard) Standard License	21 190

КОД БЕЗОПАСНОСТИ

Наименование	цена, руб.
Средства защиты информации Secret Net 6 (версия 6.5, автономный режим)	6 400
Средства защиты информации Secret Net 6 (версия 6.5). Сервер безопасности класса С	35 200
Средства защиты информации Secret Net 6 (версия 6.5). Сервер безопасности класса В	88 500
Средства защиты информации Secret Net 6 (версия 6.5). Сервер безопасности класса А	172 000
Средства защиты информации Secret Net 6 (версия 6.5). Клиент (сетевой режим). за 1 клиента при покупке 1-10 клиентов	7 100
Системы защиты информации Secret Net 5.1 (автономный вариант)	6 400
Системы защиты информации Secret Net 5.1. Сервер безопасности класса С	35 200
Системы защиты информации Secret Net 5.1. Сервер безопасности класса В	88 500
Системы защиты информации Secret Net 5.1. Сервер безопасности класса А	172 000
Программно-аппаратный комплекс Соболь (версия 3.0), PCI сертифицированный ФСТЭК России	8 220
Программно-аппаратный комплекс Соболь (версия 3.0), PCI сертифицированный ФСБ России	8 220
Средство Защиты Информации Security Studio 6 - Trusted Boot Loader	2 000
АПКШ Континент 3.6. ЦУС. Платформа IPC-1010	690 000
АПКШ Континент 3.6. ЦУС - Сервер Доступа. Платформа IPC-1010	716 800
АПКШ Континент 3.6. Крипто Шлюз. Платформа IPC-1010	665 000
АПКШ Континент 3.6. Сервер Доступа. Платформа IPC-1010	691 800
ЦУС Континент 3.6 (1 дополнительное подключение КШ к ЦУС Континент 3.6)	3 500
программного продукта Сервер Доступа АПКШ Континент 3.6, с правом использования КриптоПро CSP 3.6.	26 800
TrustAccess для защиты 1 сервера (от 1 до 10 шт.)	14 000
TrustAccess для защиты 1 рабочей станции (от 1 до 50 шт.)	3 000
TrustAccess-S для защиты 1 сервера (от 1 до 25 шт.)	50 000
TrustAccess-S для защиты 1 рабочей станции (от 1 до 50 шт.)	8 500
Сервера авторизации vGate R2 (за 1 экземпляр Сервера авторизации vGate).	89 000
резервного Сервера авторизации vGate R2 (за 1 экземпляр Сервера авторизации vGate).	89 000
vGate R2 для защиты ESX-хостов (за 1 физический процессор на защищаемом ESX-хосте)	24 500
vGate R2 для защиты одной виртуальной машины, за месяц.	150
Код Безопасности: Инвентаризация версия 2 (до 30 PM)	29 100

LUMENSION

Наименование	цена, руб.
L.E.M.S.S. Platform with Learning Center	98 835
Lumension Device Control 25-99 Licenses	1 148
Lumension Application Control 25-99 Licenses	2 313
Lumension Patch & Remediation - Windows 25-99 Licenses	1 818
Lumension AntiVirus 25-99 Licenses	1 485
Lumension Content Wizard 25-99 Licenses	627
Lumension Enterprise Reporting 25-99 Licenses	333
Lumension Power Management Reporting 25-99 Licenses	660
Lumension Security Configuration Management 25-99 Licenses	660
Lumension Scan 25-99 Licenses	746
Lumension Device Control 10-249 Licenses	1 069
Lumension Application Control 10-249 Licenses	1 706
Lumension Application Control Server Edition 1-9 Licenses	33 660
Lumension Application Control Terminal Services Edition 1-9 Licenses	53 460

MCAFEE

Наименование	цена, руб.
MFE TotalPrtxn forEndpt-Ent.Ed.P:1GL[P+] 11-25 A ProtectPLUS	5 903
MFE Endpoint Protection - Adv P:1 GL[P+] 11-25 A ProtectPLUS	2 984
MFE Total Protection fr SecBus P:1GL[P+] 11-25 A ProtectPLUS	3 580
MFE Total Protection for ServerP:1GL[P+] 1-25 A ProtectPLUS	36 527
MFE SaaS Total Protection 1:1 GL 5-25 A	2 127
MFE SaaS Endpt & Email Protection 1:1 GL 5-25 A	1 532
MFE SaaS Endpoint Protection Adv 1:1GL 5-25 A	1 129
MFE SaaS Endpoint Protection 1:1GL 2-25 A	895
MFE Vulnerabilty Assessment SVC 1:1 GL 1-+ A	2 598
MFE HIP for Desktops P:1 GL [P+] 1-25 A ProtectPLUS	861
MFE HIP for Svrs P:1 GL [P+] 1-25 A ProtectPLUS	28 038
MFE Web Filtering for Endpt P:1 GL (P+) 11-25 A ProtectPLUS	422
MFE ePolicy Orchestrator P:1 GL [P+] 11-25 A ProtectPLUS	645
MFE Network Access Control P:1 GL [P+] 11-25 A ProtectPLUS	1 220
MFESec/MS Exch/LotusD MSw/Epo P:1GL[P+] 11-25 A ProtectPLUS	973
MFE Anti Spam for GSS P:1 GL [P+] 11-25 A ProtectPLUS	758
MFE Endpoint Protection fr Mac P:1GL[P+] 11-25 A ProtectPLUS	2 275
MFE Virusscan for MAC P:1 GL [P+] 11-25 A ProtectPLUS	936
MFE Sec for MS SharePoint P:1 GL [P+] 11-25 A ProtectPLUS	724
MFE MOVE AntiVirus for Virtual DsktopsP:1GL[P+] 11-25 A ProtectPLUS	889
MFE Virusscan Suite Virtualization P:1 GL 1-10 A	38 272
MFE VS for MAC Student Use LIC 1:1 Sp 5-+ A	13
MFE eBusiness Server P:1 GL 1-1 A	336 000
MFE Anti-Spyware P:1 GL [P+] 11-25 A ProtectPLUS	512
MFE Total Prtxn for Endpt-Adv P:1GL[P+] 11-25 A ProtectPLUS	3 412
MFE Total Prtxn for Endpoint P:1 GL[P+] 11-25 A ProtectPLUS	2 984
MFE Total Prtxn Endpt-Essen P:1 GL [P+] 11-25 A ProtectPLUS	2 275
MFE Active Virus Defense P:1 GL [P+] 11-25 A ProtectPLUS	2 275
MFE Active Virusscan P:1 GL [P+] 11-25 A ProtectPLUS	1 317
MFE Content Security Suite1:1 GL 11-25 A	968
MFE Web Protection Suite 1:1 GL 11-25 A	880
MFE Cloud Identity Manager 1:1GL 11-25 A	1 890
MFE Services Gateway 1:1GL 1-+ A	1 113 600
MFE Web Security P:1 GL 11-25 A	2 258
MFE Web Anti-Malware P:1 GL 11-25 A	1 411
MFE Email Protection Suite1:1 GL 11-25 A	659
MFE VirtualPatching f/Databases 1:1GL 1-25 A	28 160

MICROSOFT

Наименование	цена, руб.
Forefront TMG Standard 2010 64Bit English DVD 1 Proc	58 079
Forefront TMG Standard 2010 64Bit Russian DVD 1 Proc	58 079
Forefront UAG Server 2010 Single OLP NL	199 297
Forefront UAG CAL 2010 Single OLP NL Device CAL	461
Forefront UAG CAL 2010 Single OLP NL User CAL	461
Forefront UAG External Connector 2010 Single OLP NL Qlfd	1 042 452
Forefront TMG Enterprise 2010 Russian OLP NL 1Proc	177 463
Forefront TMG Enterprise 2010 Single OLP NL 1Proc	177 463
Forefront TMG Enterprise 2010 Single OLP 25License C 1Proc	2 239 886
Forefront TMG Enterprise 2010 Single OLP 25License NL 1Proc	2 285 597
Forefront TMG Enterprise 2010 Russian OLP 25License C 1Proc	2 239 886
Forefront TMG Enterprise 2010 Russian OLP 25License NL 1Proc	2 285 597
Forefront TMG Standard 2010 Russian OLP NL 1Proc	40 368
Forefront TMG Standard 2010 Single OLP NL 1Proc	40 368
Forefront Identity Manager 2010R2 Single OLP NL	457 120
Forefront Identity Manager CAL 2010R2 Single OLP NL User CAL	549
Forefront Identity Manager External Connector 2010R2 Single OLP NL Qlfd	563 781
Forefront TMG Mid Business Russian OLP NL 1Proc	39 885
Forefront TMG Mid Business Single OLP NL 1Proc	39 885

PANDA

Наименование	цена, руб.
Panda Internet Security 2012 for Netbooks	1 480
Panda Antivirus Pro 2012	1 080
Panda Internet Security 2012	1 600
Panda Global Protection 2012	1 960
Panda Antivirus Pro 2012 - Пакет на 5 лицензий для SMB	2 919
Panda Internet Security 2012 - Пакет на 5 лицензий для SMB	5 619
Panda Global Protection 2012 - Пакет на 5 лицензий для SMB	6 488
Panda Security for Enterprise 2 - 25 лицензий	1 504
Panda Security for Business with Exchange 2 - 25 лицензий	1 310
Panda Security for Business 2 - 25 лицензий	1 156
Panda Security for Desktops 2 - 25 лицензий	854
Panda Security for File Servers 2 - 25 лицензий	474
Panda Security for Exchange Servers 2 - 25 лицензий	481
Panda Security for Domino Servers 2 - 25 лицензий	401
Panda Security for CommandLine 2 - 25 лицензий	155
Panda Security for ISA Servers 2 - 25 лицензий	258
Panda Security for Sendmail 2 - 25 лицензий	168
Panda Security for Qmail 2 - 25 лицензий	168

POSITIVE TECHNOLOGIES

Наименование	цена, руб.
XSpider 7.8, лицензия на 4 хоста	9 000
XSpider 7.8, лицензия на 4 хоста, Дополнительный хост	2 000

RSA SECURITY

Наименование	цена, руб.
RSA SecurID Appliance Bundle For 25 Users	296 645
RSA SecurID Appliance 130 Hardware (includes Advanced Hardware Replacement for Years 1-3)	139 950
RSA SecurID Appliance Base Software License per User for qty's between 10 - 25	4 299
RSA SecurID Appliance Enterprise Software License per User for qty's between 10 - 25	5 794
RSA SecurID Appliance Enterprise Plus per User for qty's between 5,000 - 10,000	2 336
RSA SecurID Authenticator On-demand per User for qty's between 10 - 250	1 157
RSA SecurID 3 Year Business Continuity Option per User qty's between 5 - 250	3 271
RSA Authentication Manager Base Edition per User for qty's between 10 - 25	4 299
RSA Authentication Manager Enterprise Edition per User for qty's between 10 - 25	5 794
RSA Authentication Manager Enterprise Plus per User for qty's between 5,000 - 10,000	2 336
RSA SecurID Authenticator On-demand per User for qty's between 10-250	1 157

Если вам не понравилось, как с вами общался наш менеджер, консультант, курьер или вы хотите посоветовать, как можно сделать обслуживание еще лучше, напишите об этом Председателю совета директоров Softline **Игорю Боровикову** (igorb@softline.ru)

Мы продаем продукцию более 1000 мировых производителей программного обеспечения, и эта цифра постоянно растет. Если вы не нашли в списке нужную компанию, отправьте запрос на info@softline.ru — вдруг она уже появилась?

SZ.: Stbernard, Steema, Stockbyte, Stocona, Strata, Stringbean, StroyEkspertiza, SumTotal, Sunbelt, Sun Microsystems, SurfControl, Sybari, Sybase, Symantec, Synfusion, Systat, TechnoDesign, Techsmith, Telerik, Telocator, TheBat, ThinPrint, Timberlake, TMU, Tobit, Tor, TotalCommander, Trados, TrafficFilter, Trapcode, TrendMicro, TriCerat, TrollTech, TurboDemo, TWDIndustries, Ulead, Ultrabac, UserGate, Utimaco, VectorNetworks, VentaFax, Vintela, VMware, Websense, WebSpy, Webtrends, WildPackets, WinGate, WinProxy, Winternals, WinZip, WMSoftware, Wolfram Research, Worldnet21, WRQ, Xara, Yandex, Yosemite, Zend.

Наименование	цена, руб.
RSA SecurID 3 Year Business Continuity Option per User qty's between 5-250	3 271
RSA SecurID Select one time fee for qty's between 1 - 999	77 880
RSA SecurID Select per User for qty's between 1000 - 50000	78
RSA SecurID Select Key Sheet Artwork	253 110
RSA SecurID Authenticator SD200 (24 months) 5 Pack	11 682
RSA SecurID Software Token Seeds (6 month) per User for qty's between 10 - 250	900

SMARTLINE

DeviceLock V7.1 Base 5 to 24 Licenses (per client)	1 500
DeviceLock V7.1 NetworkLock 5 to 24 Licenses (per client)	900
DeviceLock V7.1 ContentLock 5 to 24 Licenses (per client)	1 800
DeviceLock V7.1 DLP Suite 5 to 24 Licenses (per client)	4 200
DeviceLock Search Server 50K	11 000

STONESOFT

Аппаратная платформа StoneGate FW-105-C1	7 995
Право на использование программного обеспечения StoneGate FP-1Y-WF2-202, сроком на 12 мес.	4 551
Базовый пакет сертифицированного ПО StoneGate FW для StoneGate FW 105	8 200
Аппаратная платформа StoneGate FW-105-C2	11 029
Право на использование программного обеспечения StoneGate FW-105-C2	18 491

SYMANTEC ALTIRIS

SYMC WORKSPACE VIRTUALIZATION 6.1 WIN PER NODE BNDL	2 044
SYMC WORKSPACE STREAMING 6.1 WIN PER NODE BNDL	3 180
ALTIRIS Deployment Solutions for SERVERS 7.1 XPLAT PER NODE BNDL	8 085
ALTIRIS Deployment Solutions for THIN CLIENTS 6.9 XPLAT PER NODE BNDL	1 590
SYMC WORKSPACE VIRTUALIZATION for TERMINAL SERVERS 6.1 WIN PER CONCURR User BNDL	4 088
SYMC WORKSPACE STREAMING for TERMINAL SERVERS 6.1 WIN PER CONCURR User BNDL	6 177
SYMC SERVICEDESK ANALYST 7.1 WIN PER CONCURR User BNDL	280 703
SYMC SERVICEDESK BASE 7.1 WIN PER Enterprise BNDL	1 403 515
ALTIRIS Deployment Solutions for SOLARIS 1.0 SOL PER NODE BNDL	18 123
ALTIRIS PATCH Management Solutions for CLIENTS 7.1 XPLAT PER NODE BNDL	1 363
ALTIRIS PATCH Management Solutions for SERVERS 7.1 XPLAT PER NODE BNDL	3 225
ALTIRIS SOFTWARE Management for CLIENTS AND SERVERS 7.1 XPLAT PER NODE BNDL	2 089
SYMC MOBILE Management 7.2 PER NODE BNDL	2 816
ALTIRIS INVENTORY Solutions 7.1 XPLAT PER NODE BNDL	1 544
ALTIRIS BARCODE Solutions 7.1 XPLAT PER DEVICE BNDL	135 673
ALTIRIS INVENTORY Pack for SERVERS 7.1 XPLAT PER NODE BNDL	1 681
ALTIRIS Server Management Suite 7.1 XPLAT PER NODE BNDL	18 668
ALTIRIS PCANYWHERE Solutions 12.6 XPLAT PER NODE BNDL MULTI LIC Express BAND S BASIC 12 MONTHS	2 180
ALTIRIS IT Management Suite 7.1 XPLAT PER NODE BNDL	10 492
SYMC MOBILE Management for CONFIGURATION MANAGER 7.2 PER NODE BNDL	2 816
ALTIRIS Deployment Solutions for CLIENTS with REMOTE 7.1 XPLAT PER NODE BNDL	2 180
ALTIRIS ASSET Management Suite 7.1 XPLAT PER CONCURR User BNDL	795 325
ALTIRIS Client Management Suite 7.1 XPLAT PER NODE BNDL	4 315

Наименование	цена, руб.
SYMC Backup Exec 2012 Small Business Edition Agent for Windows Windows PER Server BNDL	21 663
SYMC SYSTEM Recovery Small Business Server 2011 Windows PER Server BNDL	13 488
SYMC Backup Exec 2012 Agent for APPLICATIONS And Databases Windows PER Server BNDL	27 113
SYMC Backup Exec 2012 Enterprise Server OPTION Windows PER MANAGED Server BNDL	81 612
SYMC Backup Exec 2012 Agent for Macintosh MAC PER Server BNDL	10 763
SYMC Backup Exec 2012 Server Windows PER Server BNDL	27 113
SYMC DESKTOP LAPTOP OPTION 7.0 Windows 1-10 Users BNDL	13 488
SYMC Backup Exec 2012 V-RAY Edition Windows 8 Plus CORES PER CPU BNDL	78 887
SYMC Backup Exec 2012 V-RAY Edition Windows 2 To 6 CORES PER CPU BNDL	44 008
SYMC Backup Exec 2012 Agent for Windows Windows PER Server BNDL	16 213
SYMC SYSTEM Recovery Linux Edition 2011 LNX PER Server BNDL	13 488

SYMANTEC CLOUD

MESSAGELABS EMAIL SAFEGUARD.CLOUD From 0 To 49 Users	135
MESSAGELABS EMAIL AND WEB SAFEGUARD.CLOUD From 0 To 49 Users	221
MESSAGELABS SECURITY SAFEGUARD.CLOUD From 0 To 49 Users	247
MESSAGELABS EMAIL PROTECT.CLOUD From 0 To 49 Users	122
MESSAGELABS EMAIL SAFEGUARD.CLOUD From 0 To 49 Users	135
MESSAGELABS EMAIL ANTI-VIRUS.CLOUD From 0 To 49 Users	154
MESSAGELABS EMAIL ANTI-SPAM.CLOUD From 0 To 49 Users	154
MESSAGELABS EMAIL CONTENT CONTROL.CLOUD From 0 To 49 Users	147
MESSAGELABS EMAIL IMAGE CONTROL.CLOUD From 0 To 49 Users	147
MESSAGELABS WEB V2 PROTECT AND CONTROL.CLOUD From 0 To 49 Users	226
MESSAGELABS WEB V2 PROTECT.CLOUD From 0 To 49 Users	150
MESSAGELABS ENDPOINT PROTECTION.CLOUD From 5 To 24 Users	111

SYMANTEC SECURITY

Norton AntiVirus 2012 Russian 1 User 3Licence MM	880
Norton Internet Security 2012 Russian 1 User 3Licence MM	1 172
Norton 360 5.0 Russian 1 User 3Licence MM	1 612
SYMC ENDPOINT Protection Small Business Edition Small Business Edition 12.0 Russian CD 5 User BNDL Business Pack BASIC 12 MO	3 422
Norton SYSTEMWORKS BASIC Edition 12.0 In CD 1 User RET	1 208
Norton Partition magic 8.0 R1 CD In RET	1 888
Norton Personal Firewall Macintosh 3.0 NODE BNDL	3 207
SYMC AntiVirus for Caching 5.2 User BNDL	432
SYMC AntiVirus for MESSAGING 5.2 User BNDL	490
SYMC AntiVirus for Network Attached Storage 5.2 User BNDL	549
SYMC AntiVirus 4.3 for Microsoft ISA SVR BNDL	488
SYMC Scan Engine 5.2 1 User BNDL	532
SYMC ENDPOINT Encryption 8.2 PER DEVICE BNDL	5 401
SYMC ENDPOINT Encryption DEVICE CONTROL 8.2 Windows PER DEVICE BNDL	1 845
SYMC ENDPOINT Encryption FULL DISK 8.2 PER DEVICE BNDL	4 921
SYMC ENDPOINT Encryption REMOVABLE Storage 8.2 PER DEVICE BNDL	1 845
SYMC ENDPOINT Protection 12.1 PER User BNDL	1 070
SYMC ENDPOINT Protection for XP EMBEDDED 5.1 Windows User BNDL	1 070
SYMC ENDPOINT Protection MOBILE Edition 6.0 XPLAT PER DEVICE BNDL	725
SYMC ENDPOINT Protection Small Business Edition 12.1 PER User BNDL	660
SYMC Mail SECURITY for Domino 8.1 PER User BNDL	893
SYMC Mail SECURITY for MS Exchange AntiVirus 6.5 Windows 1 User BNDL	804
SYMC Mail SECURITY for MS Exchange AntiVirus And Antispam 6.5 Windows 1 User BNDL	1 183
SYMC MOBILE SECURITY Suite for Windows 5.1 Windows BNDL	1 450
SYMC Network ACCESS CONTROL MOBILE Edition 6.0 XPLAT PER DEVICE BNDL	622
SYMC Network ACCESS CONTROL STARTER Edition 12.1 PER User BNDL	611
SYMC Protection for SHAREPOINT Servers 6.0 PER User BNDL	292
SYMC Protection Suite Advanced Business Edition 4.0 PER User BNDL Multi	1 554
SYMC Protection Suite Enterprise Edition 4.0 PER User BNDL Multi	2 065
SYMC Protection Suite Small Business Edition 4.0 PER User BNDL Multi	885

SYMANTEC VERISIGN

QuickSSL Premium 1 Year	5 808
RapidSSL 1 Year	1 914
Secure Site 1 Year	15 543
Secure Site Professional 1 Year	38 775
Secure Site with EV 1 Year	38 775
SGC SuperCerts 1 Year	27 225
SSL Web Server 1 Year	9 702
SSL Web Server Wildcard 1 Year	29 733
SSL Web Server with EV 1 Year	23 331
SSL123 1 Year	5 808
thawte Code Signing 1 Year	11 649
True BusinessID 1 Year	7 755
True BusinessID SAN Pakage w Certification 1 Year	7 755
True BusinessID w EV SAN Pakage w Certification 1 Year	11 649
True BusinessID Wildcard 1 Year	19 437
True BusinessID with EV 1 Year	11 649
VeriSign Code Signing 1 Year	19 437
VeriSign Trust Seal 1 Year	11 649

TREND MICRO

Trend Micro Titanium Antivirus + 2012 12 mths 3 Users	1 099
Trend Micro Titanium Internet Security 2012 12 mths 3 Users	1 374
Trend Micro Titanium Maximum Security 2012 12 mths 3 Users	1 648

WINGATE

WinGate 7.x Standard 3 concurrent users	2 919
WinGate 7.x Professional 6 concurrent users	6 423
WinGate 7.x Enterprise 6 concurrent users	8 760
WinGate VPN 7.x single User license	2 140
WinGate VPN 7.x gateway license for 3 computer LAN	2 919
WinGate VPN 7.x single User license multi-pack (5 installations)	9 733
PureSight for WinGate 7.x 3 User 1 yr Subscription	2 726
Kaspersky AntiVirus for WinGate 7.x 3 User 1 yr Subscription	2 726
NetPatrol Standard	9 733
NetPatrol Enterprise	19 468
SMS Connector for WinGate	1 945

Обратите внимание!
Цена не включает стоимость доставки.

Если вам не понравилось, как с вами общался наш менеджер, консультант, курьер или вы хотите посоветовать, как можно сделать обслуживание еще лучше, напишите об этом Председателю совета директоров Softline **Игорю Боровикову** (igorb@softline.ru)

Знания — ваш главный козырь

Каждый месяц мы проводим специализированные мероприятия по программному обеспечению ведущих производителей совершенно бесплатно!

Семинары и вебинары Softline — это:

— квалифицированные докладчики. У нас выступают ведущие российские и западные специалисты компаний-разработчиков программного обеспечения и признанные эксперты;

— богатый комплект раздаточных материалов;

— удобное место проведения и отличная организация.

Предварительная регистрация обязательна. Зарегистрироваться для участия и получить более подробную информацию о предстоящих семинарах в Москве и региональных центрах можно на сайте: seminars.softline.ru

Пишите нам: seminars@softline.ru

softline®

RISSPA СЕМИНАРЫ

BE PROFESSIONAL ОБМЕН ОПЫТОМ

СООБЩЕСТВО ПРОФЕССИОНАЛОВ

ПОДКАСТЫ БЛОГИ ЭКСПЕРТОВ НОВОСТИ

АКТУАЛЬНЫЕ ТЕМЫ **WWW.RISSPA.RU**

ОНЛАЙН МАСТЕР-КЛАССЫ НОВЫЕ ЗНАНИЯ

НОВЫЕ ВОЗМОЖНОСТИ КАЛЕНДАРЬ СОБЫТИЙ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ **ОНЛАЙН И ОЧНО**

ПОЛЕЗНЫЕ ЗНАКОМСТВА

НОВЫЕ ИДЕИ ДИСКУССИОННЫЕ ГРУППЫ

RISSPA

be professional

www.risspa.ru