softline direct

20 лет в IT

КАТАЛОГ ПРОГРАММНЫХ РЕШЕНИЙ НОЯБРЬ 2013

Специальный выпуск

Информационная безопасность

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**

спецвыпуск
информационная безопасность

softline DIRECT НОЯБРЬ 2013

КАТАЛОГ ПРОГРАММНЫХ РЕШЕНИЙ

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 программных решений Softline direct

НОЯБРЬ 2013-11(141)**-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 ФС77-23773
Отпечатано в типографии «ScanWeb», Финляндия

SoftlineCompany Softlinegroup

SOFTLINE

Почему большинство клиентов выбирает Softline в качестве поставщика программного обеспечения, обучения и IT-услуг?

1 Надежность и профессионализм

Компания Softline работает на рынке программного обеспечения с 1993 года. В настоящий момент мы — лидирующая компания в этом сегменте рынка IT. Сегодня в компании работает более 1700 человек, оборот составляет свыше $456 млн. У нас самый широкий ассортимент программного обеспечения (более 3000 производителей). Соответствие нашей системы менеджмента качества стандарту ISO 9001 документально подтверждает качественное выполнение работ и высокий уровень надежности компании.

2 Softline — авторизованный партнер крупнейших мировых производителей

Softline обладает высшими статусами партнерства ведущих поставщиков программных решений, таких как Microsoft, Oracle, SAP, Symantec, Citrix, Adobe, Corel, Check Point, Trend Micro, «Лаборатория Касперского» и многих других. Приведем статусы, полученные Softline за время сотрудничества с компанией Microsoft:

- статус Microsoft Partner с 11 компетенциями Gold (лицензирование, интеграция приложений, CRM и др.) и 7 компетенциями Silver.
- Microsoft Large Account Reseller — позволяет работать с крупными (более 250 ПК) компаниями по специальным условиям лицензирования.

3 Консалтинг и обучение

Softline предлагает заказчикам весь спектр услуг по внедрению программного обеспечения и обучению пользователей. Учебный центр Softline занимает лидирующее положение на рынке образовательных услуг в области IT. Консалтинговое подразделение обладает уникальным опытом по внедрению и развертыванию инфраструктурных и специализированных решений.

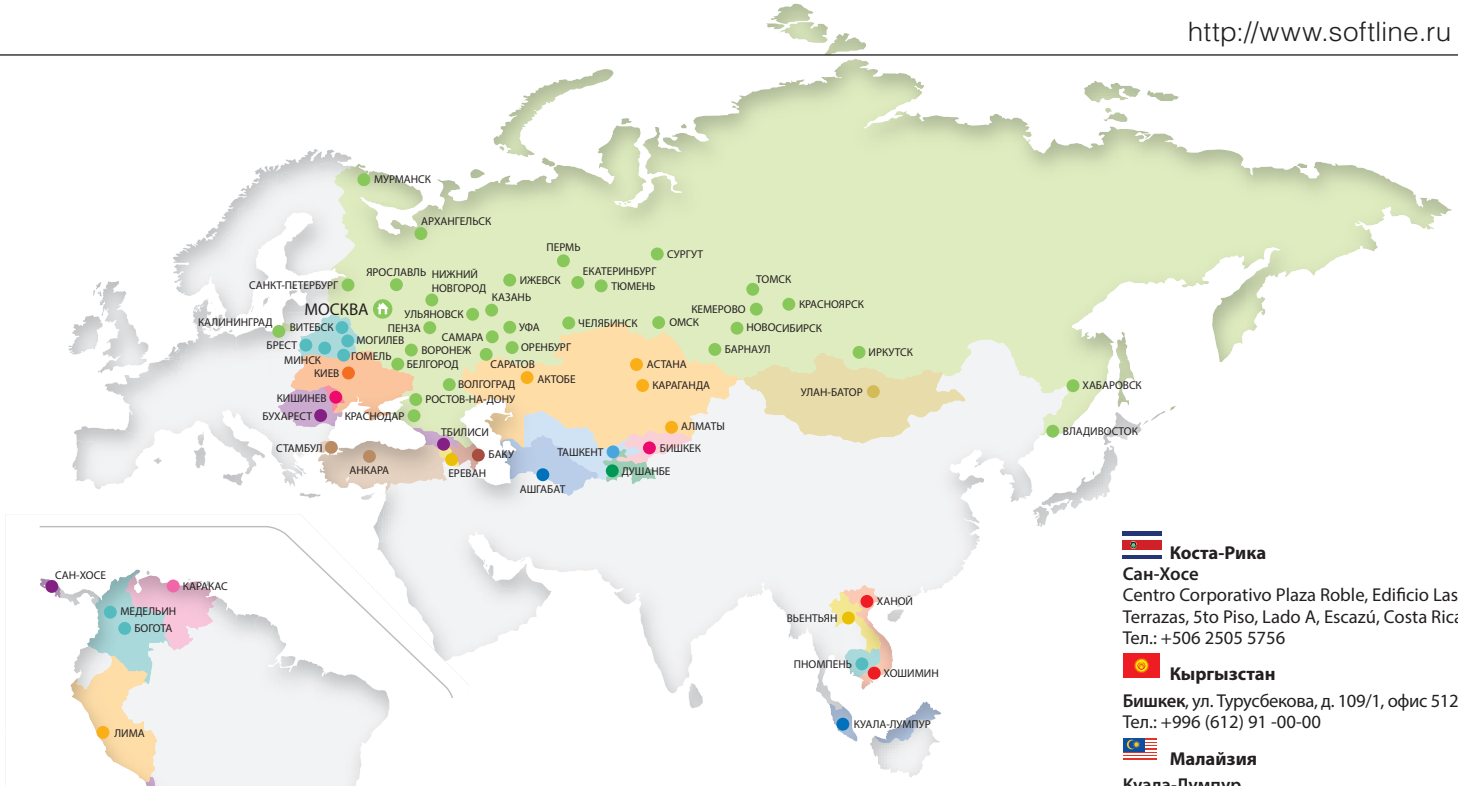
4 Softline всегда рядом

Сегодня, помимо центрального офиса в Москве, компания имеет представительства в 34 крупных городах России, а также филиалы в странах СНГ — в Украине, Белоруссии, Казахстане, Узбекистане, Кыргызстане, Молдове, Азербайджане, Таджикистане, Туркменистане, Армении. Также действуют филиалы Softline в Аргентине, Венесуэле, Вьетнаме, Грузии, Египте, Колумбии, Малайзии, Монголии, Румынии и Турции.

5 Наши клиенты

Среди клиентов Softline — ведущие российские и зарубежные компании: Газпром, Лукойл, Центральный банк РФ, РУСАЛ, Базовый Элемент, Норильский Никель, Северсталь и более десяти тысяч других компаний.

Статусы Softline



Россия

Москва, Дербеневская наб., д. 7.
Тел./факс: +7 (495) 232-00-23
Архангельск, ул. Поморская, 61, офис 40
Тел.:+7 (8182) 63-59-22
Барнаул, пр-т Калинина, д. 6 А, офис 207.
Тел.: +7 (3852) 53-50-01
Белгород, ул. Князя Трубецкого, д. 24, оф. 3.6
Тел.: +7 (4722) 58-52-55
Владивосток, ул. Пушкинская, д. 109, офис 306.
Тел.: +7 (423)260-00-10
Волгоград, ул. Рабоче-Крестьянская, д. 22, офис 305.
Тел.: +7 (8422) 90-02-02
Воронеж, пр-т Труда, д. 65.
Тел.: +7 (4732) 50-20-23
Екатеринбург, ул. 8 Марта, д. 194, корпус И.
Тел.: +7 (343) 278-53-35
Ижевск, ул. Пушкинская, д. 270, офис 416.
Тел.:+7 (3412) 93-66-51
Иркутск, ул. Рабочая, д. 2А, офис 520.
Тел.: +7 (3952) 50-06-32
Казань, ул. Спартаковская, д. 6, офис 608.
Тел.: +7 (843) 526-55-26
Калининград, ул. Октябрьская, д. 8, БЦ «Рыбная биржа», офис 409.
Тел.:+7 (4012) 77-76-50
Кемерово, ул. Кузбасская, д. 31, офис 111.
Тел.: +7 (3842) 45-59-25
Краснодар, ул. Красноармейская, д. 116/2, литера «А».
Тел.: +7 (861) 251-65-14
Красноярск, ул. К. Маркса, д. 48, офис 6-1-1.
Тел.: +7 (391) 252-59-91
Мурманск, ул. Книповича, д. 23, офис 713.
Тел.: +7 (8152) 68-88-46
Нижний Новгород, ул. Новая, д. 28.
Тел.: +7 (831) 220-00-36
Новосибирск, ул. Фрунзе, д. 88.
Тел.: +7 (383) 347-57-47
Омск, ул. Герцена, 34.
Тел.:+7 (3812) 43-31-90
Оренбург, ул. Туркестанская, д. 161, офис С4.
Тел.: +7 (3532) 45-20-10
Пенза, ул. Московская, д. 23, офис 2.
Тел.:+7 (8412) 20-00-51
Пермь, ул. Луначарского, д. 3/2.
Тел.:+7 (342) 214-42-01
Ростов-на-Дону, ул. Текучева, д. 139 Г, офис 204.
Тел.: +7 (863) 237-99-49
Самара, ул. Авроры, д. 63.
Тел.: +7 (846) 270-04-80
Санкт-Петербург, пр-т Непокоренных, д. 49, БЦ «Н-49», оф. 610.
Тел.: +7 (812) 777-44-46
Саратов, ул. Аткарская, д. 66, оф. 602 .
Тел.: +7 (8452) 24-77-32
Сургут, пр-т Мира, д. 42, офис 706.
Тел.: +7 (3462) 22-35-00
Томск, ул. Гагарина, д. 7, офис 503, АТК «Аврора».
Тел.: +7 (3822) 90-00-81
Тюмень, ул. Комсомольская, д. 57, оф. 4.
Тел.: +7 (3452) 69-60-63
Ульяновск, ул. К. Маркса, д. 13 А, корп. 2, офис 702.
Тел.: +7 (8422) 41-99-09
Уфа, ул. Пархоменко, д. 156/3, офис 405.
Тел.: +7 (347) 292-44-50
Хабаровск, ул. Шеронова, д. 56 А, офис 910.
Тел.: +7 (4212) 74-77-24
Челябинск, пр. Ленина, д. 21В, офис 607.
Тел.:+7 (351) 222-40-10
Ярославль, ул. Победы, д. 16 Б, офис 108.
Тел.: +7 (4852) 58-88-09

Азербайджан

Баку, ул. Сулеймана Рагимова, д. 23.
Тел.: +994 (12) 597-30-58

Аргентина

Буэнос-Айрес
Carlos Pellegrini 1043 — 3P (1001)
Buenos Aires, Argentina.
Tel.: +54 (11) 4321-3650

Армения

Ереван, ул. Амиряна, д. 4/7, сектор 8.
Тел: + 374 (10) 541-084

Беларусь

Минск, ул. Богдановича, д. 155, офис 1215.
Тел.: +375 (17) 290-71-79
Брест, ул. Гоголя, д. 75, офис 411.
Тел.: +375 (162) 22-03-84
Гомель, ул. Советская, д. 29, комн. 437.
Тел.: +375 (232) 710-075
Витебск, ул. Замковая, д. 4, офис 215.
Тел.: +375 (212) 35-95-78
Могилев, ул. Первомайская, д. 29, ТЦ «Днепр», офис 327.
Тел.: +375 (222) 23-02-67

Венесуэла

Каракас
Av. Libertador, Multicentro Empresarial del Este; Torre Miranda, Nucleo A; Piso 10 — Office 105; Chacao Caracas, Venezuela 1060.
Tel.: +58 (212) 740-66-22

Вьетнам

Ханой
Room 1101, HITTC Building, 185 Giang Vo Str, Dong Da dist. Hanoi, Vietnam 84.
Tel.: +84 (4) 220-024-34

Хошимин
Room D32, Fosco Building, 40 Ba Huyen Thanh Quan Str. Ward 6, District 3
Ho Chi Minh, Vietnam.
Tel.: +84 (8) 393-069-28

Грузия

Тбилиси, ул. Гамрекели, д.19, офис 505
Тел.: +999 (32) 36-52-70

Казахстан

Алматы, ул. Манаса, д. 32а, офис 501.
Тел.: +7 (727) 250-75-70
Астана, ул. Ауэзова, д. 8, Бизнес-центр «Азия».
Тел.: + 7 (7172) 688-708
Актобе, ул. Маресьева, д. 95 А, офис 11.
Тел.: +7 (7132) 594-694
Караганда, пр-т Нуркена Абдирова, д. 5, офис 530.
Тел.: +7 (7212) 58-91-11

Камбоджа

Пномпень
3rd floor, S.I Building, #93 Preah Sihanouk Blvd, Phnom Penh, Cambodia
Тел.: +855 23990039

Колумбия

Богота
Autopista Norte No. 103-34 Oficina 704
Edificio Logic 2 — Bogota, Colombia.
Tel: + 57 (1) 489-04-44
Медельин
Carrera 43ª No.15 sur — 15, Edificio Xerox Oficina 801.
Tel: +574-326-7000

Коста-Рика

Сан-Хосе
Centro Corporativo Plaza Roble, Edificio Las Terrazas, 5to Piso, Lado A, Escazú, Costa Rica
Тел.: +506 2505 5756

Кыргызстан

Бишкек, ул. Турусбекова, д. 109/1, офис 512.
Тел.: +996 (612) 91 -00-00

Малайзия

Куала-Лумпур
Unit 21.4, floor 21, Menara Genesis, 33 Jalan Sultan Ismail 50250, Kuala Lumpur, Malaysia.
Tel: +603 2141 8987

Молдова

Кишинев, MD-2004, бд. Штефан чел Маре 202, Бизнес-центр «Kentford».
Тел.: +373 (22) 855-042

Монголия

Улан-Батор
Od plaza, #509. Seoul Street-6/2, Sukh-baatar District 1st khoroo, Ulaanbaatar 210620a, P.O.Box-121, Mongolia.
Тел.: +976 (70) 11-07-65

Перу

Лима
Av. Víctor Andrés Belaúnde 147, Torre Real 10, Oficina 102, Centro Empresarial Real, San Isidro, Lima — Perú.
Tel.: +51 (1) 637-1200

Румыния

Бухарест
Spl. Unirii 16, Muntenia Business Center, Room 306, Bucharest, 040035, Romania.
Tel.: +40 (21) 387 34 40

Таджикистан

Душанбе, ул. Айни, д. 24а, офис 406.
Тел.: +992 (44) 600-60-00

Туркменистан

Ашхабад, ул. Гарашсызлык, д. 8.
Тел.: +993 (12) 48-22-86

Турция

Стамбул
Bayar Caddesi Gülbahar Sokak No:17 Perdemsac Plaza 5/51, 34742, Kozyatağı, Kadıköy/ İstanbul.
Tel: +90 (216) 373-44-07
Анкара
Konya Devlet Yolu No:84 Akman Condominium Plaza D:164 Karakusunlar Balgat, Ankara.
Tel.: +90 (312) 284-00-81

Узбекистан

Ташкент, ул. У. Юсупова, д. 36.
Тел.: +998 (71) 120-49-09

Украина

Киев, ул. Игоревская, д. 14-А.
Тел.: +38 (044) 201-03-00

Чили

Сантьяго, San Sebastian 2807, Flat 914, Las Condes, Santiago, Chile, 7550180
Tel.: +56 (2) 2653-7430

SOFTLINE

Уважаемые коллеги!

С радостью представляем вашему вниманию ноябрьский выпуск специализированного журнала Softline Direct, полностью посвященный актуальным вопросам из сферы информационной безопасности.

Направление по информационной безопасности Softline за прошедший год сделало еще один большой шаг в своем развитии. Мы приумножили свой опыт, обрели новые уникальные компетенции и теперь хотим поделиться ими с вами.

Это издание выходит в самый «горячий» период на рынке и наполнено материалами по наиболее актуальным темам. Мы надеемся, что оно послужит надежным источником информации для вас и ваших коллег, поможет сориентироваться в вопросах, требующих быстрых ответов и принесет вам практическую пользу.

В этом выпуске вашему вниманию представлен подробный отчет об изменениях в требованиях по защите персональных данных, проведен анализ законодательства о национальной платежной системе, раскрыты вопросы, связанные с новыми для российского рынка решениями IdM, а также затронуты темы DLP, контентной фильтрации, сетевой безопасности и многие другие.

Мы желаем вам приятного чтения и успехов в делах!

С уважением, руководитель департамента информационной безопасности

Вячеслав Железняков

ВСТРЕЧАЙТЕ МЕЖДУНАРОДНЫЙ ФОРУМ В ВАШЕМ ГОРОДЕ!

Что такое Гранд-Форум?

Это – однодневный праздник для всех профессионалов в области IT.
Это – несколько тематических конференций, посвященных самым востребованным темам в области IT: дата-центры и облачные сервисы, IP-сети и кабельные системы, опыт применения информационных технологий в бизнесе.
Это – более 40 презентаций отраслевых экспертов, посвященных наиболее актуальным и интересным темам.
Это – выставка инновационных технологий и продуктов, последних разработок мировых IT-лидеров.
Это – порция новых знаний и навыков, которые позволят вам идти в ногу со временем и расти, как профессионалу
Это – живое общение с известными экспертами и с вашими коллегами.
Это - заряд позитивной энергии и хорошего настроения.

На Гранд-Форумах есть все, что нужно, чтобы создать **атмосферу праздника** для **IT-специалистов, энтузиастов и профессионалов.**
Единственное, чего нам не хватает на наших форумах – **это Вас!**
Приходите, чтобы увидеть все своими глазами и приглашайте своих коллег!

ТЕМАТИЧЕСКИЕ КОНФЕРЕНЦИИ: НОЯБРЬ 2013 — ФЕВРАЛЬ 2014

ВОКРУГ ЦОД	Казань	ноябрь
ВОКРУГ КАБЕЛЯ	Москва	ноябрь
ВОКРУГ ОБЛАКА	Барнаул	декабрь
ВОКРУГ IP	Краснодар	январь
БИЗНЕС и ИТ	Москва	февраль
	Киев	февраль

ВСЕ НОВЫЕ ТЕХНОЛОГИИ В ОДИН ДЕНЬ И В ОДНОМ МЕСТЕ!

Организаторы:
CIS Events Group
your new marketing wave
Дни Решений
DCNT.RU
A-HOM

Регистрация на мероприятия:
www.formreg.com

Видео-отчеты о наших мероприятиях:
www.youtube.com/teleinfoTV

20 лет успеха: Softline

В этом году Softline исполняется 20 лет! За этот срок компания выросла из небольшого реселлера научного ПО в международную организацию, представленную в 25 странах и 68 городах. 2200 специалистов нашей команды ежедневно делятся эффективными и доступными IT-технологиями с компаниями по всему миру. Мы сотрудничаем с 3000 вендоров, постоянно развиваемся и совершенствуемся.

Департамент информационной безопасности

54%
рост в 2012 г.
по сравнению с 2011 г.

Немного истории

Департамент информационной безопасности компании Softline начинался как специфическое направление по продаже софта. Традиционно этот сегмент является наиболее развитым, и линейка брендов уже тогда впечатляла. Но шло время, и стратегические ориентиры были перенаправлены на развитие компетенций команды безопасности.

Что было сделано за последние несколько лет:

- сформулирована четкая стратегия развития,
- проведено углубленное техническое обучение специалистов,
- усилены взаимосвязи с вендорами,
- создана матрица продаж (решений),
- обеспечено четкое соответствие требованиям рынка,
- увеличен в 2,5 раза список вендоров по безопасности.

Нам удалось развить сегмент крупных продаж и сервисных проектов, стать экспертами по новейшим технологиям, научиться решать самые нетривиальные задачи. Это привело с росту сделок по направлению «Услуги» в 1,5 раза.

Активно развиваются новые направления, такие как:

- тонкая настройка DLP-систем и сред защиты,
- мониторинг корреляции событий (SIEM),
- углубленная экспертиза систем,
- пентесты и бизнес-аналитика,
- расследование инцидентов.

200+
проектов

4
место среди IT-компаний России по ИБ по данным CNews Analytics

100+
вендоров

Наши партнеры

KASPERSKY
Symantec
Код безопасности
Check Point SOFTWARE TECHNOLOGIES LTD.
AccessData
software AG
Аладдин РД
McAfee
websense
eset
INFOWATCH
ca

— лидер IT-рынка

Информационная безопасность относится к приоритетным и стратегически важным для Softline направлениям деятельности. В юбилейный для компании год хочется говорить о пройденном пути — том прошлом, которое формирует будущее.

Мы предлагаем нашим клиентам индивидуальный и комплексный подход к решению задач в области информационной безопасности.

Нужно отметить, что Softline ведет активную экспансию на рынки СНГ и дальнего зарубежья, в частности, в регионе Юго-Восточной Азии, который переживает небывалый рост. Объединяя опыт континентов, мы становимся еще более открытыми ко всему нестандартному, новому, лучшему!

Спектр услуг

Обеспечение соответствия требованиям	Защита персональных данных, режим коммерческой тайны, юридическая значимость ЭЦП. Соответствие стандартам ISO 27001, PCI / DSS, СТО БР и др. Закон о НПС и Положение Банка России №342-П.
Внедрение мер обеспечения ИБ: прикладные решения	Контентная фильтрация, контроль носителей информации, защита от утечек конфиденциальной информации, безопасность файловых серверов, управление правами доступа к информации, безопасность электронной почты, безопасность web-ресурсов. Противодействие мошенничеству.
Внедрение мер обеспечения ИБ: инфраструктурные решения	Безопасность серверов и рабочих станций, сетей и виртуальных сред, безопасность критичных и фиксированных систем, безопасность удаленного доступа к корпоративным ресурсам, безопасность мобильных устройств, криптографическая защита, аутентификация и управление правами доступа, архивирование и поиск в неструктурированных данных.
Внедрение мер обеспечения ИБ: специализированные решения	Безопасность АСУТП, безопасность систем ЭДО, безопасность корпоративных порталов, безопасность САПР, безопасность Active Directory.
Экспертные услуги	Аудит ИБ, анализ защищенности, тестирование на проникновение. Настройка средств защиты. Расследование инцидентов. Комплексное сравнение решений. Проведение специальных исследований на ПЭМИН. Заказная разработка ПО по ИБ.
Построение процессов управления ИБ	Построение процесса управления информационными активами, рисками ИБ, инцидентами ИБ, построение процесса безопасной разработки приложений, управления уязвимостями, внутреннего аудита ИБ.
Сервисные услуги	Юридическая и техническая поддержка в области ИБ. Обучение специалистов в области ИБ. Аутсорсинг и аутстаффинг.

Строго конфиденциально

Рынок предоставляет множество различных решений для защиты конфиденциальных данных. Особой популярностью и большим спросом пользуются DLP-системы — решения, контролирующие выход конфиденциальной информации за периметр компании.

Автор: Антон Афанасьев, руководитель направления прикладных решений по ИБ, Департамент информационной безопасности Softline

DLP-системы разрабатываются как российскими специалистами, так и их коллегами из стран СНГ. На российском рынке также представлены зарубежные производители и зарубежные технологии, которые пользуются спросом. Разрабатываемых сегодня DLP-систем не хватает для того, чтобы определить и защитить весь требуемый объем конфиденциальной информации. В большинстве случаев это связано с тем, что DLP-системы обозначены и предназначены для контроля информации, выходящей за периметр компании, но не всегда способны решать сторонние сопутствующие задачи.

Что собой представляет технология DLP, и на что она направлена?

Технологии DLP — это компоненты или модули анализа информации, которая передается по самым распространенным каналам передачи данных, таким как съемные носители, печать, корпоративная почта, любые вариации, связанные с веб-направлением (с отправкой данных через протокол HTTP). Также в современном мире существуют такие распространенные каналы передачи данных, как MSN Messenger, Microsoft Lync, Skype, ICQ и т.д. Со временем появляются все новые каналы выхода конфиденциальной информации, такие как облачные календари, которые становятся популярными у сотрудников компаний, Яндекс.Диск, DropBox и многие другие. Производители DLP-систем активно развиваются, стремясь увеличить количество каналов, которые они могут контролировать.

Уровни защиты

На практике с помощью DLP-системы нельзя контролировать всю конфиденциальную информацию, поэтому существуют отдельные классы продуктов, которые позволяют защитить компанию от рисков утечки конфиденциальных данных. Самым существенным риском для каждой организации являются привилегированные пользователи, обладающие расширенными правами доступа на компьютере, серверах или в других системах. Сотрудники компании реализуют поставленные им задачи, часто имея доступ к конфиденциальной информации, что в случае недобросовестности или невнимательности пользователя повышает риск ее распространения или утечки. Ввиду этого наиболее активное развитие получают решения, связанные с защитой баз данных, поскольку именно они являются одним из наименее охваченных направлений в области защиты конфиденциальной информации.

В качестве примера можно рассмотреть компанию, имеющую собственную базу данных SQL, в которой содержится конфиденциальная информация. Пользователь, обладающий привилегированными правами доступа, может получить выгрузку этих данных, используя вполне легальные средства и легальные инструменты, которые

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.

компания сама предоставила ему для работы. После выгрузки информации из базы отслеживать ее распространение становится сложно. Ввиду этого разрабатываются определенные системы, которые позволяют анализировать запросы, обращенные к базам данных, и, исходя из этого, определять, какую информацию из базы данных пользователь намерен получить. Если пользователь намеревается выгрузить большой массив данных, содержащий конфиденциальную информацию, система может оповестить об этом офицера безопасности либо запретить пользователю проведение такой операции. Подобная работа системы обеспечивает защищенность на уровне сетей и представляет собой отдельный класс продуктов, никак не связанный с DLP-системами. Такого рода системы позволяют защитить как саму базу данных, так и информацию, хранящуюся в ней.

Варианты защиты конфиденциальной информации, хранящейся на внутренних ресурсах

Потребность в защите часто появляется у организаций, которые хранят конфиденциальную информацию на файловых ресурсах (файловые сервера, порталы и т.д.). В таком случае службе ИБ или людям, которые отвечают за сохранение конфиденциальности данных, нужно понимать, что происходит на местах их хранения, кто к ним обращается, как с ними работают в конкретный момент времени, что именно пользователь открывает. DLP-системы не имеют возможности анализировать такого рода информацию и предоставлять соответствующие отчеты службе ИБ. Именно поэтому на рынке ИБ существует смежный класс продуктов, который позволяет анализировать то, что происходит на файловом ресурсе, отслеживать модель поведения пользователя. Если по каким-то параметрам она противоречит его обычному поведению, система выдает оповещение. Таким образом, если человек работает за компьютером и обращается за день к 20 файлам, хранящимся на файловом ресурсе, тогда, например, аномальным будет считаться такое поведение, при котором пользователь в течение короткого промежутка времени обратился сразу к 100 файлам. Это позволяет сделать вывод о том, что пользователь моментально открывает и просматривает файлы или копирует их. Этого достаточно для того, чтобы офицер безопасности акцентировал свое внимание на действиях сотрудника. Реализация такого рода функционала — это следующий этап для производителей в разработке DLP-систем.

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.

Сотрудники внешних организаций с привилегированными правами доступа

Многие компании предоставляют партнерам или клиентам удаленный доступ к своим информационным системам. Организации пользуются технической поддержкой от разного рода интеграторов, от производителей программного обеспечения. Предоставление повышенных привилегий доступа в корпоративную среду создает дополнительные проблемы контроля за действиями внешних пользователей. Для защиты информации компании приходится отвечать на ряд вопросов: что пользователь делает в тот или иной момент, к каким системам он обращается, какие действия производит. Для контроля за пользователями, понимания того, чьи действия привели к тем или иным ошибкам и в какой момент времени, а также для контроля за рисками, связанными со всеми несанкционированными активностями людей, обладающих повышенными привилегиями доступа к информационным ресурсам и к серверам, на российский рынок выходит отдельный класс систем информационной безопасности. Основными заказчиками таких систем являются банки, которые осуществляют поиск определенного рода средств защиты, подбирая их под свои нужды с целью минимизации всевозможных рисков, связанных с утечкой конфиденциальных данных.

Существуют ли решения, которые могут работать в связке с DLP-системами?

С большинством DLP-систем интегрируется система контроля доступа к информации Information Rights Management. На российском рынке широкое распространение получили системы Rights Management (Microsoft) и LiveCycle (Adobe).

В большинстве случаев работа систем основана на принципе шифрования, «запечатывания» конфиденциального документа ключом или сертификатом пользователя. В случае если он оказывается за пределами защищаемого периметра, его невозможно открыть и ознакомиться с его содержанием. Система Information Rights Management также ограничивает распространение информации между сотрудниками внутри компании, так как передать информацию внутри компании можно различными способами, а внутреннюю утечку данных DLP-системы не всегда в состоянии предотвратить. Такого рода системы приобретают все большую популярность и активно используются в работе в связке с DLP-системами. «Узкое» место Information Right Management состоит в том, что автор документа собственноручно должен ограничить доступ к создаваемому документу, т.е. распределить права: кому можно открывать документ, кому — печатать его, кому можно вносить правки и т.д.

Предотвращение утечки данных с мобильных устройств

Автор: Алексей Титков, менеджер по продажам услуг, Департамент информационной безопасности Softline

Развитие информационных технологий подарило уникальную возможность решать бизнес-задачи в любом месте в любое время. Тот мобильный мир, о которым сравнительно недавно мечтали фантасты, уже стал явью. Каждый день мы сталкиваемся с людьми, работающими буквально на ходу. Это подтверждает и перераспределение игроков на рынке персональных ПК и мобильных устройств, планшетов и смартфонов. В 2013 году российский рынок персональных компьютеров «просел» на треть, в то время как рынок планшетных вырос и составляет все более жесткую конкуренцию традиционным ПК.

Проблематика

Тенденция тотальной мобилизации (в корпоративном сегменте так называемая концепция BYOD — Bring your own device) вызывает головную боль IT- и ИБ-служб, т.к. обеспечивать информационную безопасность, ее целостность становится все труднее: точек входа в периметр становится все больше и, как следствие, их все сложнее контролировать. Простой запрет доступа к корпоративной почте, внутренним ресурсам в ущерб мобильности не только не эффективен, но и наносит прямой ущерб производительности. Теперь уже необходимо защищать информацию, получаемую и передаваемую пользователями с помощью мобильных устройств.

Традиционно за информацией, покидающей периметр компании, следили DLP-системы. Действительно, обеспечить наблюдение за основными каналами связи (почтой, веб-трафиком, программами быстрого обмена сообщениями, облачными хранилища информации и т. д.) не составляет труда. Достаточно выбрать подход к перехвату информации — мониторинг и уведомление ответственной службы компании или метод активной блокировки, когда информация, классифицированная как конфиденциальная, будет заблокирована в момент отправки по одному из каналов передачи, вывода на печать или записи на съемный USB-носитель. В последнем случае обычно используется программа-агент, которая в явном или скрытом виде занимается контролем на уровне рабочей станции пользователя. Используя различные средства администрирования, не составляет труда установить такую программу на ПК сотрудника. Однако с мобильными пользователями, вписывающимися в концепцию BYOD, так поступить не удастся. Во-первых, нельзя обязать сотрудников не использовать мобильные устройства. Во-вторых, шифрованные каналы связи не могут контролироваться без подмены сертификата (это касается как протокола HTTPS, так и многих программ, использующих SSL, например ICQ, Skype, Jabber и т. д.).

Как решить?

Очевидно, что практически нереально обязать сотрудников компании соблюдать осторожность с корпоративными данными, используя собственные мобильные устройства (достаточно вспомнить, что распространенность систем «антивор» — антивирусного ПО для мобильных платформ — оставляет желать лучшего). Поэтому необходимо обеспечить целый комплекс мер.

Производители DLP-систем понимают сложившуюся ситуацию и предлагают различные способы решения проблемы.

Простой способ

Во-первых, можно применить ряд простых организационных мер имеющимися средствами администрирования:

1. Настроить DMZ-зону для неавторизованных устройств, к которым можно отнести все устройства, подключаемые по беспроводной сети. Для этой зоны применить ряд ограничительных мер, например, доступ только к разрешенным веб-страницам, к общим файловым ресурсам корпоративной сети. Простой принцип – что не разрешено, то запрещено.
2. При использовании мобильных устройств запретить приложениям доступ по шифрованным каналам из корпоративной сети.
3. При удаленном доступе (например, RDP) в корпоративную сеть настроить запрет простого «перетаскивания» объектов из интерфейса программы удаленного доступа на устройство сотрудника.
4. Отключить возможность скачивать вложения писем из корпоративной почты (например, в Outlook Web Access это штатная возможность).

Очевидно, что данные ограничительные меры дадут иллюзию защищенности, но не помогут решить ряд проблем — доступ привилегированных пользователей (руководство), контроль пересылки вложений на личную почту сотрудников.

Специализированные решения

Symantec DLP for Tablet

Ведущие производители систем ИБ понимают очевидную проблему и анонсируют различные решения, в т. ч. и DLP-системы. Одним из первых вендоров, разработавших специализированный модуль, стала американская компания Symantec, которая в 2011

году анонсировала первое решение в рамках комплексного продукта — Symantec DLP.

Решение работает через VPN и позволяет маршрутизировать трафик, генерируемый мобильным устройством. К трафику применяются предустановленные или настроенные политики.

Решение позволяет мониторить исходящие сообщения и вложения электронной почты (Gmail, Yahoo!, Mail и другие HTTP(S)), отслеживать веб-трафик и исходящую на сайты и в социальные сети (Dropbox, Twitter, Facebook, в т. ч. и по HTTPS) информацию и удалять при этом из общего потока передаваемых данных конфиденциальные данные.

На данный момент поддерживаются устройства, работающие под руководством операционной системы iOS (iPhone, iPad).

DLP-система для мобильных устройств уже стала реальностью, что позволяет использовать весь комплекс политик обращения с конфиденциальными данными и на мобильных корпоративных устройствах.

Как быть с пользователями за периметром?

McAfee Enterprise Mobility Management (McAfee EMM)

Спектр решаемых задач справедлив для полноценных решений комплексного управления информационной безопасностью. Корпоративные политики, разрабатываемые IT-службами и применяемые для ноутбуков и стационарных ПК, теперь могут быть доступны и мобильным устройствам.

Для правильной эксплуатации EMM-системы необходимо априори принять несколько основных правил:

1. При утере устройства пользователи должны незамедлительно сообщить об этом в ответственную службу компании для скорейшей блокировки доступа к корпоративным данным.
2. Пользователи должны понимать, что на мобильное корпоративное устройство, которое они получили в свое распоряжение, распространяются все политики и правила, принятые внутри организации, т.е. это устройство является инструментом компании.
3. Устройства, которые используются в компании, не должны иметь возможности подключения съемных носителей, внесения изменений в список ПО самостоятельно. Это позволит минимизировать риски использования пиратского ПО, а также способы обойти систему защиты.
4. Отдельно необходимо решить вопрос с поддержкой EMM-системой устройств с пиратскими ОС (Jailbreak).

McAfee EMM представляет собой систему, которая предустанавливает средства обеспечения безопасного доступа к установленным мобильным приложениям, обеспечивает защиту от вредоносных программ, строгую аутентификацию в корпоративных сервисах компании, масштабируемую архитектуру и функции формирования отчетности и инвентаризации парка мобильных устройств.

Решение интегрируется с платформой McAfee ePolicy Orchestrator (McAfee ePO), позволяет IT-службам применять политики безопасности, обеспечивая в то же время защиту устройств и корпоративной сети от вредоносных программ. Помогает снизить затраты на поддержку и управление мобильными устройствами.

Стоит отметить, что решением поддерживается большинство операционных систем, в их число входят iOS, Android, Blackberry, Windows Phone. Для двух последних версий продукта не предусмотрено агентской части, которую необходимо установить на смартфон. Администрирование осуществляется с помощью собственных средств ОС.

Некоторые возможности McAfee EMM:

- Управление различными мобильными устройствами (Android, iOS, Blackberry, Windows Phone).
- Управление конфигурацией ПО.
- Принудительное использование паролей.
- Инвентаризация устройств.
- Частичная блокировка функционала (Bluetooth, Wi-Fi).
- Удаленная блокировка и стирание данных (полное или частичное).
- Принудительное шифрование данных (полное или частичное).
- Контроль ActiveSync и возможность блокировки доступа к почте.
- Возможности массовой рассылки сообщений.
- Формирование ролей доступа к устройствам.
- Сбор логов, архивация SMS-сообщений и многое другое.

Обеспечение безопасности мобильных устройств системами EMM позволит IT- и ИБ-службам контролировать такой непростую часть распределенного периметра, как мобильные устройства. Подобный функционал поможет компаниям снизить стоимость владения парком мобильных устройств, а также обеспечит централизованный контроль за безопасностью.

Выводы

Подводя итоги, можно сказать, что концепция BYOD актуальна как никогда, и простой комплекс мер позволит организациям минимизировать потенциальный ущерб от использования личных устройств внутри собственной сети компании. Тем самым можно убить двух зайцев — не потерять в общей мобильности и свободе доступа к работе «на бегу» и, в тоже время, обеспечить комплекс мер для защиты своей конфиденциальной информации.

В производстве решений DLP для мобильных пользователей сделан первый шаг — многие компании вслед за Symatec анонсируют разработку клиентов для мобильных устройств и перечень инструментов со временем будет только расти.

Контроль корпоративных устройств, предоставляемых компанией-нанимателем сотрудникам для работы, предполагает куда больше инструментов не только контроля информации, но и защиты украденных устройств, шифрования и возможности инвентаризации и контроля программного обеспечения мобильных устройств, вне зависимости от привязки к операционной системе смартфонов.

Что выбрать бизнесу для собственной безопасности? Комплексные решения!

В наш век информационных технологий компьютер просто обязан быть подключенным к глобальной или, в крайнем случае, локальной вычислительной сети. Без этого он превращается или в печатную машинку, или в калькулятор.

Олег Сыч, эксперт в области антивирусной защиты

Автор: Александр Вахтель, менеджер по поддержке продаж услуг ИБ, Департамент информационной безопасности Softline

Защита информации в сетях. Кому и для чего это нужно?

Всем хорошо известно об угрозах бизнесу со стороны информационных технологий. Все чаще появляются сообщения о тех или иных инцидентах, так как государство законодательно обязывает компании обнародовать определенные случаи нарушения информационной безопасности. Примером могут служить некоторые данные, опубликованные в 2012 году (источник: материал «Самые громкие утечки информации в России», РБК daily от 19.06.2013. http://rbcdaily.ru/society/562949987433402):

- в апреле 2012 года близ Казани среди мусора нашли личные дела военнослужащих расквартированной неподалеку воинской части МВД специального назначения;
- в декабре 2012 года на сайте Следственного комитета России в открытом доступе появились тексты обращений граждан через интернет-приемную;
- концерн «Тракторные заводы»: коммерческую тайну похитил экс-сотрудник. По предварительным оценкам владельцев коммерческой тайны, им был нанесен ущерб свыше 50 млн руб.;
- инсайдеры из ОАО «МТС» и ОАО «Вымпелком» с 2010 по 2012 год «сливали» информацию о переговорах трех абонентов — высокопоставленных российских чиновников. Идет расследование. В МТС заявили, что внутренней службой безопасности фактов утечки не выявлено;
- утечка баз пользователей, всего 760 тыс. человек. У 92 тыс. человек из базы помимо имен и адресов электронной почты указаны также номера мобильных телефонов. Предполагают, что утечка произошла с сайтов-«купонаторов».

У каждой организации есть конфиденциальная информация, и чаще всего она обрабатывается и хранится на компьютерах. Это данные о сотрудниках, клиентах, коммерческая тайна (научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющая секреты производства, «ноу-хау»).

Наверняка и в вашей компании есть информация, которая не подлежит разглашению. А сколько она стоит? Задумывались ли вы, какие могут быть последствия, если эти данные «нечаянно» удалит кто-то из сотрудников? А если их украдут, изменят некоторые факты? Что будет, если кто-то выложит ваши конфиденциальные данные для публичного доступа (например, в Интернет)? Что произойдет, если злоумышленник получит свободный доступ к файлам о ваших клиентах (номерам кредитных карт, телефонам, счетам и др.)? Или доступ к вашим счетам или технологическим процессам? Или воспользуется брендом вашей компании для мошеннических действий? Украдут маркетинговые планы по выпуску продукта на рынок? Посмотрите еще раз на этот список. Нашли важные для вас причины защитить информацию в своей компании?

Как показала практика, наибольшую опасность представляют последствия, называемые репутационными рисками, и нарушение или прекращение бизнес- или технологических процессов. Очень часто для компаний СМБ-сектора они являются критическими и могут стать причиной закрытия бизнеса.

И это только незначительный список возможных последствий. Есть еще информация, которая защищена государством, отраслевыми и международными стандартами. Например, персональные данные сотрудников и клиентов (см. ФЗ-152). Технологические процессы в ключевых системах информационной инфраструктуры (предприятия топливно-энергетического комплекса, водоснабжения и т.д.), национальная платежная система (см. ФЗ-161). В этом случае наступает еще и уголовная или административная ответственность, в том числе для руководителей и отдельных сотрудников организации, отвечающих за безопасность при обработке и хранении информации.

Перечисленные выше, и не только, основания позволяют сделать вывод, что необходимость защищать данные не зависит от размера компании. Важность потери информации для малого и среднего бизнеса трудно переоценить, потому что ресурсов на компенсацию рисков у него нет.

Средний бизнес: вопросы рынка ИБ

Существуют определенные проблемы развития систем информационной безопасности на рынке малого и среднего бизнеса. Решения зачастую получаются либо достаточно дорогими, либо с ограниченным функционалом. Продукты, которые предлагают производители, нуждаются в дополнительных программных или аппаратных решениях. В качестве примера можно привести отсутствие в комплексном решении единой консоли управления или полноценного DLP-решения. Компании-разработчики стремятся устранить подобные «бреши» и выпустить на рынок полноценный, по-настоящему комплексный продукт. Это позволяет компаниям-потребителям, во-первых, экономить на построении системы безопас-

ности, во-вторых, получить легко управляемую ИБ-систему.

Решения для СМБ в области защиты информации существуют, хоть и в ограниченном количестве. Вариантов для крупного бизнеса — множество, и на рынке информационной безопасности постоянно появляются новые предложения. Впрочем, в последние несколько лет ситуация начала меняться: отчасти из-за снижения темпов роста рынка в сегменте EPG, отчасти — из-за стремительного роста конкуренции. После кризиса 2009 года рынок ИБ-продуктов для предприятий среднего и малого бизнеса стабилизировался.

Однако, его специфика не так проста. С одной стороны, программные и аппаратные решения, предлагаемые для компаниям малого бизнеса, по уровню защиты информации, быстродействию и количеству обрабатываемых данных не удовлетворяют сегмент среднего бизнеса, потому что объем данных у последнего зачастую существенно больше. Скорость увеличения этого объема в активно развивающихся компаниях достаточно высока, у них жестче требования к уровню защищенности и предотвращению утечки информации, так как высока конкуренция и различного рода риски.

С другой стороны, решения, разработанные для сегмента крупных организаций (госкорпораций, холдингов и др.), удовлетворяющие требованиям по уровню безопасности и быстродействия, слишком дороги и требуют наличия штата высококвалифицированных специалистов. Среднему бизнесу такой вариант подходит далеко не всегда.

Постоянно возрастающее количество и качество угроз, их «совершенствование» и изменение, усложнение антивирусного ПО, появление новых средств защиты и аппаратных решений, усложнение IT-инфраструктуры организаций, вынужденных использовать имеющиеся ресурсы — такие проблемы характерны для ИБ среднего бизнеса.

Критерии выбора продукта

Учитывая все вышеперечисленные сложности, идеальным вариантом может стать модульное масштабируемое решение, обеспечивающее высокий уровень защиты информации. Подобные продукты стали появляться на рынке информационной безопасности в ограниченном количестве и пока внедряются с осторожностью.

В рамках комплексного подхода к обеспечению информационной безопасности в компании программно-аппаратное решение должно иметь централизованное управление и для наиболее полной защиты включать следующие подсистемы:

1. Подсистему виртуальных частных сетей (VPN).
2. Подсистему защиты удаленных и мобильных пользователей (MDM).
3. Подсистему межсетевого экранирования.
4. Подсистему обнаружения и предотвращения вторжений (IDS/IPS).
5. Подсистему безопасного доступа к сети Интернет, защиты веб-трафика (брандмауэр, файервол, защита электронной почты, прокси-сервер).
6. Подсистему фильтрации электронной почты (Antivirus/Antispam).
7. Подсистему предотвращения утечек конфиденциальных данных (DLP).
8. Подсистему мониторинга и управления средствами защиты (единая консоль управления).

Дополнительно для обеспечения еще большего уровня защиты данных и управляемости система может включать в себя:

9. Подсистему сбора и анализа журналов регистрации событий.
10. Подсистему шифрования данных при хранении.
11. Подсистему резервного копирования данных.

Ниже несколько примеров задач, решаемых внедрением комплексных систем защиты информации в сетях.

- Организация защищенного обмена данными между главным офисом компании и удаленными подразделениями.
- Организация защищенного доступа мобильных и удаленных пользователей компании к разрешенным ресурсам корпоративной сетевой инфраструктуры.
- Организация защищенной демилитаризованной зоны (DMZ) в сетевой инфраструктуре компании.
- Сокрытие топологии и внутренней организации сетевой инфраструктуры компании от внешних пользователей.
- Контроль и разграничение доступа внутри корпоративной сетевой инфраструктуры компании и на ее периметре.
- Аутентификация внутренних и внешних пользователей компании.
- Организация безопасного, контролируемого доступа сотрудников компании в Интернет с защитой от вирусных атак и спама.
- Централизованное управление средствами защиты, находящимися как в главном офисе компании, так и в удаленных подразделениях.

Почему решение должно быть комплексным?

Масштабируемость и гибкость системы информационной безопасности (как и любой IT-системы) — достаточно критичный показатель для бизнеса. Это связано с динамичным изменением как объемов, так и структуры бизнеса, процессов, протекающих внутри организации. В случае если бизнес не может перестроить процессы из-за жесткой структуры и невозможности быстро и просто изменить настройки системы информационной безопасности, последнюю необходимо перестроить. Если же система ИБ достаточно гибкая и легко поддается изменениям или масштабируется, сохраняя свои функции и поддерживая необходимый уровень безопасности, бизнес будет развиваться стремительнее. Это ключевой плюс для комплексных решений в ИБ.

Взаимодействие разных подсистем общей системы информационной безопасности может сопровождаться различными про-

граммными конфликтами в том случае, если используются программные и (или) аппаратные продукты разных производителей. Для работы системы без инцидентов придется достаточно тщательно подбирать различные компоненты и должным образом их настраивать и поддерживать.

Появляется возможность получения консолидированных отчетов о состоянии и об инцидентах безопасности в едином виде, более быстрым и простым способом. Такой подход намного удобнее сбора разрозненных отчетов от различных продуктов и сведения их в единую форму.

Простота эксплуатации и удобство обслуживания — важнейшие преимущества. Если ваш сотрудник управляет всем набором программных и/или аппаратных решений для обеспечения информационной безопасности через единый интерфейс, комплексный продукт значительно сэкономит его время и ресурсы, а значит, время и ресурсы компании. Оптимизируется процесс внедрения, так как освоение функционала и особенностей системы управления одного решения — более легкая задача по сравнению с необходимостью изучения разных подсистем в разных консолях и с различными требованиями. Через централизованный модуль управления проще получать сводные отчеты о состоянии и инцидентах службы ИБ, чего не скажешь о случае, когда применяются различные программные и аппаратные продукты.

Как правило, стоимость комплексного продукта и его внедрения весьма приемлема.

Проанализировав опыт компаний СМБ-сектора в области построения ИБ-систем, мы пришли к выводу, что всеми перечисленными выше свойствами и подсистемами не обладает ни один продукт. В практике внедрения, как правило, появлялась необходимость использовать несколько решений.

Связка Fortinet + «Лаборатория Касперского»

Компания Softline готова предложить вам вариант построения комплексной системы ИБ на основе двух продуктов. Это позволит, с одной стороны, сократить издержки на внедрение по сравнению с другими вариантами, с другой — вы получите все необходимые подсистемы.

Примером выгодного для клиента варианта построения системы ИБ служит использование продуктов компаний Fortinet и «Лаборатории Касперского». Это один из самых успешных вариантов работы двух продуктов, обеспечивающих безопасность хранения и использования информации внутри сети организации. Аппаратное решение компании Fortinet позволяет полностью закрыть потребности в безопасности IT-инфраструктуры организации в сети, ПО «Лаборатории Касперского» обеспечивает безопасность на локальных компьютерах и в программной среде сети. Благодаря такому разделению конфликты между продуктами отсутствуют.

Продукт компании Fortinet для среднего бизнеса — шлюз безопасности FortiGate-100D — это:

- полный набор функций, включая контроль приложений, встроенный беспроводной контроллер, локальное логирование и управление политиками безопасности для конечных пользователей;
- единая панель управления, которая облегчает задачи развертывания и управления;
- возможность интеграции с FortiManager и FortiAnalyzer;
- внутреннее хранилище (16 ГБ), позволяющее локально хранить данные по безопасности сети, отчетности и оптимизации WAN.

Шлюз комплексной безопасности FortiGate имеет следующий функционал: маршрутизатор (роутер); межсетевой экран (Next-Generation Firewall); IPSec и SSL VPN; WAN-оптимизация; Traffic shaping (трафик-монитор); контроль доступа к сети (NAC); интеллектуальный контроль приложений; веб-фильтр; предотвращение утечки данных (DLP); контроль уязвимостей; антиспам (AS); антивирус (AV); система предотвращения вторжений (IPS — Intrusion Prevention System); WiFi-контроллер.

Устройство FortiGate-100D позволяет закрыть большую часть указанных нами требований к системе информационной безопасности. Однако некоторые задачи все же остались невыполненными. Поэтому рекомендуется использовать в комплексе с FortiGate-100D разработку компании «Лаборатория Касперского» для среднего бизнеса — Kaspersky Endpoint Security. Это программное обеспечение дублирует некоторые функции FortiGate-100D, но уже на уровне рабочих станций и серверов в программной среде, и дополняет теми, которые физическое устройство не в силах закрыть.

Возможности, реализованные в Kaspersky Endpoint Security:

- контроль и защита всех рабочих мест (рабочих станций, ноутбуков и файловых серверов);
- шифрование данных;
- контроль и защита мобильных устройств;
- управление мобильными устройствами;
- средства системного администрирования;
- контроль программ, устройств и веб-ресурсов;
- централизованная консоль управления.

Контроль и защита всех рабочих мест

Защита от вредоносного ПО; анализ поведения программ; система предотвращения вторжений (HIPS — Host-based Intrusion Prevention System) и сетевой экран; функция защиты от сетевых атак; гибкие возможности управления и формирования отчетов; поддержка виртуализации; простое управление и формирование отчетов.

Шифрование данных

Для обеспечения безопасности данных в случае несанкционированного доступа к файлам в Kaspersky Endpoint Security предусмотрена возможность как полного шифрования диска, так и шифрование файлов данных. Все задачи шифрования и дешифрования выполняются «на лету», работает контроль активности программ.

Контроль и защита мобильных устройств

Проверка каждого файла, программы и вложения электронной почты на наличие вре-

доносных программ; контроль приложений на мобильных устройствах; шифрование данных на мобильных устройствах; раздельное хранение данных на мобильных устройствах; блокировка мобильного устройства в случае кражи или утери, определение его местонахождения и (или) удаление с устройства любых корпоративных данных.

Управление мобильными устройствами

Kaspersky Endpoint Security дает возможность управления мобильными устройствами (MDM), включая поддержку Active Directory, Microsoft Exchange ActiveSync и Apple MDM Server; запрет незащищенным устройствам доступа к системам и данным.

Средства системного администрирования

Автоматическое обнаружение устройств и программ в сети и занесение их в реестр; автоматическое обнаружение уязвимостей и установка необходимых исправлений; удаленный доступ к любому компьютеру в корпоративной сети, в том числе развертывание нового программного обеспечения в другом офисе; защита от проникновения вредоносного программного обеспечения при подключении гостевых устройств к вашей сети.

Контроль программ, устройств и веб-ресурсов

Отслеживание и контроль программ, работающих в корпоративных системах; контроль устройств в зависимости от способа подключения, типа или заводского номера устройства; контроль активности сотрудников в интернете и фильтрация веб-ресурсов.

Единая консоль управления

Консоль обеспечивает управление всеми модулями Kaspersky Endpoint Security через единый интерфейс; централизованный модуль управления позволяет получать сводные отчеты о состоянии и об инцидентах службы информационной безопасности.

Более подробное описание состава продуктов и их функциональные возможности можно прочесть на сайте компании-разработчика.

Учитывая краткую характеристику представленных продуктов, мы можем сделать вывод, что в случае их совместного применения они позволяют закрыть все обязательные требования, предъявляемые к системе информационной безопасности, и два из трех дополнительно рекомендуемых.

Применение комплексного подхода в решении задач информационной безопасности помогает решить сразу несколько задач:

- обеспечение непрерывности бизнес процессов;
- гибкость и масштабируемость системы ИБ;
- обеспечение оптимального сочетания уровня безопасности и производительности IT-инфраструктуры;
- организации простой эксплуатации и удобного обслуживания;
- экономия ресурсов.

С чего начать? ИБ-аудит

Перед серьезными структурными изменениями информационной системы необходимо провести аудит информационной безопасности, который выявит реальную текущую картину (состояние системы), поможет сформулировать цели и задачи перед службой ИБ, позволит собрать и структурировать необходимую для проекта информацию.

Результаты аудита, который сэкономит средства и время компании и поможет избежать ошибок при построении системы ИБ, помогут выбрать оптимальное решение и путь его внедрения.

Конечно же, «правильного» или типового аудита не бывает. Для разных секторов экономики, компаний, различающихся по масштабу и структуре, этот процесс существенно различается. Типовая услуга, как правило, несостоятельна, так как модель ведения бизнеса, его цели и задачи являются уникальными.

Softline предлагает услуги по аудиту и внедрению всем заинтересованным в сотрудничестве клиентам. Наши специалисты готовы выполнять любые работы, начиная от аудита и заканчивая поддержкой реализованного проекта. Инженеры и аналитики нашей компании имеют все соответствующие компетенции, подтвержденные дипломами, отраслевыми и международными сертификатами.

Как и в случае с выбором продукта, к внедрению необходим комплексный подход, и Softline готова помочь на всех этапах его реализации. Если вы желаете получить проект под «ключ» — вы обратились по адресу!

№ п/п	Подсистема общей системы информационной безопасности	FortiGate-100D	Kaspersky Endpoint Security
1.	Подсистема виртуальных частных сетей (VPN)	+	
2.	Подсистема защиты удаленных и мобильных пользователей (MDM)		+
3.	Подсистема межсетевого экранирования	+	+
4.	Подсистема обнаружения и предотвращения вторжений (IDS/IPS)	+	
5.	Подсистема безопасного доступа к сети Интернет, защита веб-трафика (брандмауэр, файервол, защита электронной почты, прокси-сервер)	+	+
6.	Подсистема фильтрации электронной почты (Antivirus/Antispam)	+	+
7.	Подсистема предотвращения утечек конфиденциальных данных (DLP)	+	
8.	Подсистема мониторинга и управления средствами защиты (единая консоль управления)	+	+
9.	Подсистема сбора и анализа журналов регистрации событий		+
10.	Подсистема шифрования данных при хранении		+

Семейство решений IdM

Автор: Виктор Ивановский, заместитель руководителя направления инфраструктурных решений ИБ, Департамент информационной безопасности Softline

На российском рынке средств защиты информации значительное место начинают занимать системы управления идентификацией и доступом к информационным ресурсам предприятия (IdM).

IdM-система, занимающаяся задачей управления учетными записями, организует несколько важных процессов.

1. Создание единой инфраструктуры для управления всеми учетными записями. Этот сегмент включает в себя продукты и решения, которые непосредственно формируют информационное пространство для управления аккаунтами: директории, метадиректории и виртуальные директории.
2. Централизованное управление аккаунтами и связанными с ними привилегиями. Сюда можно отнести продукты для управления аккаунтами пользователей, их атрибутами и правами, включая создание, удаление, управление ролями, паролями и привилегиями. Эта категория также включает в себя функциональные элементы, как для собственного, так и для делегированного администрирования.

Сочетание этих функций представляет собой стандартное IdM-решение. Следующие две группы относятся к продуктам Identity and Access Management (IAM) — системам управления идентификацией и доступом. Они могут осуществлять:

- контроль доступа к IT-ресурсам. Эти решения координируют доступ пользователей к различным приложениям. Сюда можно отнести всевозможные продукты для унифицированного доступа к ресурсам посредством одной учетной записи Single Sign-on (SSO) и группировки по уровням доступа (Federation);
- аудит доступа и административных активностей. К этому сегменту относится ПО, которое позволяет записывать и контролировать действия аккаунтов с административными привилегиями (так называемый Identity Audit). Сюда же относятся средства аудита и корреляции активностей учетных записей (может использоваться SSO), а также средства аттестации привилегий, которые позволяют проверять корректность выдачи прав отдельным аккаунтам.

До прихода на рынок IdM-решений перечисленный выше список задач решался либо с помощью встроенных в операционную систему и прикладных инструментальных решений, либо организационно.

Что нового в функционале IdM и IAM?

Управлять учетными записями — не значит управлять всеми процессами, которые с ними связаны. Представьте себе, что вы руководите выдачей водительских прав (самая наглядная аналогия с учетными данными). Руководство процессом не позволит вам управлять механизмами использования документами. Не получится контролировать правомерность использования, возможность предоставления прав в качестве удостоверения личности в других органах государственной власти — у вас в руках будет только функционал по управлению базой владельцев удостоверений.

В данном примере IAM — это «дорожно-постовые сотрудники», контролирующие подлинность прав, легитимность их предоставления, правомерность их использования для данного транспортного средства. Это также и механизмы, подтверждающие возможность использования прав в качестве удостоверения личности в государственных и коммерческих организациях.

IdM же позволяет навести порядок в учетных данных пользователей и информационных системах, вводить правила предоставления документов, задействовать механизмы контроля исполнения правил.

Возвращаясь к аналогиям — в сентябре этого года на авиашоу МАКС-2013 в небе находились российские истребители Су-27 и Ту-50. Первый относится к четвертому поколению истребителей, второй — к пятому. Критерий для причисления самолетов к той или иной категории — дополнительный функционал. Если отсутствуют малозаметность, изменяемый вектор тяги, многоканальная ЭДСУ — речи о пятом поколении быть уже не может. Так и с описываемыми системами: если нет механизмов многофакторной аутентификации, возможности организовать Single Sign-on-процессы, то решение не может называться IAM, только IdM.

Кому интересны IdM-решения?

В первую очередь, компаниям финансового сектора. Кредитные организации проявляют четко выраженный интерес к внедрению систем такого класса. За ними идут телекоммуникационные компании и ритейл. Если ранее разговоры чаще всего шли об IdM-системах, то сейчас наблюдается рост запросов именно на комплексные решения.

Существует несколько критериев, по которым можно определить, стоит ли компании внедрять IdM или IAM. Один из таких критериев — количество пользователей. Калькуляторы ROI позволяют четко определить, что возврат затрат на внедрение в организациях с числом сотрудников менее 300 человек может растянуться на долгое время.

Дополнительно накладывается фактор количества информационных систем, эксплуатируемых в компании, и разветвленность филиальной структуры.

Финансовая привлекательность инвестиций в IdM напрямую зависит от особенностей администрирования инфраструктуры: чем она сложнее, тем больше выгода от использования IdM/IAM-решений.

Внедрение «чистого» IdM позволяет снизить нагрузку на службы администрирования, а появление в компании механизмов IAM

помогает улучшить работу пользователей и усилить меры безопасности (SSO, многофакторная аутентификация).

Появление единого программного комплекса, позволяющего автоматизировать многие процессы и значительно снизить ресурсные затраты на обслуживание инфраструктуры, привело к возникновению новой продуктовой ниши на стыке ИБ и управления информационной инфраструктурой. По оценке исследовательской компании Forrester Research (Identity Management Market Forecast: 2007 to 2014), объем рынка IdM в 2012 году оценивался в $10 млрд, а прогноз на 2014 год дает число $12,3 млрд. Среднегодовой рост этого рынка за последние 8 лет составил более 21%.

Российский рынок можно приблизительно оценить в 1/20 мирового, не более $500 млн. Это связано с недоверием, с которым компании относятся к решениям IdM, с переменным успехом работающим на западном рынке. Если сверяться с квадратом Гартнера, то оказывается, что множество упомянутых там программных продуктов просто отсутствует в числе предлагаемых российскими интеграторами.

Дело в том, что компании не стремятся внедрять у себя информационные системы, не прошедшие апробацию в российских условиях. Исключение составляют лишь организации с долей участия западного капитала или топ-менеджерами из стран Европы или Америки. Как правило, они стараются использовать в работе те методики и инструменты, с которыми привыкли иметь дело ранее, а это приводит их к расставлению приоритетов в пользу дебютантов на российском рынке.

Что касается лидеров отрасли и наличия универсального решения, то таковых не наблюдается. Во-первых, это связано с уникальностью каждого серьезного проекта. Во-вторых, индустрия находится в постоянном движении. Год-два назад были популярны инструменты для оптимизации процессов управления инфраструктурой Active Directory. Сейчас наблюдается движение от Enterprise-решений в сторону IdMaaS-сервисов. Причиной сложившейся ситуации стала ориентация на пул решений с постоянным пересмотром его основного состава. Выбор конечного продукта зависит от задач, которые стоят перед клиентом. На основании его потребностей и предлагаются те варианты, которые будут максимально эффективными с точки зрения функциональности и затрат.

Дорого ли это — внедрить IdM-систему?

Говорить о четком ценнике на внедрение системы невозможно. Скорее это будет крайне широкая вилка цен с размытой дальней границей. Естественно, все базируется на наборе факторов, которые определяются как постановкой задачи, так и сложностью инфраструктуры.

Объект, с которым работает IdM- или IAM-система, — это не учетная запись, как может показаться на первый взгляд, а процесс. Например, создания учетных данных, их синхронизации с целевыми информационными системами, процесс согласования предоставления доступа, процесс самого предоставления доступа в систему. И тут крайне важно понимать: необходимо ли менять информационные процессы или достаточно их только автоматизировать.

В случае автоматизации (внедрение «снизу») задача специалистов — заставить IdM выполнять задачи, за которые ранее отвечали администраторы. Этот процесс может занять от месяца до трех в зависимости от сложности интеграции с кадровыми и целевыми информационными системами.

В тех же случаях, когда внедрение идет «сверху», от информационных процессов, перед непосредственной настройкой комплекса требуется сформировать набор модифицированных правил, процессов, требований, моделей. Все они позволят не только ускорить операции, производящиеся в инфраструктуре заказчика, но и оптимизировать процессы целиком за счет выбора лучшего пути принятия решений. Итогом разработки новых моделей может послужить возможность, например, вдвое сократить число согласований при рассмотрении заявок.

Новые веяния в архитектуре информационных систем и идеология IAM

Набирающий популярность BYOD-подход расширяет границы применимости политик, правил и процессов предоставления доступа. При этом мобильность сильно влияет на развитие технологий аутентификации: наблюдается высокий спрос на решения на базе одноразовых паролей, и, возможно, однажды они нацелятся на вытеснение SSO-решений в компаниях численностью до 200–300 пользователей, но это лишь часть IAM-блока. На рынке появляются «облачные» решения, которые предоставляют возможность держать базы учетных записей за пределами организации, во внешнем ЦОД, и это уже серьезное изменение архитектуры IAM. Можно утверждать, что будущее IAM — за сервисной моделью, на внутриорганизационном уровне, либо на базе сервисной аутсорсинговой модели.

Главным препятствиям на пути активного роста данной ниши рынка стала осторожность потенциальных заказчиков и их неосведомленность о потенциальной выгоде внедрения системы. Тем не менее, существует набор калькуляторов ROI, с помощью которых можно рассчитать окупаемость затрат на внедрение и поддержку инфраструктуры.

Опасения выражаются и в неготовности передачи ряда процессов и функций, связанных с безопасностью, автоматизированной системе. В пресс-релизах российских компаний чаще всего возникает упоминание о внедрении Microsoft Forefront Identity Manager. Данный продукт успешно вошел в инфраструктуры российских компаний вместе с пакетами Enterprise Agreement и примером своих внедрений вдохновляет других специалистов и директоров, которые начинают рассматривать его в качестве IdM-инструмента.

Для принятия решения о переходе на новую модель управления учетными данными некоторым российским предприятиям может понадобиться время на дополнительное изучение предлагаемых рынком IdM-систем.

Контентная фильтрация и решения, представленные на рынке: McAfee, Websense, Blue Coat

Автор: Юлия Кизимова, менеджер по продаже услуг, Департамент информационной безопасности Softline

Контентная фильтрация — процесс фильтрации данных, передаваемых по различным каналам, на основе их содержания и последующая блокировка нежелательного контента.

Стоит отметить, что контентная фильтрация представляет собой совокупность различных методов (а не одну технологию), например: анализ на основе регулярных выражений, распознавание изображений, использование репутационных баз URL. Современные системы контентной фильтрации позволяют мгновенно определять категории новых сайтов и динамического контента, в режиме реального времени анализировать весь веб-трафик, обнаруживать угрозы и блокировать доступ.

Контентная фильтрация помогает предотвратить:

- влияние вредоносных программ;
- доступ к запрещенным сайтам;
- утечки данных;
- фишинг-атаки;
- веб-угрозы;
- включение развлекательных функций порталов и т.д.

Контентная фильтрация широко распространена и встречается как в виде отдельной системы, так и в составе современных корпоративных систем безопасности (например, DLP-систем).

Использовать или нет?

Необходимость применения систем контентной фильтрации — вопрос дискуссионный. Использовать ее в учебных заведениях призывает государство, игнорирование требований которого грозит вполне реальной ответственностью. Целесообразность принятия этой меры можно поставить под сомнение, ведь у учеников на уроках в принципе не должно быть времени на поиски и просмотр постороннего контента в Интернете, да и жесткие рамки поиска информации в школе вовсе не ограничивают возможностей учеников дома.

В сфере бизнеса дела обстоят по-другому, и использовать контентную фильтрацию никто никого не призывает и не заставляет. Таким образом, возникает масса вопросов, касающихся обоснования использования данной системы, которые работодатели склонны решать положительно. По статистике, около 65% работников пользуются социальными сетями в рабочее время, и если полный запрет их использования во многих компаниях уже считается «негуманным», то запрет использования, например, всевозможных развлекательных приложений особых возражений не вызывает.

Преимущества

Системы контентной фильтрации легко решают проблемы безопасности, возникающие в связи с использованием всевозможных облачных приложений (Skype, YouTube и др.).

Кроме того, подобные системы позволяют защититься от утечек данных, нарушения нормативных требований, спама, вредоносного мобильного кода и многого другого. Современные системы также позволяют обеспечить веб-защиту мобильных сотрудников, отличную масштабируемость и управляемость, а результаты работы руководитель всегда сможет оценить с помощью гибко настраиваемой по различным показателям отчетности. В зависимости от структуры и бизнес-задач компании при выборе системы контентной фильтрации необходимо учитывать:

- количество выходов в Интернет;
- ширину канала;
- платформу реализации (физическая или виртуальная);
- необходимость контроля мобильных устройств сотрудников (ноутбуки, планшеты, телефоны).

Системы поставляются в виде ПО, аппаратных средств и в формате облачного сервиса.

Рынок систем контентной фильтрации постоянно развивается, и, безусловно, уже сформировались лидеры. Рассмотрим более подробно решения трех производителей — McAfee, Websense, Blue Coat.

McAfee

В состав продукта, предлагаемого McAfee, входит два антивирусных «движка», что обеспечивает хорошую защиту от вредоносного программного обеспечения (с применением эмуляции) и позволяет настраивать чувствительность его обнаружения. ПО McAfee имеет хороший контроль приложений и предоставляет возможности удаления выбранных функций веб-приложений (например, блокировку создания сообщений в социальных сетях). Поддерживается квотирование трафика по времени и объему, при этом пользователь по умолчанию видит остаток лимита трафика. Решение интегрируется с McAfee DLP и может управляться

из единой консоли управления McAfee ePolicy Orchestrator, что немаловажно для клиентов, уже использующих продукты McAfee.

Слабые стороны: не поддерживаются конечные точки на базе Mac OS X; решение в формате «облачного» сервиса не имеет достаточной детализации политик, а отсутствие поддержки IPsec в облаке препятствует поддержке мобильных устройств. Присутствуют недостатки при категоризации сайтов Рунета.

Websense

Решение обладает надежной защитой от вредоносного программного обеспечения, интегрируется с решением Websense DLP и имеет единую консоль управления Triton. Есть возможность квотирования трафика. Решение обладает самой полной URL-базой и наилучшей категоризацией сайтов благодаря дополнительной классификации с помощью «облачного» сервиса. Трудностей с «пониманием» российских сайтов при работе не возникает. Облако поддерживает IPsec и несколько вариантов аутентификации пользователей (в том числе и SAML).

Однако данное решение является довольно дорогим, а модель лицензирования по количеству IP-адресов не очень удобна в условиях все более набирающей популярность модели BYOD.

Blue Coat

Proxy SG является «сильным» решением из-за богатого набора функций, внушительного количества поддерживаемых протоколов и поддержки мобильных устройств на базе Mac OS X, Apple iOS и Windows. Поддерживает квотирование трафика по времени и скорости. Решение аппаратного вида хорошо интегрируется с облаком и позволяет синхронизировать политики, настроенные в облаке, с локальным устройством, а отчетность можно просматривать с помощью единой консоли Reporter. Также с помощью облачного сервиса осуществляется дополнительная категоризация.

Антивирус для данного решения приобретается отдельно, на выбор можно приобрести один из пяти антивирусных «движков» — McAfee, Kaspersky, Sophos и т. д. Решение поставляется на английском языке, и русификация не ожидается. Российские сайты категоризированы, можно гибко настроить политики доступа пользователей к ресурсам выбранного сайта (например, заблокировать доступ к видеоконтенту vk.com).

Помимо описанных выше систем, на российском рынке представлены решения от Check Point, Symantec, Barracuda, PineApp и др., и у каждого из производителей имеются свои отличительные функциональные особенности.

Новое в области персональных данных

Автор: Сергей Карпунин, менеджер по продаже услуг, Департамент информационной безопасности Softline

Вопрос обеспечения безопасности персональных данных (ПДн) можно назвать одним из наиболее актуальных в области информационной безопасности в России за последние несколько лет. До появления всем известного Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в отечественном законодательстве не были закреплены обязанности по «массовой» защите информации. Существовали требования в части сведений, отнесенных к государственной тайне (ГТ), однако масштабы распространения ГТ и ПДн существенно различаются. Когда в 2006 году был принят 152-ФЗ, появились совершенно новые для российской действительности правовые категории: оператор, информационная система персональных данных, обработка и т. д.

Разумеется, появление нового закона сразу же породило массу вопросов, неясностей, спорных моментов. Но наиболее значимым стало то, что почти для всех юридических лиц страны появились обязательные требования по соблюдению конфиденциальности обрабатываемых ими ПДн и обеспечению надлежащего порядка их обработки.

Закон распространяется на всех

Объектом дискуссий долгое время оставалась трактовка самого термина «персональные данные». Причиной тому было нежелание многих операторов признавать факт обработки ими персональных данных и, как следствие, обязанностей по защите ПДн. Нежелание тратить усилия и материальные ресурсы на построение адекватной системы защиты вполне объяснимо. Достаточно широкое распространение получила ошибочная точка зрения, что персональными данными являются лишь сведения, позволяющие однозначно идентифицировать субъекта. Однако поправка к закону (Федеральный закон от 05.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных») расставила все по своим местам, закрепив на законодательном уровне тот факт, что персональными данными является «любая информация, прямо или косвенно относящаяся к определенному или определяемому лицу». Таким образом, стало ясно, что каждая организация, согласно законодательству о ПДн, является оператором и должна соблюдать ряд правил, касающихся обработки и защиты персональных данных.

Какова позиция операторов в отношении безопасности ПДн?

Она до сих пор остается неоднозначной: многие так и не пришли к ясному пониманию того, что закон распространяется на всех. Закон есть закон, и его следует соблюдать. Следовательно, если ведется обработка персональных данных, то необходимо обеспечить и их защиту. Часть операторов просто игнорирует требования по защите ПДн, уповая на то, что проверка их не коснется, а потому нет нужды что-либо делать. Иные сочли достаточным просто принять соответствующую политику внутри организации, получить согласия субъектов на обработку ПДн, решив, что этого достаточно для выполнения всех требований. Некоторые операторы решили ограничиться установкой удобных для себя средств защиты, оставляя за скобками остальные подсистемы защиты ПДн. Безусловно, описанные выше подходы являются недостаточными для выполнения всех требований законодательства в части защиты ПДн. По сути, это либо отсутствие знаний и желания вникать в суть проблемы, либо сознательное нарушение закона, спровоцированное стремлением сэкономить.

В противовес желающим отделаться «малой кровью», значительное число компаний выделили защиту ПДн в качестве приоритетного направления ИБ и выразили готовность приводить свои системы в соответствие требованиям законодательства. В основном речь идет о предприятиях, работающих в тех сегментах рынка, для которых необходимость проведения мер, касающихся ИБ, следует из понимания рисков, сопряженных с возможными утечками ПДн. Для таких операторов риски выражаются не только в денежном эквиваленте, но и в потере деловой репутации, снижении доверия со стороны клиентов и контрагентов, повышении уязвимости перед конкурентами. Особенно актуальна данная тема для тех, кто в процессе своей деятельности аккумулирует и обрабатывает всевозможные базы клиентов, — гостиниц, банков, страховых компаний и т. д. Они одними из первых начали интересоваться вопросами защиты персональных данных, выполнять мероприятия по защите своими силами или с привлечением системных интеграторов. И как показывает практика, информационные системы подобных фирм защищены лучше других и чаще удовлетворяют всем требованиям регуляторов.

Вышесказанное резюмируют следующие тезисы:

1. Персональные данные в том или ином виде обрабатывают почти все организа-

Постановление № 1119 внесло существенные коррективы в сложившуюся практику защиты, но и привело к некоторым «нестыковкам»:

- возникла ситуация, когда старые нормативные документы были признаны утратившими силу, а новые еще не появились в объеме, достаточном для проведения всех необходимых работ. То есть было известно, что вместо класса ИСПДн необходимо определить уровень защищенности, но требований по защите каждого из уровней защищенности не существовало;
- появилась проблема с выбором сертифицированных средств защиты. Официальная позиция регуляторов в отношении необходимости применения сертифицированных СЗИ выражена достаточно категорично: если оператор использует какие-либо механизмы защиты, то они должны проходить процедуру оценки соответствия. Единственная на сегодняшний день форма оценки, не вызывающая вопросов у регуляторов, — это сертификация. Сертификация СЗИ проводится на соответствие руководящим документам по защите от несанкционированного доступа. Эти документы были разработаны до появления законодательства о ПДн, поэтому в сертификатах не упоминается о возможности применения СЗИ для обеспечения того или иного уровня защищенности. Не до конца ясно, как соотносить уровни защищенности и требования РД. Эта ситуация была разрешена выходом официального информационного сообщения ФСТЭК России.

ции. И они должны предпринимать меры по обеспечению безопасности ПДн.

2. Необходимость соблюдения требований по обеспечению безопасности ПДн прописана в законе и является очевидной.
3. К защите ПДн лучше подходить ответственно, чтобы минимизировать риски, связанные с невыполнением требований законодательства.

Ключевые изменения в законодательстве

С появлением в 2006 г. Закона о ПДн и последующим выходом подзаконных актов и руководящих документов обеспечение безопасности ПДн выделилось как отдельное направление. Конечно, нормативно-правовая база была далека от идеала и оставляла немало неразрешенных вопросов и спорных моментов. Однако за несколько лет ее существования был создан единый подход к защите ПДн, наработан практический опыт. Опираясь на этот подход, значительная часть операторов приступила к созданию систем защиты персональных данных, основываясь на существующих требованиях, и многие организации уже успешно выполнили требования законодательства.

Новой вехой в процессе становления и развития темы ПДн стало внесение изменений в ФЗ-152 в 2011 году. Они коснулись основных понятий закона, в частности, самого определения персональных данных, понятия автоматизированной обработки ПДн и законных оснований для обработки ПДн. Вместе с тем был существенно расширен и конкретизирован перечень мер по защите персональных данных, а также добавлены положения, касающиеся условий поручения обработки ПДн третьим лицам и назначения ответственных за организацию обработки ПДн. Также в данной редакции ФЗ было анонсировано появление в скором времени подзаконных актов, определяющих новые подходы к классификации (установлению уровней защищенности) ИСПДн и изменение требований по защите.

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» повлекло существенные изменения в подходе к защите ПДн. Ранее набор необходимых организационных и технических мер по защите ПДн определялся классом ИСПДн, который присваивался операторам по результатам рассмотрения совокупности показателей, таких как количество субъектов ПДн в системе, характера ПДн, а также с учетом модели угроз (порядок классификации ИСПДн от К4 до К1 устанавливался совместным приказом ФСБ России, ФСТЭК России и Мининформсвязи России от 13.02.2008 № 55/86/20). В ПП-1119 вместо присвоения ИСПДн класса появилась необходимость установления уровня защищенности, причем методология определения уровней защищенности существенно отличается от методологии присвоения класса. Новый нормативный документ связал уровни защищенности с актуальными угрозами наличия недекларированных возможностей программного обеспечения, категориями ПДн, количеством и типом субъектов.

Одним из последних на сегодняшний день документов стал приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Наконец появилось руководство к действию, снявшее целый ряд вопросов относительно того, какие меры по защите ПДн должны быть реализованы. Новый документ внес существенные изменения как в методологию выбора и порядок реализации защитных мер, так и в сам состав этих мер. Были добавлены новые подсистемы защиты ПДн, соответствующие современным тенденциям в области развития IT (например, необходимость защиты виртуальной инфраструктуры). Выбор и реализация мер по защите ПДн, согласно новому приказу, должны осуществляться с учетом их экономической целесообразности, что соответствует лучшим мировым практикам в области ИБ. То, что разработка

приказа велась при участии экспертного сообщества, благоприятно отразилось на качестве этого документа. По сравнению с предыдущими нормативными документами, предлагаемые в приказе ФСТЭК России от 18.02.2013 № 21 меры выглядят более убедительно и современно, сам подход к построению системы защиты ПДн допускает значительно больше гибкости и свободы. Однако выполнение всех новых требований влечет за собой повышение сложности реализации СЗПДн, что предполагает наличие специальных знаний в области защиты информации.

Модернизация

Первоначально предполагалось (и было отражено в проекте приказа), что новые требования будут распространяться лишь на вновь создаваемые ИСПДн или СЗПДн. Однако это положение не вошло в окончательную версию документа. Таким образом, под действие приказа ФСТЭК России от 18.02.2013 № 21 попадают как создаваемые, так и уже созданные ИСПДн и СЗПДн.

Что делать тем, кто уже привел свои системы в соответствие требованиям нормативно-правовых актов, ныне утративших силу? Операторы, уже выполнившие все необходимые требования, поступили разумно, и все их старания не напрасны. Да, на реализацию СЗПДн были затрачены определенные усилия и средства, но утверждать, что с изменением нормативной базы все придется переделывать, неверно. Отметим, что новые требования не предполагают кардинально иного подхода к защите ПДн, базовые принципы остались теми же. Изменения коснулись лишь некоторых, хоть и немаловажных, деталей.

Кроме того, существующие сертифицированные средства защиты также остаются актуальными для использования. Необходимости в существенной переработке технической составляющей СЗПДн нет. Имея уже реализованную и функционирующую систему, адаптировать ее под новые требования гораздо проще и дешевле, чем создавать заново. Поэтому можно утверждать, что тот, кто раньше уже что-то сделал для защиты ПДн, в любом случае оказывается в выигрышной позиции по сравнению с теми, кому только предстоит провести полный комплекс работ. Анализируя текущую ситуацию, можно с определенной уверенностью сказать, что дальнейшее развитие нормативно-правовой базы неизбежно. Будут выходить новые документы, новые требования, появятся новые обязанности. Сегодня операторам необходимо всерьез задуматься о модернизации созданных ими систем защиты ПДн. Системы, реализованные по старым требованиям, не пройдут проверку регуляторов. Существуют новые, четко определенные, официально утвержденные и вступившие в силу требования — придется соответствовать.

Что необходимо переделать? Скорее всего, придется пересмотреть разработанные модели угроз, уточнив актуальность угроз, связанных с НДВ в операционных системах и прикладном программном обеспечении. Также потребуют переработки акты классификации ИСПДн. Согласно новым требованиям нужно разработать и оформить акты, определяющие уровень защищенности систем с учетом анализа ряда характеристик и факторов, которые до этого не рассматривались при классификации ИСПДн. Следующими шагами станут: определение набора требований, выбор способов их выполнения, сопоставление с уже реализованными мерами защиты, принятие решения о необходимости доработки и доработка СЗПДн.

При этом важно понимать, что сложность процесса модернизации системы защиты напрямую зависит от масштабов ИСПДн. Для крупных организаций с большим количеством ИСПДн, АРМ и серверов оптимальным представляется проведение актуализации полным комплексом работ: начиная от аудита соответствия требованиям законодательства в области ПДн, заканчивая процедурой аттестации (при наличии ее необходимости). При этом большая часть работ придется на долю пересмотра имеющихся документов и создания новых.

Отдельно хотелось бы упомянуть о сертификатах на уже используемые средства защиты информации. Если для защиты ИСПДн класса К1 использовались сертифицированные средства защиты, то согласно официальному разъяснению ФСТЭК России эти СЗИ могут быть использованы для защиты ИСПДн самого высокого уровня защищенности. Если же система имела класс К2, то используемые в ней средства защиты (при условии, что они сертифицированы до К2 включительно) не могут обеспечить уровня защищенности выше четвертого. Очевидно, что при установлении по каким-либо причинам более высокого уровня защищенности для ИСПДн, придется использовать СЗИ, имеющие подходящие сертификаты.

Делать самим или привлекать интегратора?

Наверное, этот вопрос звучит так же часто, как часто возникает необходимость внедрения какого-либо проекта в области ИБ. Есть две точки зрения, каждая из которых в равной мере имеет право на существование. Одна из них заключается в том, что если в штате организации есть квалифицированные специалисты по информационной безопасности, то им под силу самостоятельно привести свои ИСПДн в соответствие с требованиями регуляторов. Законодательно такие работы проводить не запрещено. К слову, всем известно, что долгое время вопрос о необходимости получения лицензии на деятельность по технической защите конфиденциальной информации оставался открытым, велись оживленные дискуссии на данную тему. Не так давно ФСТЭК России все же дал свои разъяснения, согласно которым получать лицензии нет нужды, если оператор не планирует извлекать прибыль из деятельности по защите информации и если защита информации не указана в каче-

стве основного вида деятельности в учредительных документах юридического лица.

В качестве аргументов в поддержку привлечения интегратора можно назвать массу преимуществ (хотя, конечно, есть и свои недостатки). Наиболее весомыми доводами в пользу работы с интегратором можно считать следующие:

- работая с интегратором, вы поручаете решение конкретных задач профессионалам в данной области, имеющим богатый опыт, что в какой-то мере гарантирует положительный результат. Действительно, штатные специалисты по ИБ могут быть (точнее, должны быть) достаточно квалифицированными, но в компании-интеграторе работают люди, постоянно занятые в подобных проектах, обладающие необходимой базой знаний, инструментарием, практическими навыками разработки и внедрения СЗПДн, знающие возможные проблемные ситуации и пути выхода из них, что в значительной степени обеспечивает качество выполнения работ. Работа с интегратором позволит избежать многих распространенных ошибок и выработать решения по оптимизации процессов обработки персональных данных, инфраструктуры заказчика, системы защиты, что может существенно снизить затраты на реализацию мер по обеспечению безопасности ПДн. Для достижения наилучшего результата при работе с интегратором от заказчика требуется правильно формулировать свои требования и контролировать процесс реализации проекта на всех стадиях. Еще одним явным плюсом сотрудничества с компаниями, специализирующимися на оказании услуг в сфере ИБ, является наличие в их штате высококвалифицированных инженеров, способных в короткие сроки корректно внедрить СЗИ, что зачастую оказывается не под силу штатным специалистам заказчика ввиду отсутствия опыта и постоянной практики. В компании-интеграторе же, как правило, есть вся необходимая материально-техническая база (тренировочные стенды и набор наиболее часто применяемых аппаратных и программных средств защиты) для того, чтобы инженеры имели возможность изучить особенности установки и настройки конкретных технических решений, что позволяет значительно снизить вероятность возникновения ошибок и сбоев на площадках клиента;
- приведение ИСПДн в соответствие требованиям законодательства силами интегратора позволит уйти от части рисков, связанных с реализацией угроз безопасности ПДн и, как следствие, нарушений характеристик безопасности ПДн. Это утверждение в полной мере справедливо в случаях, когда работы по обеспечению безопасности ПДн завершаются аттестацией ИСПДн на соответствие требованиям безопасности информации. В этом случае интегратор как лицензиат ФСТЭК России несет ответственность за выданные аттестаты соответствия (иными словами, никто не будет рисковать своей лицензией и выдавать аттестат на систему, которая явно не соответствует требованиям). И хотя аттестация в большинстве случаев носит добровольный характер и влечет за собой дополнительные денежные затраты, оператору очень часто бывает целесообразно провести аттестацию своих систем, получив официальное подтверждение соответствия по результатам проведения работ по защите ПДн.

Приведенные доводы не отвечают однозначно на вопрос о необходимости привлечения интегратора к выполнению работ по защите персональных данных, окончательное решение остается за оператором, так как именно на него законом возложены обязательства по обеспечению безопасности ПДн и он вправе выбирать, каким путем ему пойти.

Почему Softline?

Число компаний, позиционирующих себя как системных интеграторов, достаточно велико. Все они имеют множество различий и особенностей, как то: масштабы выполняемых проектов, перечень оказываемых услуг, целевые группы потребителей, количество и квалификация специалистов в штате, принципы организации работы и др. Поэтому при выборе людей, которым все-таки стоит доверить реализацию проекта, могут возникнуть затруднения. Ориентироваться в решении данного вопроса следует, в первую очередь, на качество выполняемых работ.

Особенностью подхода компании Softline является клиентоориентированность. Мы знаем, что каждый клиент уникален и у каждого свои потребности. Одним из наших ключевых стремлений является отказ от шаблонного подхода, практикуемого многими интеграторами сегодня. Мы поможем вам провести необходимые работы в области ИБ (и в области защиты персональных данных в том числе). Перед началом каждого проекта нам важно понять, какие цели ставит перед собой клиент и что он хочет увидеть в результате. Если речь идет о compliance в чистом виде, мы можем создать систему, позволяющую выполнить все нормативные требования и при этом не перегружающую IT-инфраструктуру, не затрудняющую ход основных бизнес-процессов. Наши специалисты имеют богатый опыт применения эффективных решений по обеспечению безопасности информации и готовы предложить на выбор несколько вариантов решения проблемы с детальным обоснованием преимуществ и недостатков каждого из них. Клиенту остается лишь правильно формулировать цели и задачи и сделать свой выбор.

Порталы как элемент управления информационной безопасностью

Управление информационной безопасностью становится все более сложной задачей, связанной с функционированием большого числа различных внутренних процессов, которые так или иначе влияют на деятельность всей организации. При внедрении комплексной системы управления ИБ часто возникает необходимость оперативного доступа к большому количеству документации, своевременным и удобным коммуникациям с ответственными лицами из различных подразделений компании, управлению задачами в области ИБ, контролю достижения целевых показателей по процессам ИБ и многие другие вопросы.

Автор: Андрей Ивушкин, руководитель направления экспертных услуг и решений отдела поддержки продаж, Департамент информационной безопасности Softline

Разработка и реализация методологии подготовки и механизмов контроля сотрудников в части ИБ с использованием современных информационно-коммуникативных технологий является эффективным и экономичным решением большинства управленческих задач, позволяющим снять с руководства ряд рутинных вопросов и облегчить организации взаимодействие по процессам ИБ.

Принимая во внимание существующий уровень развития информационно-коммуникативных технологий и необходимость осуществления полноценного интерактивного взаимодействия с сотрудниками, наиболее эффективной платформой для достижения целей в текущих реалиях представляется использование портальных технологий, которые, в том числе, позволяют получить ряд новых специализированных разделов по вопросам информационной безопасности на внутреннем корпоративном ресурсе.

Помимо удобства использования подобные решения способны выполнять различные требования и рекомендации специализированных стандартов в сфере ИБ, которые ставят перед специалистами по безопасности задачи по эффективному информированию сотрудников в сфере ИБ, повышению общего уровня лояльности персонала с целью понижения рисков мошенничества и различных злоупотреблений.

Решение с минимальными затратами и максимальным эффектом

Внутренний корпоративный портал по информационной безопасности, разрабатываемый для организации, выполняет, как правило, следующие базовые функции:

- визуализирует требования по ИБ в простой и наглядной форме и удобном формате;
- ведет базу документации по ИБ;
- дает возможность публиковать новости;
- обеспечивает настройку и подключение RSS-каналов в области ИБ;
- размещает обучающие курсы, презентации, видеоуроки;
- дает возможность создавать тесты по ИБ различных уровней сложности, конкурсы, опросы (в том числе анонимные);
- обеспечивает обратную связь;
- предоставляет площадку для форума по вопросам ИБ;
- предоставляет статистику по результатам обучения и проведения опросов в области ИБ для просмотра и анализа;
- помогает создавать автоматические рассылки по нововведениям на портале;
- осуществляет поиск по содержанию.

Данная система может взаимодействовать с другими системами и сервисами в рамках процессов обеспечения информационной безопасности организации. Интеграция возможна как с промышленными решениями ServiceDesk, системами СКУД, так и с собственными разработками. При этом могут быть разработаны различные интерфейсы для бизнес-пользователей и администраторов системы с функционалом, необходимым сотрудникам для выполнения своих обязанностей в рамках системы ИБ.

Возможна разработка структуры документации по ИБ различной иерархии, наполнение как международными и отечественными материалами по информационной безопасности, так и внутренней нормативной базой; файлы могут быть доступными для всех пользователей или только для определенных групп.

Новости, конкурсы, тесты

Заметим, что публикация новостей по ИБ, — одна из важнейших составляющих повышения осведомленности в области безопасности. В мировом и отечественном ИБ-сообществе имеется ряд доверенных внешних ресурсов в области защиты информации. Для своевременного ознакомления с последними тенденциями, получения новостей, публикаций сообщества по ИБ портал может быть оснащен возможностью поддержки технологии RSS.

Тесты по информационной безопасности — еще один эффективный элемент повышения осведомленности и контроля выполнений требований по обеспечению информационной безопасности. Предусмотрена возможность создания тестов разного уровня сложности и подготовки по их результатам аналитических отчетов. Создание самих тестов значительно упрощает применение специализированного конструктора, что позволяет специалистам по ИБ самостоятельно создавать и публиковать на портале различные тесты, не овладевая навыками программирования.

Конкурсы по теме информационной безопасности могут также рассматриваться в качестве аспекта повышения лояльности персонала. Реализация подобного механизма достаточно проста, что позволяет быстро включать наиболее активную часть трудового коллектива в общий процесс творчества.

Анонимные обращения, форум, рассылки...

Условная обезличенность опросов по информационной безопасности помогает собрать во всей организации сведения о выполнении какого-либо аспекта требований по ИБ, при этом для пользователя данный опрос является анонимным, что позволяет собрать более объективные данные.

Кроме того, зачастую информация об инцидентах ИБ не доходит до подразделения ИБ, так как пользователи просто боятся обратиться за помощью или заявить о каком-либо факте нарушения. Опция «анонимное обращение» в службу ИБ помогает позволить получить от пользователей подобную информацию. Понимание анонимности при этом весьма относительно, но в случае организации телефонной связи также является эффективным инструментов для повышения лояльности трудового коллектива.

Форум по вопросам ИБ позволяет организовать обсуждение проблем, которые актуальны для всех сотрудников компании. Это также место, где администраторы ИБ официально доносят точку зрения компании до персонала.

Также портал способен реализовывать рассылку об изменениях, происходящих в сфере защиты информации. В зависимости от параметров настройки сообщения информация будет адресована как отдельным группам пользователей, так и всем сотрудникам организации в целом.

Одна из наиболее важных функций подобного решения — поиск всей необходимой сотрудникам информации с различными вариантами ее выдачи.

Все указанные опции реализуются быстро и легко, собственными силами организации или с минимальным привлечением консультантов и разработчиков, но вместе с тем обеспечивают максимальный эффект повышения осведомленности персонала в области ИБ.

...и многое другое!

Также с помощью портального решения возможно управление задачами IT- и ИБ-служб. Руководители данных подразделений смогут определять задачи, сроки, ресурсы, показатели эффективности работы для каждого из своих подчиненных и видеть процент выполнения данных задач, загрузку сотрудников и корректировать ее. Данная опция позволяет уйти от рутинной отчетности в работе подразделения и облегчает подготовку аналитических отчетов руководству.

Возможности портальных технологий для нужд ИБ не исчерпываются вышеуказанными опциями. По мере возникновения в компании новых потребностей они могут расширяться как благодаря использованию специализированных дополнительных программных продуктов, так и посредством доработки портала под нужды заказчика. Это могут быть модули самообслуживания для представления доступа к автоматизированным ресурсам, согласование заявок или документации, управление рисками в масштабах предприятия, классификации информационных активов.

Система коллективного взаимодействия, эффективная в первую очередь в интересах службы ИБ, помогает снижать затраты на внутрикорпоративную коммуникацию, увеличивать производительность труда сотрудников, позволяет совершенствовать бизнес-процессы и повышать общую эффективность бизнеса. Конкретное решение задачи построения комплексной системы управления информационной безопасностью находит свое воплощение в соответствии с потребностями заказчика.

Новое и старое в законодательстве о Национальной платежной системе

Автор: Дмитрий Тирский, менеджер по продажам услуг, Департамент информационной безопасности Softline

Ключевой целью ведения банковского бизнеса является получение прибыли за счет предоставления банковских услуг и продуктов физическим и юридическим лицам. Традиционно безопасность в банковском деле была направлена на сохранение денежных ценностей и банковской тайны (сведений об операциях, клиентах и остатках на счетах), делопроизводство осуществлялось в бумажной форме. Проще говоря, раньше нужны были сейф и охранная сигнализация. Таким образом, исторически сложилась важная, но вторичная роль обеспечения безопасности в банке.

Роль ИБ в банковском бизнесе

Развитие электронных форм обработки информации предопределило, в свою очередь, взрывной рост развития банковского бизнеса. Банки стали ближе к клиенту, сократилось время на обработку операций, стало возможным предоставление банковских продуктов удаленным способом. Таким образом, выделилась отдельная отрасль обеспечения безопасности ведения банковской деятельности — информационная безопасность, направленная как на сохранение в секрете банковской тайны, так и на предотвращение несанкционированного доступа к средствам обработки информации в банке и к телекоммуникационным каналам в случае дистанционного банковского обслуживания (ДБО).

Современные информационные и телекоммуникационные технологии продолжают стремительно прогрессировать. Вместе с тем, их использование позволяет злоумышленникам найти способы получения ценной для банка и клиентов информации и, в конечном итоге, упростить задачу хищения денежных средств.

Таким образом, грамотно сформированная и обслуживаемая система обеспечения информационной безопасности (СОИБ) прямых доходов не принесет, но при этом позволит существенно снизить ущерб при попытках реализации угроз, направленных на несанкционированный доступ к банковской тайне и хищения денежных средств, то есть предотвратит возникновение прямых или косвенных убытков для банка.

«Бумажная» vs «техническая» ИБ

В попытке определить, кто может быть специалистом по информационной безопасности, помимо формальных требований следует определить область его ответственности. Классический процедурный подход в банковской сфере выделяет 4 области:

- информация;
- процессы, в рамках которых проходит ее обработка;
- информационные системы, в которых реализуются данные процессы;
- персонал, реализующий их.

Для обеспечения ИБ в каждой из областей выделяют свои группы требований, выполнение которых требует отдельных, уже неявно формализуемых, качеств у специалиста по информационной безопасности.

Так, например, реализация требований по обеспечению ИБ требует навыков аналитической работы по оценке ее значимости (с учетом владельца информации), полноты, совокупной критичности для ведения банковского бизнеса.

Обеспечение ИБ банковских технологических процессов требует понимания специфики банковской деятельности, знания линейки банковских продуктов, изучения технологий обработки информации и особенностей реализации процессов в соответствии с нормативными документами банковской системы России.

Выполнение требований по обеспечению ИБ для банковских информационных систем требует глубоких знаний технической направленности. Необходимо знание того, как функционируют эти системы, способность к анализу их «слабых»

мест, пониманию работы средств защиты информации (СЗИ), внедренных в данных системах и пр.

Группа требований обеспечения ИБ, направленных на работу с персоналом, требует совсем иных навыков: способности провести обучение, довести до сотрудников причины требований, то есть требуют готовности к активной коммуникации.

Как мы видим, набор требований к специалисту по ИБ достаточно широк. Создать подразделение с группой специалистов, обладающих полным набором компетенций, для банков не всегда представляется возможным. Создание внутренней нормативной базы и выстраивание процессов обеспечения ИБ в банке для выполнения всех остальных групп требований в этом случае отходит на второй план по двум причинам:

- даже очень хороший технический специалист не всегда умеет так же хорошо составлять внутренние нормативные документы (для этого требуется несколько иной бэкграунд — навыки делопроизводства, знание юриспруденции, умение работать с нормативными правовыми актами и пр.);
- не всегда банк имеет возможность привлечь специалиста, обладающего навыками разработки внутренних нормативных документов, с наличием хороших знаний в ИБ, или прием на работу такого специалиста может быть нецелесообразен ввиду кратковременности его работы.

Нормативные особенности ведения банковского бизнеса и ИБ

Ключевыми особенностями банковского бизнеса в России являются требования к формализации всех процессов и сильная роль Банка России, регулирующего банковскую деятельность. В ближайшем рассмотрении каждая из особенностей имеет как свои плюсы, так и минусы.

Формализация процессов банковской деятельности строго определяет круг сотрудников банка в рамках исполняемых ими ролей, что позволяет четко разграничить сферы ответственности и локализовать перечень информации, доступ к которой необходим для процесса. Отрицательной стороной является обилие внутренней нормативной базы по каждому процессу, сложность ее администрирования и коррекции в случае изменения самого бизнес-процесса.

Плюс регулятивной роли Банка России выражается в том, что она позволяет установить однозначные требования по каждому из процессов банковской деятельности и, соответственно, формализовать нормативно-правовую базу. Минус проявляется в том, что на банки ложатся повышенные требования к разработке внутренних нормативных документов и предоставлению отчетности.

Не являются исключением и процессы обеспечения ИБ. С одной стороны, определен четкий набор критериев, которым должны соответствовать банки в этой области. С другой — Банком России однозначно установлены принципы деятельности в рамках построения системы менеджмента ИБ:

- наличие внутренних нормативных документов нескольких уровней иерархии (от политики информационной безопасности до детализованных инструкций по действиям персонала по обеспечению ИБ);
- сбор свидетельств подтверждения деятельности по обеспечению ИБ (акты и протоколы различных этапов при эксплуатации системы ИБ и ее контроля);
- подготовка отчетности по выполнению требований ИБ, состоянию ИБ и произошедших инцидентов.

Таким образом, локализуется проблема коммуникации между банковским бизнесом и подразделением ИБ, которое помимо бизнес-задач также должно решать задачу по приведению обеспечения информационной безопасности в соответствие с требованиями Банка России.

Область применения законодательства об НПС в отношении ИБ

Если провести анализ всей деятельности подразделения ИБ в банке на основании комплекса Стандартов Банка России «Обеспечение информационной безопасности банковской системы Российской Федерации», то можно выделить следующие этапы:

1. Анализ активов банковской организации, выделение информационных активов, их классификация в зависимости от значимости.

2. Выделение критичных информационных активов и ресурсов, формирование требований системы ИБ применительно к различным активам и ресурсам (в зависимости от типа информационного актива, используемых информационно-коммуникационных технологий, вовлеченности персонала и др.).
3. Выполнение требований за счет создания соответствующих внутренних нормативных документов, поставки и внедрения СЗИ, обучения персонала.
4. Контроль достаточности выполненных организационных и технических мер защиты информации при эксплуатации информационных ресурсов и активов.
5. Выявление новых угроз ИБ, уязвимостей в составе действующей системы информационной безопасности.
6. Совершенствование системы ИБ в части доработки документации, приобретения и внедрения дополнительных СЗИ, совершенствование системы менеджмента ИБ.

В настоящее время комплекс Стандартов информационной безопасности Банка России носит рекомендательный характер и может служить планом развития ИБ в банках.

Вместе с тем, с учетом экспоненциального роста рынка ДБО и использования платежных систем, в соответствии с Федеральным законом № 161-ФЗ «О национальной платежной системе», полный ряд требований к обеспечению защиты информации в банковских технологических процессах, реализуемых банками в рамках участия в платежных системах, является обязательным.

Набор требований к обеспечению защиты информации установлен в Положении Банка России № 382-П «Положение о требованиях к обеспечению защиты информации при переводах денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при переводах денежных средств». В сравнительном анализе между требованиями, изложенными в стандарте Банка России СТО БР ИББС 1.0 и Положении № 382-П, следует отметить, что требования к защите информации унаследованы из требований Стандарта, но имеют следующие особенности:

1. Требования к системе ИБ в рамках СТО определены как требования к защите информации в Положении, то есть произошло смещение от термина «информационная безопасность» к термину «защита информации».
2. Исключены из области действия Положения требования к обеспечению банковских платежных технологических процессов и банковских информационных технологических процессов, так как роли участников, их функции и действия уже определены как область регулирования взаимоотношений участников платежных систем.
3. Явно выражено разделение на организационные и технические меры защиты информации при переводах денежных средств, причем отдельные требования к техническим мерам однозначно закреплены в Положении исходя из консолидации лучших практик ведущих банков РФ.
4. В Положении № 382-П сокращен объем требований, предъявляемых к системе менеджмента ИБ согласно СТО БР ИББС 1.0. Оставлены только те группы, которые связаны с защитой информации при переводах денежных средств, повышением осведомленности, выявлением инцидентов и реагированием на них, оценкой выполнения требований к защите информации, совершенствованием защиты информации при переводах денежных средств.
5. Выделена отдельная группа требований по доведению операторами по переводу денежных средств и другими участниками платежных систем информации об обеспечении в платежной системе защиты информации.

Таким образом, стоит отметить, что между требованиями стандарта СТО БР ИББС 1.0 и требованиями Положения № 382-П есть много общего. Если в банке велась работа по приведению системы защиты информации в соответствие требованиям СТО БР ИББС 1.0, то полученные в ходе данной работы материалы также в почти полной мере выполняют требования Положения.

Также действует и обратное — приведение системы ИБ банка в соответствие требованиям по защите информации согласно Положению Банка России № 382-П обеспечит выполнение существенной части требований по Стандарту.

Поэтому для банка не является существенным, с какой стороны подойти к вопросу приведения в соответствие СОИБ — выполнением требований СТО БР ИББС 1.0 или требований Положения № 382-П, — полученный результат будет соответствовать лучшим практикам обеспечения ИБ в банковской сфере.

Реализация требований по обеспечению ИБ согласно Положению Банка России № 382-П

Классической моделью организации процессов управления в соответствии с ГОСТ Р ИСО 9001 и ISO/IEC IS 27001 2005 является циклическая модель Деминга, построенная по принципу «… — планирование — реализация — проверка — совершенствование — планирование — …». Данная модель была также положена в основу реализации системы менеджмента ИБ в стандарте СТО БР ИББС 1.0. С

учетом родственности требований СТО БР ИББС 1.0 и Положения № 382-П логичным будет применение цикличной модели Деминга к процессам управления защитой информации в банках.

Рассмотрим подробнее этапы модели Деминга:

1. Планирование. На данном этапе определяется область применения Положения № 382-П, то есть локализуются те бизнес-процессы, которые связаны с платежными системами. Определяются группы требований к обеспечению защиты информации, степень соответствия реализованных организационных и технических защитных мер. Осуществляется постановка задач к созданию/модернизации как системы ИБ, так и системы менеджмента ИБ.
2. Выполнение/реализация. Осуществляется поставка необходимых технических СЗИ, их настройка и ввод в эксплуатацию. Документально оформляются дополнительные организационные меры защиты информации (разработка нормативных документов). Оптимизируются существующие процессы по переводу денежных средств (с точки зрения назначения ролей, разграничения доступа к информации) и порядок обеспечения защиты информации при них.
3. Проверка. На этом этапе осуществляется мониторинг функционирования реализованных организационно-технических мер защиты информации и анализ эффективности как системы ИБ, так и системы менеджмента ИБ. Также осуществляется оценка соответствия требованиям в форме самооценки или внешнего аудита.
4. Совершенствование. Целью данного этапа является выработка корректирующих (превентивных) мер, направленных на повышение уровня защищенности бизнес-процессов банков в рамках участия в платежных системах, снижение вероятности возникновения ущерба и его масштабов в денежной форме, улучшение порядка обеспечения защиты информации при переводах денежных средств.

Процесс оптимизации защиты информации при переводах денежных средств является итерационным, и период повторения определяется:

- выявлением новых угроз и совершенствованием системы защиты информации за счет внедрения дополнительных мер защиты, как на основе изучения опыта других организаций, так и за счет реагирования на самостоятельно выявленные инциденты;
- проведением оценки соответствия требованиям к обеспечению защиты информации в соответствии с установленными Банком России в Положении 382-П сроками.

Системный интегратор — зачем и почему?

С учетом обозначенного объема работ, а также неоднородности требований, предъявляемых к штатным специалистам по ИБ, в условиях сжатых сроков перед руководством банка встает основной вопрос: как это все выполнить?

В общем виде можно выделить два подхода:

- осуществить приведение системы ИБ банка в соответствие требованиям Положения № 382-П силами штатных специалистов;
- привлечь для выполнения данной работы системного интегратора, специалисты которого обладают необходимым опытом работы и компетенциями.

Классический взгляд на системного интегратора как партнера по созданию систем базируется на том, что обычно он привлекается только в части из полного цикла работ по обеспечению ИБ — на этапе выполнения/реализации. Все остальные работы из модели Деминга, как правило, ложатся на плечи собственных специалистов.

Однако при внимательном изучении каждого из этапов выявляется факт, что взаимодействие между заказчиком и системным интегратором может выйти за рамки классического подхода, так как постепенное наращивание компетенций сотрудников интегратора может оказаться полезным для заказчика при реализации практически всех этапов.

Таким образом, системный интегратор в состоянии оказать полный спектр услуг по приведению кредитной организации в соответствие требованиям к обеспечению защиты информации согласно Положению № 382-П:

1. Сбор необходимой информации, анализ внутренних нормативных документов, сбор сведений и интервьюирование специалистов банка на местах.
2. Обработка и анализ собранных сведений, свидетельств выполнения требований Положения № 382-П.
3. Разработка рекомендаций по совершенствованию и приведению системы обеспечения информационной безопасности (СОИБ) в соответствие требованиям нормативных документов по защите информации в НПС.
4. Разработка и совершенствование существующей организационно-распорядительной документации.
5. Техническое проектирование системы ИБ.

6. Поставка и внедрение СЗИ, обеспечивающих техническую защиту при переводах денежных средств.
7. Проведение итоговой оценки соответствия выполнения требований к защите информации при переводах денежных средств (внешний аудит).
8. Повышение осведомленности по вопросам обеспечения ИБ при переводах денежных средств.
9. Сопровождение СОИБ, включая консультационную и техническую поддержку, инспекционные проверки.

Таким образом, для системного интегратора перестает быть определяющим исходный уровень состояния СОИБ банка. Включаясь на любом уровне соответствия — от начального, до полной готовности — системный интегратор может провести качественную оценку данного уровня и выполнить действительно необходимый заказчику объем работ, оптимизируя тем самым его затраты по обеспечению ИБ. В начальном уровне соответствия требованиям это может быть полный цикл работ. В случае полного соответствия — только проведение внешнего аудита с подготовкой отчетных форм для предоставления формы 0403202 в соответствии с требованиями Положения № 382-П и Указания Банка России № 2831-У.

Кроме того, стремясь максимально расширить объем предоставляемых ИБ-услуг, системный интегратор стремится привлечь наиболее профессионально подготовленный и разнородный по компетенциям и специализации персонал. Сотрудники системного интегратора могут выполнить на высокопрофессиональном уровне практически любую возникающую перед отделом ИБ задачу — начиная от услуг по разработке организационно-распорядительных документов и вплоть до обучения сотрудников заказчика навыкам обеспечения ИБ и защиты информации.

В итоге привлечение системного интегратора как исполнителя полного или частичного комплекса работ снижает нагрузку на специалистов отдела ИБ, оставляя время у них на выполнение своей основной задачи, — снижения рисков реализации угроз, направленных на несанкционированный доступ к банковской тайне и хищения денежных средств.

Приведение ИБ банка в соответствие требованиям законодательства — здесь и сейчас!

Выбор и привлечение системного интегратора основывается на следующих критериях:

- Объем оказываемых услуг по ИБ. Важно выбрать такого системного интегратора, который имеет в своем портфеле услуг полный комплекс работ. Ведь ничего не может быть хуже для заказчика, чем ситуация, когда после подписания договора оказывается, что исполнитель не в состоянии проделать весь необходимый объем или возникает объективная необходимость в проведении дополнительных, не учтенных ранее видов работ.
- Штат сотрудников и их профессиональная подготовка. Системный интегратор должен обладать не только квалифицированным персоналом, но и достаточным количеством сотрудников, чтобы выполнять работы в соответствии с установленным графиком.
- Наличие представительств в различных регионах РФ. Многие банковские организации имеют территориально-распределенную структуру, что требует от системного интегратора осуществлять производство работ на разных площадках. Как правило, командировочные затраты составляют заметную долю в бюджете проекта. И только наличие представительств системного интегратора на местах позволяет добиться экономии.
- Опыт реализации подобных проектов. Наличие опыта у системного интегратора гарантирует не только возможность выполнения объема заявленных работ, но и, что немаловажно, проведение их в установленный срок и с надлежащим качеством.

Как можно заметить, требования к системному интегратору предъявляются серьезные. На рынке ИБ остается не так уж много игроков, в полной мере удовлетворяющих таким требованиям. И одну из лидирующих позиций на этом рынке с полным основанием занимает компания Softline.

Softline существует на рынке 20 лет, является одним из крупнейших системных интеграторов в России и странах СНГ, обладает штатом квалифицированных специалистов и обширным опытом выполнения работ в области оценки состояния системы ИБ, разработки и реализации технических проектов систем обеспечения ИБ, поставки и внедрения СЗИ.

В заключение стоит отметить, что в июне 2013 года Банк России Указанием № 3007-У внес изменения в Положение № 382-П в части обязательности проведения оценки соответствия участников платежной системы требованиям к защите информации и установил срок проведения оценки соответствия — до 01.01.2014. Фактор времени начинает играть ключевую роль, и, выбирая компанию Softline своим системным интегратором, вы выбираете лучшую команду, способную решить любую задачу в части выполнения требований Положения Банка России № 382-П.

ЦОДы.РФ

специализированный журнал о ЦОД

БЕСПЛАТНАЯ ПОДПИСКА НА САЙТАХ

http://цоды.рф http://dcjournal.ru

Особенности издания:

- Чётко обозначенный фокус на рынок ЦОД
- Фотоэкскурсии в крупнейшие ЦОД
- Акцент на события российского рынка ЦОД
- Интервью с экспертами рынка
- Западный опыт строительства и инноваций в ЦОД
- Обзоры инженерных систем ЦОД
- Аналитические обзоры

MEDIA GRUS
media & marketing

По всем вопросам обращайтесь:
+7 (499) 638-21-81, info@mediagrus.ru
www.mediagrus.ru

Журнал «ЦОДы.РФ» зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовой коммуникаций 20 августа 2012 г., ПИ № ФС77-51010.

Тенденции в развитии UTM

Автор: Денис Гундорин, руководитель направления инфраструктурных решений ИБ, Департамент информационной безопасности Softline

Термин UTM (Unified Threat Management) — унифицированное управление угрозами — был введен исследовательской компанией IDC для обозначения многофункциональных сетевых устройств, являющихся многоуровневыми системами защиты и способных обезопасить сеть компании от самых различных видов угроз.

UTM включает в себя комплексный набор функций: межсетевое экранирование, антиспам, антивирус, систему предотвращения/обнаружения вторжений (IDS/IPS), контентную фильтрацию и средства для построения защищенных виртуальных частных сетей (VPN).

UTM-устройства обеспечивают защиту от широкого спектра угроз и представляют собой великолепную альтернативу традиционным узкоспециализированным решениям.

Бизнес-эффективность

Подавляющее большинство современных компаний ежедневно подвергается многочисленным угрозам, связанным со все большим проникновением всемирной сети Интернет в корпоративную сеть и внутренние бизнес-процессы. Желание упростить и облегчить доступ клиентам, партнерам и собственным сотрудникам к информационным ресурсам и системам неизбежно вступает в противоречие с необходимостью уменьшить риск несанкционированного доступа. Пренебрегающие первым рискуют проиграть конкурентную борьбу, а вторым — потерять ценную информацию и в перспективе, быть может, долю рынка или даже весь бизнес. Необходимость надежной и эффективной защиты от потенциальных угроз сегодня, пожалуй, уже никем не оспаривается, а вот способы и методы построения ее пока еще выбираются разные.

Классический подход предполагает использование набора разных решений для обеспечения защиты от разных угроз. Основным аргументом в его пользу служит тезис о том, что специализированный продукт лучше справляется со своей задачей, чем решение «все-в-одном» за счет более узкой направленности и ориентированности всех своих компонентов на конкретный аспект обеспечения безопасности. Однако с учетом нынешнего уровня развития технологий противопоставление качества и универсальности утратило свою актуальность.

Важно заметить, что технические свойства (производительность, надежность и т.д.) для продуктов информационной безопасности крайне важны, но не стоит забывать, что с точки зрения эффективности бизнеса любое внедряемое решение также должно как минимум соответствовать следующим требованиям:

- увеличение эффективности существующих ресурсов и инвестиций;
- уменьшение сложности инфраструктуры безопасности;
- снижение эксплуатационных и капитальных затрат.

Использование единой платформы комплексной безопасности как нельзя лучше соответствует данным требованиям, и, в частности, именно по этой причине UTM-устройства по праву завоевывают популярность среди все большего числа клиентов. Рассмотрим оба метода более детально.

Эволюция традиционного подхода

Для комплексной защиты сетей (рис. 1) первыми начали использоваться межсетевые экраны. Появляющиеся же со временем все новые и новые угрозы привели к необходимости существенного расширения спектра решений, обеспечивающих сетевую безопасность.

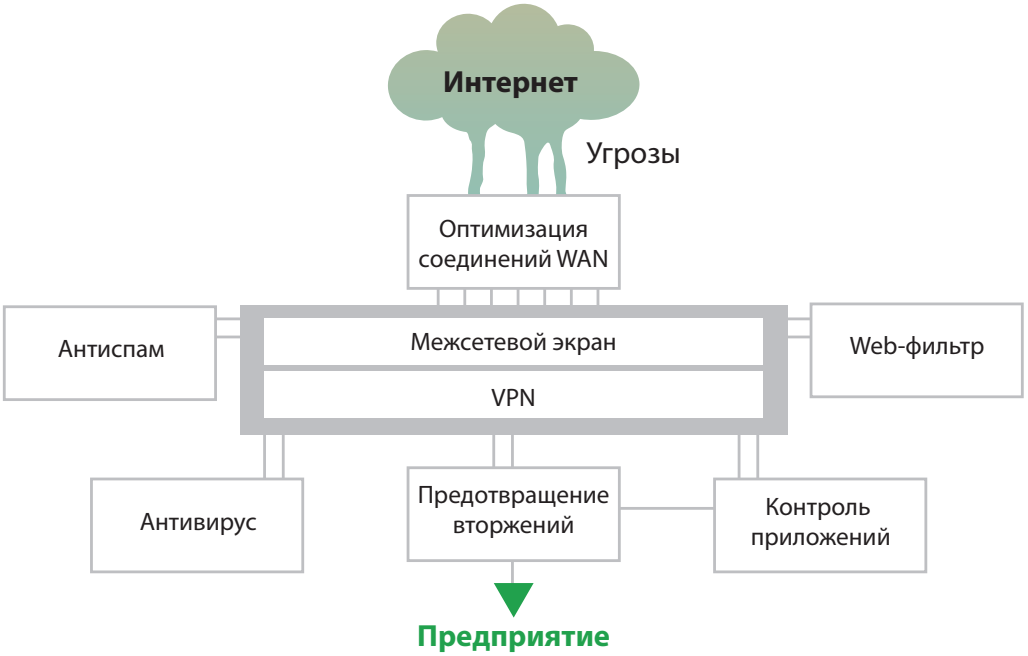
Так, для безопасного удаленного доступа потребовалось внедрение технологий виртуальных частных сетей (VPN), а совершенствование хакерских техник и рост сложности корпоративного программного обеспечения вынудило разработать принципиально новые методы защиты, такие как системы обнаружения вторжений.

Решения по борьбе со спамом и защиты от вирусов в настоящее время также активно используются на периметре сети организации, разгружая ресурсы рабочих станций и серверов и останавливая вредоносный код еще на границе корпоративной сети.

Усложнение содержимого html-кода веб-страниц, тенденция к повсеместному использованию интерактивности и применение скриптовых языков программирования вызвало необходимость внедрения веб-фильтров, которые теперь не столько блокируют доступ сотрудников к нежелательным сайтам, сколько активно защищают корпоративные сети от вторжений извне.

Ориентация большинства современных приложений на сетевое взаимодействие выявила потребность в контроле передаваемого

Рис.1 Традиционная схема защиты «по функциям»



ими контента, невидимого классическими средствами межсетевого экранирования.

Наконец, необходимость повышения надежности соединений и эффективности использования пропускной способности канала, напрямую связанная с повышением уровня доступности, побуждает компании к установке WAN-оптимизаторов.

На практике продукты для обеспечения информационной безопасности, помимо своего основного предназначения, как правило, имеют тот или иной дополнительный функционал. Встраивание элементов системы предотвращения/обнаружения вторжений в межсетевые экраны, контентный анализ с одновременной проверкой на наличие вредоносного кода, комплексная защита электронной почты от спама и вирусов — явления на сегодняшний день вполне обычные. Таким образом, построенная по традиционной схеме система безопасности зачастую имеет множество дублирующих компонентов, что, в частности, снижает быстродействие и увеличивает ее стоимость.

Можно выделить следующие характерные признаки традиционного подхода:

- использование автономных, не интегрированных между собой средств защиты;
- применение смеси из аппаратных (коробочных) решений и программных продуктов (приложений);
- высокая совокупная стоимость владения;
- сложность внедрения, управления и обслуживания;
- большие эксплуатационные затраты.

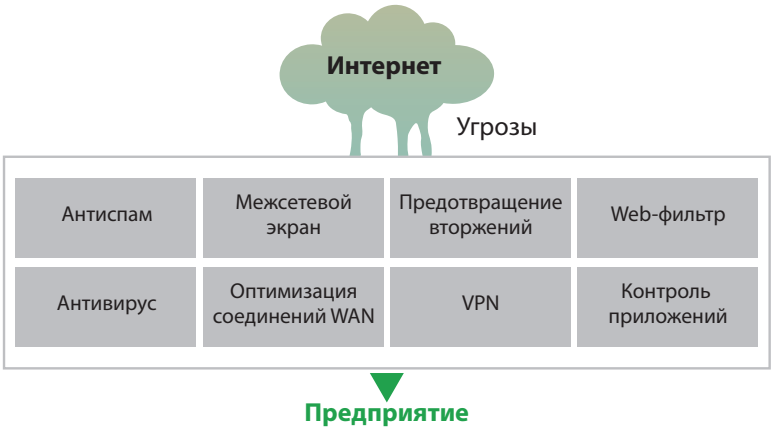
Тенденции развития и секрет успеха современных UTM-устройств

В противовес традиционному подходу производители UTM-решений предлагают использование единой комплексной платформы безопасности (рис. 2), объединяющей в себе все функции по обеспечению безопасности.

Вместо постоянного внедрения новых элементов системы защиты, призванных отвечать вновь возникающим угрозам и опасностям, применяется одно-единственное устройство, целиком осуществляющее всесторонний контроль и обеспечивающее безопасность сразу на всех уровнях.

Огромным экономическим плюсом такого подхода является снижение издержек на содержание парка различных устройств, для обслуживания которых требуется штат квалифицированных специалистов. Не секрет, что даже при несложной процедуре конфигурации самих устройств по отдельности основные проблемы внедрения и последующего использования решений от нескольких вендоров возникают как раз при настройке их взаимодействия между собой. Различная логика подхода производителей к построению систем управления, корреляции событий, анализу и отчетности еще больше затрудняет конфигурирование и требует от специалистов дополнительных знаний и практических навыков. Использование UTM-устройств снимает необходимость конфигурации взаимодействия различных компонентов защиты между собой, так как это уже сделано самим вендором, причем оптимальным образом. Столь тесная интеграция средств защиты между собой позволяет более эффективно бороться с угрозами, поскольку результаты проверок могут в полном объеме использоваться на последую-

Рис.2. Единая комплексная платформа безопасности



щих уровнях для достижения максимально глубокого анализа сетевого трафика. Таким образом, комбинация и корреляция подсистем, работающих на одном устройстве, существенно повышает общий уровень обеспечиваемой безопасности.

Ключевыми признаками данного подхода к построению системы безопасности являются:

- интегрированные сервисы безопасности;
- использование специализированных платформ и высокая общая производительность;
- низкая совокупная стоимость владения;
- простота внедрения, управления и эксплуатации.

Тенденция к расширению функционала классических устройств сетевой безопасности, о которой уже говорилось выше, достаточно ярко свидетельствует о том, что подход, предложенный производителями UTM-устройств, действительно эффективен.

Принципиально нужно отметить, что просто оснастить устройство дополнительными модулями или подсистемами, приближающими его к «чистокровным» UTM, недостаточно. Такая реализация будет иметь низкие показатели, как производительности, так и обеспечиваемого уровня безопасности. Для того чтобы решение было настоящим UTM, оно должно быть изначально спроектировано и построено как UTM.

Именно появление таких новых платформ и обусловливает текущую тенденцию к вытеснению целого «полка» отдельных специализированных устройств в инфраструктуре все увеличивающегося круга компаний.

Первые UTM-устройства, появившиеся на рынке, вызывали не очень лестные отзывы. С одной стороны, этому способствовали еще неотлаженные технологии, с другой — недостаточная мощность аппаратных платформ, применяемых в UTM и не способных с должной скоростью обрабатывать требуемый поток трафика в реальном времени. На сегодняшний день каждый производитель использует для решения этой проблемы свои уникальные запатентованные технологии: одни делают ставки на специально разработанные аппаратные платформы с применением оптимизированных на ускоренный анализ и обработку сигнатурного сетевого трафика процессоров (ASIC), вторые используют стандартные x86-процессоры, совместно со специализированной операционной системой, оптимизированной под специфические требования всего решения.

Наряду с термином UTM можно встретить такое понятие, как Next Generation Firewall (NGFW – межсетевые экраны нового поколения), используемое, в частности, компанией Gartner. По своей сути NGFW являются логическим продолжением UTM-устройств, так как обычно предоставляют еще более расширенный набор функций, хотя независимые исследователи пока считают появление класса Next Generation Firewall неким маркетинговым шагом, направленным на популяризацию UTM-систем.

Помимо уже упоминавшихся выше классических средств защиты (межсетевой экран, VPN, IPS–IDS, веб-фильтрация и пр.) UTM- и NGFW-устройства лидеров рынка предлагают все больше и больше дополнительных функций, реализуемых на базе единого устройства: предотвращение утечек информации, контроль и управление уязвимостями, анализ шифрованного SSL-трафика, контроль подключений, безопасность беспроводных сетей и многое другое.

Лидеры-производители

Если рассмотреть рынок UTM и NGFW-устройств сегодня, то лидерами, согласно маркетинговым исследованиям, являются такие компании, как Fortinet и Check Point, но технологически вперед выходят компании, делающие ставку на собственные разработки, а не отталкивающиеся от построения на уровне приложений встроенной операционной системы UTM-устройств. В качестве примера можно привести устройства компании NETASQ, разрабатываемые с учетом встроенной системы предотвращения вторжений в реальном времени на основе контекстного анализа протоколов (включая специализированные протоколы технологических сетей АСУТП/SCADA). В отличие от множества UTM-устройств предыдущего поколения используется не только сигнатурный, но и поведенческий анализ трафика, заложенного на уровне ядра самой системы. Это дает свои результаты — предотвращение вторжений и DDoS-атак происходит в реальном времени, а производительность UTM-устройств NETASQ будет одинаковой вне зависимости от включения/выключения IPS-устройства.

Значительную роль в UTM-устройствах имеет встроенное программное обеспечение, обеспечивающее антивирусную защиту на уровне сетевого трафика. Ряд компаний использует ПО собственной разработки, остальные предпочитают привлекать к разработке и встраиванию уже существующие антивирусные движки сторонних компаний, в первую очередь антивирусы с открытым исходным кодом (например, ClamAV), к сожалению, имеющие не очень большой уровень детектирования атак — на уровне 6-80%. Лидером можно назвать встроенный в NETASQ Антивирус Касперского, который детектирует более 97% атак.

Дополнительный функционал

Им обладают пока лишь отдельные NGFW-решения: контроль приложений и сканер уязвимостей, работающий на их уровне. В основе этого функционала лежит принцип аудита трафика и обнаружения уязвимостей в среде активных сетевых элементов. Технология NETASQ Vulnerability Manager определяет уязвимости в приложениях и дает рекомендации по их устранению, в отличие от других UTM-устройств, где требуется установка отдельного сканера или использование нескольких решений одного производителя (например, UTM FortiGate + сканер FortiScan), что возвращает нас к традиционному подходу, и, следовательно, увеличению капиталовложений.

Особенности настройки WAF

О системах защиты дистанционного банковского обслуживания (ДБО), представленных на современном рынке информационной безопасности, рассказывает Денис Гундорин, руководитель направления инфраструктурных решений ИБ, Департамент информационной безопасности Softline.

Лучшая защита ДБО возможна только в том случае, если на этапе разработки уделить особое внимание безопасности конечной системы и применить подходы безопасного программирования, анализа кода и встраивать средства внутренней безопасности в приложение.

Но, как показывает практика, безопасность при разработке не ставится в приоритет, а остается на втором плане. Поэтому на этапе внедрения проводятся работы по анализу защищенности и независимый анализ кода, если таковой возможен. Кроме того, применяют наложенные средства предотвращения атак, такие как потоковое выявление, средства контроля целостности программной среды и файлов.

IPS и WAF

Существуют два наложенных средства непрерывной защиты от атак:

- IPS (Intrusion Prevention System) — система предотвращения вторжений, которая умеет анализировать аномалии прикладного уровня, но «знание» уязвимостей веб-приложений сильно ограничено;
- WAF (WEB application Firewall) — специализированные средства для защиты от атак на прикладном уровне, куда входят сигнатурный анализ; система полномочного разграничения доступа; динамическое профилирование; защита от автоматизированных атак (Automated Attack), в рамках которой обнаруживаются внешняя инвентаризация, перебор, фазинг; корреляция с системами защиты БД.

Для чего необходима настройка WAF?

В первую очередь необходимо понять, почему вообще возникает потребность в настройке WAF. Интернет-банк представляет собой веб-приложение. Из опыта проведения анализа защищенности и тестов на проникновение в системы ДБО компанией Softline совместно с группой безопасности SolidLab видно, что все системы ДБО (как готовые продукты, так и продукты собственной разработки) содержат критические уязвимости. Они могут быть выявлены хакерами и использованы в собственных корыстных целях, что, несомненно, подрывает информационную безопасность любой организации.

Но действительно ли наличие WAF гарантирует компании полную защищенность?

Основная проблема как раз состоит в том, что WAF может создать в компании ложное ощущение уверенности. Средняя эффективность по всем решениям при стандартных настройках составляет 79%, и это для типичных атак автоматизированных средств. Сегодня одним из наиболее обсуждаемых вопросов в «хакерской среде» является разработка методов обхода WAF, представлены приемы обхода для каждой стадии работы средства. Это значит, что при «ручной атаке» система WAF не проявит себя и не сможет предупредить персонал о инциденте.

Защита системы ДБО и повышение уровня ИБ

Специалисты компании Softline совместно с группой безопасности SolidLab в случае, если у организации еще нет специализированных средств для защиты от атак на прикладном уровне, считают необходимым консалтинг на этапе выбора решения. Однако если WAF уже внедрен или компания уже определилась с внедряемым решением, то важно провести консалтинговые работы по профессиональной настройке решения.

Существует определенный алгоритм проведения работ по донастройке внедренного решения. В первую очередь проводится анализ используемых веб-приложений с выявлением уязвимостей. Затем настраиваются политики WAF в соответствии с текущей ситуацией. Обязательно добавляются правила по блокировке уязвимостей, найденных при анализе, и правила, затрудняющие обход системы WAF. Специалисты компании Softline совместно с группой безопасности SolidLab дают рекомендации по настройке системы мониторинга системы WAF для своевременного предупреждения о проводящийся атаке. На заключительном этапе проводится финальный тест на проникновение систем заказчика с включенной и донастроенной системой WAF для гарантии ее полной работоспособности. В результате всех выполненных этапов работ по донастройке внедренного решения при автоматизированной атаке существенно повышается защищенность целевых систем, а при ручной атаке — обеспечивается своевременное оповещение персонала об инциденте и предоставляется возможность за счет увеличенного времени на обход WAF злоумышленником принять необходимые противодействия.

Безопасность технологических сетей промышленных предприятий

Изначально офисные сети и сети АСУТП представляли собой две разные, не связанные между собой области — по сути, две различные планеты, с разными технологиями и даже разной терминологией. Технологические сети были отделены от сетей офисных, занимались ими другие люди, зачастую не имеющие IT-образования.

Автор: Вячеслав Железняков, руководитель Департамента информационной безопасности Softline

Более того, если IT-ландшафт меняется в среднем 1 раз в 5 лет, то ландшафт АСУТП — в 4 раза реже. Поэтому информационные технологии, применяемые в АСУТП, сильно отставали от IT-индустрии в целом.

Сейчас в области АСУТП наступило время перемен.

Кому это нужно?

Каким организациям необходимо задуматься о безопасности технологических систем? В России сейчас бытует мнение, и во многом оно сформировано информационной и законодательной политикой государства, что безопасность технологических сетей — это проблема крупных производственных предприятий из отраслей энергетики, химической промышленности, машиностроения, транспорта и ТЭК.

Однако не стоит думать, что проблема не касается других отраслей или предприятий меньшего масштаба. Здесь в случае сбоя технологического процесса катастрофических последствий не возникнет, однако финансовые потери для бизнеса будут очень ощутимыми.

Курс на создание единой системы управления предприятием

В отличие от промышленных объектов СССР, которые в огромных объемах десятилетиями производили одну и ту же номенклатуру продукции, современные предприятия, чтобы оставаться конкурентоспособными, должны очень гибко реагировать на изменение рыночных условий в случае необходимости быстро изменяя ассортимент и объем выпукаемых изделий.

На практике это означает интеграцию офисных информационных систем (BI, ERP, CRM) с системами технологическими в единую информационную систему управления предприятием, появление такого класса систем, как MES (Manufacturing Execution System), которые осуществляют централизованное управление производственным процессом в режиме реального времени.

Таким образом, системы становятся все сложнее, а офисная сеть уже не так надежно отделенной от сети АСУТП.

Современные информационные технологии в АСУТП

Технологические системы становятся все больше похожими на офисные — высокопроизводительные, гибко настраиваемые, обновляемые, территориально распределенные.

Усложнение технологических систем и систем управления производством вынуждает производителей оборудования и ПО искать пути для снижения издержек при разработке. Поэтому вместо собственных компонентов и протоколов используются известные ОС, СУБД, средства связи, библиотеки и протоколы. Технологов уже не удивляют программируемые контроллеры под управлением Windows CE, промышленные хранилища данных (Data historian), традиционные протоколы TCP/UDP при передаче данных…

Все это приводит к тому, что для технологических сетей современных предприятий становятся актуальны те же самые угрозы, что и для офисных сетей: вирусные заражения, DOS-атаки, ошибки конфигурации и т.п.

При этом последствия реализации таких угроз в случае технологических систем могут быть очень значительными или даже катастрофическими — от остановки производства до нарушения экологии и влияния на жизнь здоровье людей.

Человеческий фактор

Системы АСУТП становятся все более и более сложными, а знания персонала, с ними работающего, в вопросах информационной безопасности, как правило, даже ниже, чем у IT-специалистов, обслуживающих офисные сети.

Например, часто встречается ситуация, когда перенос или обновление технологических карт осуществляется инженерами-технологами с помощью обычных USB-накопителей, содержимое которых никак не контролируется. К чему это может привести, особенно в условиях ограничений АСУТП по антивирусной защите, нет необходимости объяснять дополнительно. АРМ, входящие в состава SCADA-систем (диспетчерских), используются персоналом для круглосуточного наблюдения за технологическим процессом, а зачастую — и в личных целях, для игр, просмотра фильмов и т.п. Причем контент опять-таки переносится с помощью USB-носителей.

Отдельный спектр задач безопасности приходится решать, когда требуется организовать удаленный доступ к системам АСУТП внутренних и внешних специалистов, для мониторинга, проведения профилактических работ, установки обновлений, переконфигурированию и пр. Разработчики или поставщики систем АСУТП, как правило, имеют такой доступ для того, чтобы сэкономить ресурсы и иметь возможность быстро отреагировать на сбой в технологическом процессе. С другой стороны, это означает потенциальную доступность сети АСУТП из Интернета и допуск к ней лиц, которые не являются полностью доверенными.

Stuxnet, Ducu и другие

Шум вокруг обнаружения вируса Stuxnet на иранских ядерных объектах в 2010 году и последующее выявление вредоносного кода аналогичного назначения (Ducu, Flame, Gauss) обозначили еще одну проблему, связанную с возможностью реализации атак типа Advanced Persistent Threat (APT) в отношении стратегически важных объектов информационной инфраструктуры.

Эти угрозы могут быть реализованы хорошо подготовленными хакерскими

группами по заказу террористических организаций или даже государств в отношении предприятий стратегически важных отраслей, влияющих на национальную безопасность, — атомной промышленности, энергетики, транспорта и т.п. Таким предприятиям необходимо (как описано ниже, это требуется и с точки зрения законодательства) целенаправленно заниматься защитой от APT.

Механизм реализации таких угроз уже достаточно хорошо изучен — в его основе знание злоумышленниками так называемых «уязвимостей нулевого дня», которые не детектируются средствами защиты и могут быть использованы для доставки вредоносного кода в информационные системы заказчика.

Для того чтобы завладеть информацией о подобных уязвимостях, потенциальному злоумышленнику нужно обладать высочайшей квалификацией или очень солидным бюджетом. Однако, технологии, которые сейчас знакомы только спецслужбам, через некоторое время станут доступны более широкому кругу злоумышленников (и свидетельства этому уже есть). Поэтому даже если предприятие не имеет стратегического значения для государственной безопасности, уже сейчас имеет смысл задуматься о защите против направленных угроз — чтобы защитить бизнес.

Требования и лучшие практики

В связи описанными тенденциями как за рубежом, так и у нас в стране этой теме уделяется повышенное внимание со стороны государства и экспертного сообщества. За рубежом, где проблема возникла несколько раньше, уже достаточно давно существуют и активно развиваются несколько стандартов, касающихся безопасности АСУТП. Наиболее известные — ANSI/ISA–99 Security for Industrial Automation and Control Systems, IEC IEC/PAS 62443 Security for industrial process measurement and control — Network and system security standard, NIST 800-82 Guide to Industrial Control Systems (ICS) Security.

В Российской Федерации применяется несколько другой подход. Приказом Правительства определены критичные системы информационной инфраструктуры КСИИ. К этим системам относятся госсистемы, системы промышленных предприятий, ущерб от сбоев которых может нанести вред экологии, жизни и здоровью людей или госбезопасности.

Еще в 2007 году ФСТЭК РФ разработал ряд методических документов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, определяющих требования к безопасности КСИИ, модель угроз и т.п. Кроме того, в 2012 году приказом Президента РФ был утвержден документ «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации».

Этот документ определяет факторы, влияющие на формирование государственной политики в области обеспечения безопасности КВО, ее основные принципы, направления и этапы реализации. В нем предусмотрена разработка нормативно-правовой базы по вопросам защиты АСУТП в течение ближайших 3 лет.

Подход к защите АСУТП

Для формирования общего подхода к обеспечению информационной безопасности технологических систем предприятия, можно, например, обратиться к стандарту ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, в котором описан общий подход к планированию и внедрению системы обеспечения информационной безопасности технологических систем.

И при анализе этого документа можно убедиться, что общие принципы обеспечения информационной безопасности в АСУТП практически ничем не отличаются от подходов, применяемых для защиты традиционных информационных систем.

В соответствии с лучшими практиками в АСУТП должны эффективно работать те же самые механизмы контроля — политики информационной безопасности, обучение персонала, процессы управления рисками, инцидентами, правами доступа и т.п.

Отличие только в особенностях реализации и в уровне ответственности при их внедрении. Все действия в сетях АСУТП необходимо предпринимать очень аккуратно, обязательно согласовывая действия со всеми заинтересованными сторонами, из-за чего проекты по безопасности АСУТП, как правило, оказываются сложнее с организационной точки зрения, чем проекты в офисных сетях.

В большинстве случаев технологическая сеть — это область ответственности Службы главного инженера или Главного технолога. Это люди, с одной стороны, достаточно консервативные, с другой — обладающие глубокими техническими знаниями в своей области, но зачастую не разбирающиеся в информационной безопасности. Поэтому специалистам по информационной безопасности приходится находить с ними общий язык, осваивая по сути для себя новую область.

Основное требование при реализации проектов по защите АСУТП — минимальное влияние на производство.

Поэтому, например, при обеспечении безопасности уже работающего технологического процесса необходимо выбирать специализированные средства защиты, не встроенные непосредственно в технологическую цепочку и обладающие минимальными задержками при обработке данных.

Причем для внедрения и обслуживания таких средств необходимо выбирать подходящие технологические окна, например, когда производственная система становится на плановое обслуживание или ремонт.

Системы безопасности в АСУТП должны тщательно проектироваться и тестироваться квалифицированными специалистами. Соответствие разрабатываемой проектной документации требованиям ГОСТ в этом случае является важным требованием, обеспечивающим затем возможность нормальной эксплуатации системы защиты.

Применяемые решения

Существует широкий спектр специальных решений для защиты от современных угроз — промышленные межсетевые экраны и системы IDS/IPS, системы контроля целостности для серверов и рабочих станций, дата-диоды для гарантированного разделения офисной и технологической сети, средства для мониторинга действий сотрудников и подрядчиков в сетях АСУТП и многое другое.

К этим системам предъявляются особые требования:

- высокая надежность, промышленное исполнение для аппаратных средств защиты;
- низкие задержки при обработке информации, способность работать в режиме реального времени;
- ограниченные требования к ресурсам — производительности процессора, объему памяти, пропускной способности каналов связи (как правило, компоненты АСУТП строятся для выполнения конкретного набора задач и лишние ресурсы отсутствуют);
- поддержка устаревших операционных систем (для средств защиты, устанавливаемых на промышленные серверы и рабочие станции HMI human machine interface);
- поддержка специальных приложений и протоколов, применяемых в АСУТП;
- возможность обеспечивать высокий уровень защиты без необходимости частых обновлений, (т.к. каждое обновление может негативно повлиять на работу системы и поэтому требует тщательного тестирования).

Внедрение этих средств требует от исполнителей высокой квалификации и хороших знаний в области технологических сетей. Поэтому в большинстве случаев такие проекты реализуются с помощью внешних подрядчиков, обладающих необходимыми компетенциями и опытом.

Анализ защищенности: ищем грамотный подход

В отличие от тестов на проникновение, цель анализа защищенности — найти максимальное количество уязвимостей, выявить столько, сколько возможно в условиях ограничений согласованной с заказчиком модели нарушителя.

Авторы: Михаил Плахута, руководитель отдела развития Департамента информационной безопасности Softline;
Андрей Петухов, генеральный директор лаборатории безопасности SolidLab

Почему анализ защищенности необходим?

Рассмотрим ситуацию, когда в компании работает критичное online-приложение, которое порождает свою сложную экосистему, включающую, в том числе, разработчиков, пользователей, администраторов и т.д. Такого рода приложение может быть написано под конкретную организацию, разработано программистами in house, или на аутсорсинге по заказу самой организации. Кроме того, это может быть стандартное, кастомизированное решение.

Ввиду этого появляется целый ряд актуальных вопросов, которые остро стоят в экосистеме приложения. Если система по факту разрабатывалась нештатными сотрудниками, то нет достоверной информации о том, какие процедуры применялись при разработке, насколько безопасной она была. Нет гарантий, что разработчик провел аудит и осуществил поиск уязвимостей. В большинстве случаев даже не определены требования к безопасности, выдвигаемые при создании стандартного решения. Отдельно стоят вопросы, связанные с наличием недокументированного функционала. Даже если приложение разрабатывалось «домашней» командой, проблема недокументированного функционала остается актуальной.

Раз — и готово?

Найти все уязвимости в сложной экосистеме и незамедлительно закрыть их не представляется возможным по нескольким причинам. Во-первых, это очень дорого. Во-вторых, проект по поиску всех уязвимостей в экосистеме очень длительный и трудозатратный, особенно если не предъявлялись требования к безопасной разработке продукта.

Также стоит отметить, что для обнаружения разных классов недостатков необходимо использовать различные методы анализа. Например, найти закладку, оставленную нарушителем из категории «злонамеренный программист», невозможно, осуществив тестирование методом «черного ящика».

Именно поэтому для решения поставленной задачи приходится расставлять приоритеты и ставить более конкретные задачи. Неправильный подход к анализу защищенности такого приложения — это, фактически, выброшенные на ветер деньги.

Как найти правильный подход к анализу защищенности?

Для того чтобы грамотно поставить задачу, заказчик должен частично знать ее решение. Заказчику необходимо понимание, какие процессы ИБ требуют анализа защищенности.

Например, что нужно делать с отчетом? Какую обратную связь он должен оказать на процессы по SDLC (если у заказчика in house-разработка? Как должен повлиять на внешние процессы разработки (если мы имеем дело с заказным приложением), практики администрирования и эксплуатации приложения, планы по закупке и конфигурированию дополнительных корректирующих мер по мониторингу и т.п.

При заказе анализа защищенности сложного приложения есть некоторые подводные камни — типичные ошибки, которые заказчик может допустить. Предлагаю остановиться на них более подробно в разрезе повышения уровня зрелости отношения к ИБ.

1. Заказчик понимает необходимость обеспечения ИБ, но вместо анализа защищенности с целью выявления недостатков покупает пентест, который не обеспечивает полноту исследования системы.

2. Заказчик представляет, какими методами должны решаться поставленные задачи. Но он не осознает, что понятие «защищенность» существует только в отношении конкретного класса злоумышленников, определенной модели нарушителя. Т.е. приложение, защищенное от script-kiddy или от интернет-хулиганов может быть полностью незащищенным от заказного злоумышленника или совершенно не подготовленным к встрече с группировкой anonymous.

Говорить о защищенности можно только в привязке к конкретной модели угроз или нарушителю, так как провести анализ защищенности и обеспечить защиту от всех классов нарушителей с самого начала — это достаточно дорого, поэтому необходимо расставить приоритеты. Для этого необходимо знать, какие классы нарушителей наиболее опасны, и обеспечивать защищенность в первую очередь от них, а потом уже двигаться дальше.

3. Представим заказчика, который понимает классы нарушителей; модели угроз в отношении приложения у него прописаны. Но нет знаний о том, какая методика и какой метод поиска уязвимостей могут дать нужный результат (хороший или плохой) при рассмотрении различных классов нарушителей. Такие заказчики не могут быть уверены, что исполнитель будет искать уязвимости авторизации, а не только XSS и уязвимости, позволяющие проводить атаки на внедрение. У компании такого уровня зрелости есть риск нанять исполнителя, проведя конкурс по критерию сроки/время, и не получить на выходе полный список уязвимостей, который помог бы ему устранить или выбрать соответствующие корректирующие меры. Часто задачи решаются инструментальными средствами, а качество и полнота страдают.

Таким образом, самый зрелый заказчик — это тот, который понимает методы и методики проведения анализа защищенности и выбирает в конкурсе исполнителя не только по соотношению цена/сроки, но и по результатам проведения экспертной оценки методики работ.

Типичные ошибки

Существует ряд типичных ошибок, которые могут возникнуть при проведении работ и снизить их эффективность, а также сроки возврата инвестиций в проект.

- Критичное приложение рассматривается отдельно от экосистемы, когда при оценке пропадают связи этого приложения с другими компонентами экосистемы, в том числе и с людьми.
- Тестирование рассматривается как проект, а не элемент процесса. В этом случае вы получите отчет, исправите уязвимости, но не процессы, которые привели приложение в его состояние.
- Постановка цели и задач проекта по анализу защищенности происходит в отрыве от модели угроз и профилей нарушителя.
- При выборе подрядчика на проведение анализа не оценивается методика проведения работ.

Что должен учитывать заказчик при подготовке конкурсной документации?

Рассмотрим несколько наиболее важных вопросов, на которые исполнитель должен ответить при подготовке конкурсной документации. Будут проанализированы как правильные, так и неправильные ответы на каждый из поставленных вопросов.

1. Какая методика будет использована в проекте?

Правильный ответ:

- **перечисляются классы уязвимостей, которые будут устанавливаться в процессе анализа;**
- **для каждого класса приводится процедура поиска уязвимостей этого класса;**
- **описание правильной и полной методики НЕ может занимать меньше 2–3 страниц А4.**

В качестве примера можно привести анализ уязвимости авторизации, в котором используется подход по анализу отличий интерфейсов от привилегированного и непривилегированного пользователя, строится их разность и от непривилегированного пользователя делается попытка совершения действий привилегированного пользователя.

Неправильный ответ:

- описывается только подход (черный ящик, статический анализ, инструментальный анализ, сканирование, динамический анализ и т.п.);
- методика описывается очень негранулярно: например, приводится всего пара абзацев описания того, как устроено тестирование в общем случае (поиск точек ввода данных, передача вместе с данными некорректных значений, анализ ответного поведения приложения);
- в описании методики не рассматриваются классы уязвимостей.

2. Есть ли обоснование того, что данная методика позволит решить задачи проекта?

Правильный ответ:

При анализе сложных систем возможны следующие подходы к анализу объекта исследования:

- **анализ системы в продакшене методом черного ящика;**
- **анализ системы в тестовом окружении на площадях заказчика с наличием взаимодействия с back end-системами (не требуются заглушки) методом черного ящика;**
- **статический анализ исходного кода приложения;**
- **разворачивание приложения в своем тестовом окружении и проведение динамического анализа его, но без взаимодействия с бэкенд-системами (потому что приложение у себя развернуто).**

Для достижения цели может выбираться любая комбинация этих подходов.

Неправильный ответ:

Исполнитель не готов рассуждать на тему, какая комбинация подходов лучше для конкретного заказчика в данных конкретных условиях, а предлагает дефолтную методику.

3. Какое место в этой методике занимают инструменты?

Цель данного вопроса — убедиться, что анализ не сводится к применению какого-то одного или двух инструментов. В идеале, в ответе должны быть приведены классы анализируемых уязвимостей, и для каждого класса перечислены инструменты, которые используются для поиска соответствующих уязвимостей.

4. Наличие каких классов недостатков будет устанавливаться при анализе?

Правильный ответ:

Перечень из 20 пунктов — достаточно гранулярный список классов, который перекликается с известными списками типа OWASP Top 10, WASC Threat Classification v2, CWE и т.п.

Неправильный ответ:

«Мы ищем уязвимости проектирования, уязвимости эксплуатации и уязвимости разработки. При этом анализ покрывает все классы». Ответ недостаточно гранулярный, так как внутри каждого класса есть целое множество подклассов, которые не раскрыты в данном ответе.

5. Какие классы недостатков, открытых в последнее время, будут исследоваться в рамках проекта и каким образом?

Этот вопрос необходим для того, чтобы понять, следит ли исполнитель за конференциями, выступлениями, публикациями в своей области. Если исполнителю затруднительно привести примеры современных классов атак, это значит, что он либо использует отдельные инструменты, либо не следит за предметной областью.

Правильный ответ:

XXE (external XML entity), SSRF, DOM-based XSS, HTTP Parameter Pollution, Execution after redirect (EAR).

Межсетевые экраны: эволюция подхода к сетевой защите

Применение межсетевых экранов стало стандартом сетевой безопасности, без этого инструмента не обходится ни одна корпоративная сеть. Однако с массовым распространением технологий виртуализации и облачных сервисов, мобильных устройств и приложений обнаружить и вовремя отразить угрозы сетевой безопасности становится все сложнее. Для защиты современной корпоративной сети от межсетевого экрана требуется гораздо больше функций.

Постепенное наращивание функционала привело к появлению качественно новых классов устройств. Современные Unified Threat Management (UTM) и Next Generation Firewall (NGFW) совмещают в себе функции межсетевого экранирования, возможность организации защищенного VPN-соединения, функциональность веб-фильтрации и контроля приложений, функции IPS/IDS и DLP-систем, имеют встроенные антивирусные движки и т. д. Зарубежные производители уже предлагают подобные устройства, сочетающие широкий функционал и способные обеспечить надежную комплексную защиту сети. На российском рынке первые шаги в этом направлении делает компания «Код Безопасности», которая в сентябре этого года выпустила новую версию своего флагмана АПКШ «Континент» 3.7 — программно-аппаратную платформу, сочетающую функции VPN-шлюза, межсетевого экрана и средства обнаружения вторжений.

Новая версия АПКШ «Континент»

Продукт значительно усовершенствован в технологическом плане. Реализована поддержка современного протокола IPv6, который все чаще используется для организации сети провайдеров, а также усилены механизмы межсетевого экранирования, что позволило выполнить требования ФСТЭК России к межсетевым экранам 2-го класса защищенности.

В состав новой версии «Континент» включена система обнаружения вторжений (СОВ), выполняющая функции автоматического обнаружения сетевых атак за счет динамического анализа трафика стека протоколов TCP/IP. В СОВ «Континент» применяются как сигнатурные (с коммерческими сигнатурами атак ETPro™ от Emerging Threats), так и эвристические методы обнаружения вторжений собственной разработки «Кода Безопасности», за счет чего обеспечивается гарантированная реакция на актуальные сетевые угрозы и низкий уровень ложных срабатываний. СОВ «Континент» работает на специализированной аппаратной платформе с предварительно установленным программным компонентом детектора атак. Управление и контроль функционирования системы осуществляется централизованно при помощи Центра управления сетью (ЦУС) «Континент».

Новую версию АПКШ «Континент» также отличает применение уникальной программно-аппаратной технологии ускорения криптографических операций, благодаря которой максимальная производительность криптографической обработки трафика достигает 3 Гбит/с (на платформе «Континент» IPC-3000F в режиме FW/VPN). Кроме этого, добавлена функция поддержки балансирующего кластера, позволяющего распределять шифрованный трафик внутри фермы криптошлюзов для достижения производительности свыше 10 Гб/с.

Аппаратная платформа «Континент IPC-10»

В модельном ряде АПКШ «Континент» появилась новая аппаратная платформа «Континент IPC-10», которая отличается компактными размерами и низким энергопотреблением и может применяться для комплексной защиты сети банкоматов и платежных терминалов. Криптошлюз «Континент IPC-10» поддерживает работу с внешним 3G-USB-модемом, что позволяет организовать подключение банкоматов как с применением традиционной проводной связи, так и через 3G-сети мобильных операторов.

Новая версия АПКШ «Континент» также отличается повышенным удобством эксплуатации и гибкостью управления и настройки. В версии 3.7 реализована возможность организации защищенного взаимодействия (VPN) между разными криптографическими сетями, принадлежащими разным организациям, возможно установление доверительных отношений между сетями и создание VPN-связей между криптошлюзами разных сетей из программы управления ЦУС. Расширены возможности управления политиками для групп криптошлюзов, возможен перевод сети в изолированный режим работы, который позволяет исключить попадание во внешние сети трафика в открытом виде.

Дополнительные преимущества

Новая версия АПКШ «Континент» 3.7 соответствует требованиям ФСТЭК России, предъявляемым к межсетевым экранам и системам обнаружения вторжений (СОВ), что подтверждается сертификатами соответствия по 2-му уровню контроля на отсутствие НДВ, 2-му классу защищенности для межсетевых экранов и 3-му классу защиты для СОВ. В настоящее время «Континент» 3.7 находится на сертификации в ФСБ России на соответствие требованиям, предъявляемым к средствам криптографической защиты информации класса КС3 и к устройствам типа межсетевой экран 4-го класса защищенности.

АПКШ «Континент» 3.7 с функциями СОВ — это демонстрация того, как эволюционируют отечественные системы сетевой защиты, чтобы противостоять новым угрозам. Применение таких комплексов, как АПКШ «Континент», позволит построить безопасную и надежную корпоративную сеть, обеспечивающую защищенное взаимодействие с удаленными филиалами и мобильными сотрудниками без потери производительности и удобства эксплуатации системы.

Модельный ряд СОВ «Континент»

	СОВ Континент IPC-100	СОВ Континент IPC-1000	СОВ Континент IPC-1000F
Форм-фактор	1U 19"	2U rack	2U rack
Максимальное кол-во анализирующих интерфейсов	2	3	3
Производительность анализа трафика на один интерфейс (сенсор) без эвристики	130 Мбит/с	200 Мбит/с	200 Мбит/с
Производительность анализа трафика на один интерфейс (сенсор) с эвристикой	105 Мбит/с	170 Мбит/с	170 Мбит/с
Совокупная производительность	260 Мбит/с	600 Мбит/с	600 Мбит/с

отель «Москва»
пл. Александра Невского, д. 2

7-8 НОЯБРЯ / 2013
САНКТ-ПЕТЕРБУРГ

INFOSTART 2013 EVENT REVOLUTION

III всероссийская профессиональная конференция

«Управление и технологии автоматизации учета на платформе 1С:Предприятие»

– **2** дня, **6** тематических секций, **30** докладчиков, **48** часов бесценных знаний;
– Онлайн-трансляция и видеозаписи со всех залов;
– Вечеринка в историческом месте Петербурга, в клубе **Rossi`s**.

Доклады конференции **INFOSTART EVENT REVOLUTION 2013** пройдут в рамках тематических секций:

– Платформа 8.3 + Облачные технологии;
– Организация командной работы (системы класса HelpDesk, стандарты ITIL);
– Отраслевой опыт (Производство);
– Практика внедрения учетных систем;
– Мобильная платформа + интеграция;
– Отраслевой опыт (Владение и встраивание).

Ждем вас! Такое пропускать нельзя,
это будет революция вашего сознания!
Подробнее: event.infostart.ru/november2013

Softline защитила IT-инфраструктуру «Уралмаш НГО Холдинг» с помощью решений «Лаборатории Касперского»

Softline осуществила поставку лицензий Kaspersky Total Security для компании «Уралмаш НГО Холдинг». Комплексное решение «Лаборатории Касперского» предоставило многоуровневую защиту корпоративной сети машиностроительной компании, предотвратило всевозможные риски для IT-безопасности, а также позволило значительно сократить издержки на защиту.

Ситуация

Перед IT-руководством компании стояла задача подбора антивирусного решения, способного обеспечивать не только надежную защиту всех узлов распределенной сети (пять городов, 1200 компьютеров), но и производить аудит рабочих устройств и установленного на них программного обеспечения. В итоге было принято решение об использовании продуктов «Лаборатории Касперского».

Решение

Kaspersky Total Security представляет собой универсальное средство многоуровневой защиты корпоративных сетей крупных компаний. Наряду с обеспечением безопасности файловых серверов, портативных устройств и рабочих станций, решение содержит технологии шифрования, гибкие инструменты контроля производительности труда и администрирования систем. Система защищает почтовые серверы, серверы совместной работы и трафик, проходящий через интернет-шлюзы.

Проект

В качестве поставщика программного обеспечения была выбрана компания Softline, имеющая двадцатилетний успешный опыт работы на рынке IT и обладающая наивысшим партнерским статусом Kaspersky Enterprise Partner, подтверждающим высокий уровень ее компетенций. Специалисты компании обеспечили лицензирование антивирусных программ в максимально короткие сроки.

«Мы используем антивирусные продукты «Лаборатории Касперского» с 2006 года. Kaspersky Total Security отлично справляется с задачей по защите ПК и серверов от вирусов. Также мы используем в работе возможности аудита ПО и оборудования, — функциональность, которая стала доступной в последних версиях продукта», — отметил Владимир Меденников, начальник отдела коммуникаций и системного администрирования филиала ООО «Уралмаш НГО Холдинг» в Екатеринбурге.

«Бизнес-процессы современной компании становятся все более виртуализированными. Это делает бизнес уязвимым перед интернет-угрозами. В связи с этим руководители организаций стараются уделять больше внимания усиленной защите IT-инфраструктуры. Комплексные решения «Лаборатории Касперского» для защиты корпоративных сетей являются оптимальным средством для этих целей, — и с точки зрения необходимого функционала, и с точки зрения сертификации. Продукты соответствуют требованиям, предъявляемым государством к работе с конфиденциальными данными, и имеют необходимые сертификаты ФСБ РФ», — подчеркнул Алексей Бутаков, директор по развитию бизнеса компании Softline в Уральском ФО и Пермском крае.

О компании

ООО «Уралмаш Нефтегазовое Оборудование Холдинг» (ООО «Уралмаш НГО Холдинг») — крупнейшая в России машиностроительная компания по производству бурового оборудования. Возможности «Уралмаш НГО Холдинг» позволяют проектировать и производить буровые установки всех типов и оказывать полный комплекс сервисных услуг. Установки традиционно рассчитаны на эксплуатацию в наиболее экстремальных условиях и поэтому превосходят большинство мировых аналогов по своей надежности и долговечности при строительстве скважин в условиях Крайнего Севера.

О «Лаборатории Касперского»

«Лаборатория Касперского» — крупнейшая в мире частная компания, специализирующаяся в области разработки программных решений для обеспечения IT-безопасности. Компания входит в четверку ведущих мировых производителей защитных систем класса Endpoint Security*. Вот уже более шестнадцати лет «Лаборатория Касперского» предлагает эффективные защитные решения для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. Ключевым фактором успеха компании является инновационный подход к обеспечению информационной безопасности. Технологии и решения «Лаборатории Касперского» защищают более 300 миллионов пользователей почти в 200 странах и территориях мира. Более подробная информация доступна на официальном сайте www.kaspersky.ru.

*Компания заняла четвертое место в рейтинге аналитического агентства IDC «Выручка вендоров от продажи решений класса Endpoint Security» (Worldwide Endpoint Security Revenue by Vendor) за 2012 год. Рейтинг был включен в отчет IDC «Прогноз развития мирового рынка решений класса Endpoint Security на 2013–2017 гг. и доли вендоров в 2012 г.» (Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares), опубликованный в августе 2013 года (IDC #242618). В основу рейтинга легли данные о выручке от продаж решений класса Endpoint Security в 2012 году.

V Международный форум поставщиков атомной отрасли «АТОМЕКС–2013»

атомекс

2-4 ДЕКАБРЯ 2013 ГОДА

МОСКВА, ЦВК «ЭКСПОЦЕНТР»

РОСАТОМ

www.atomeks.ru

атомэкспо

КУБ инновационное решение для комплексного управления информационной безопасностью

КУБ (Комплексное Управление Безопасностью) — уникальное кроссфункциональное решение для управления логическим и сетевым доступом к информационным ресурсам компании и контроля соблюдения ее политики безопасности. Система является разработкой компании «ТрастВерс», входящей в группу «Информзащита», — единственного в России холдинга, специализирующегося в области информационной безопасности

КУБ — это единый продукт, объединяющий в себе следующие возможности: построение ролевой модели, документооборот заявок, автоматизированное управление учетными записями и правами доступа, мониторинг соответствия выданных и запрошенных прав и др.

Эффективный инструмент службы информационной безопасности. Система позволяет максимально снизить риски ошибочно предоставленного доступа за счет грамотного разграничения прав пользователей. Любые изменения в системах происходят только на основании заявок, которые согласовываются в соответствии с политикой ИБ предприятия. Наличие динамических маршрутов согласования заявок на доступ отличает КУБ от представленных на рынке IDM. КУБ контролирует исполнение заявок и осуществляет непрерывный мониторинг соответствия запрошенных и фактических изменений прав доступа.

Присутствуют средства для автоматизации задач первоначальной настройки и анализа текущих прав доступа. Есть средства контроля корректности настройки системы, выдающие перечень недостатков и несоответствий рекомендуемым правилам, а также инструменты для автоматического построения ролевой модели.

КУБ предоставляет возможности автоматического и ручного исполнения заявок. Политика безопасности некоторых предприятий запрещает автоматическое внесение изменений в информационные системы. После согласования заявки на доступ КУБ генерирует инструкции, которые определяют, какие изменения должны произойти в информационных системах. Эти инструкции могут быть исполнены автоматически или вручную. КУБ транслирует используемую бизнес-пользователями терминологию в понятные исполнителю инструкции с указаниями корректных названий и адресов ресурсов, что исключает любую двойственность и снижает риск возникновения ошибок, связанных с человеческим фактором.

Хранение полной истории всех изменений прав доступа. КУБ фиксирует все несанкционированные действия, оповещая при этом уполномоченных лиц, и хранит полную историю всех изменений прав доступа, что дает широкие возможности для оперативного расследования инцидентов, связанных с нарушением политики ИБ. С КУБ всегда можно быстро установить, кто, когда и на каком основании выдал пользователю определенные права.

Управление сетевым доступом и средствами защиты информации. Во многих организациях сетевым доступом и доступом к информационным системам управляют разные специалисты. КУБ синхронизирует эти процессы.

Управление ПАК. В КУБ содержатся сведения о конфигурации компьютеров и установленном на них ПО. Если сотруднику необходимы дополнительные программы, он отправляет в КУБ заявку, которая согласовывается и исполняется подобно заявкам на доступ.

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.

Тираж: 20 000
Объем – до 100 полос

Контроль почтовой переписки сотрудников

Неумолимая статистика говорит, что более 50% сотрудников регулярно пересылают рабочие документы с офисной на персональную электронную почту. Учитывая, что сегодня электронная почта является основным способом связи для организаций любого масштаба, а популярность различных почтовых веб-сервисов достигла уровня, когда у каждого пользователя интернета есть по меньшей мере один собственный почтовый ящик — со стороны служб ИБ игнорировать статистику и доступность почты будет преступной халатностью.

DeviceLock®
Proactive Endpoint Security

Какие задачи следует при этом ставить перед выбираемым техническим решением? Полнофункциональное DLP-решение, выполняющее среди прочих задач функцию защиты электронной почты от утечек корпоративных данных, должно поддерживать контроль не только наиболее распространенных протоколов, используемых в почтовых системах предприятий и организаций, но и контролировать доступ сотрудников к популярным почтовым web-сервисам, используемым ими для личной переписки. При этом эффективность политик контроля определяется как возможностью проверки содержания почтовых сообщений и их вложений на наличие запрещенной к передаче информации, так и гибкостью в вопросе задания разрешенных и запрещенных типов вложений, ограничения коммуникаций по времени, избирательного применения политик к различным группам пользователей и т.д. Кроме того, исключительно важна полнота защитных реакций системы контроля на выявленные нарушения — имеем в виду блокировку отправки письма, детальное протоколирование действий пользователей, включая сохранение точных копий передаваемых писем и вложений, а также оперативное оповещение сотрудников службы ИБ организации о критически важных событиях.

В распространенных сегодня вариантах реализации DLP-системы контроля почты на базе сетевых серверов или шлюзов практически невозможно реализовать целый ряд требуемых задач, в том числе задачи управления доступа сотрудников к почтовым веб-сервисам, а также контроля использования почты в «мобильном» режиме за пределами офиса. Кроме того, для инспекции почтового трафика, защищенного SSL-криптотуннелями, такие сетевые решения требуют интеграции с отдельными прокси-системами, способными перехватить и дешифровать пересылаемые по сети данные. Единственно возможным техническим решением без перечисленных критических функциональных недостатков является использование DLP-агентов, устанавливаемых на защищаемых настольных и портативных компьютерах сотрудников и перехватывающих почтовый трафик непосредственно на его источнике.

DeviceLock Endpoint DLP Suite

Всем перечисленным выше требованиям к DLP-системе в полной мере отвечает российский программный комплекс DeviceLock Endpoint DLP Suite, агенты которого работают непосредственно на защищаемых компьютерах и обеспечивают инспекцию и протоколирование корпоративной почты и других коммуникационных приложений независимо от используемых ими портов и способа выхода в Интернет.

Принципиальным преимуществом такой архитектуры является реализация защитных действий по блокировке и протоколированию почтовых отправлений в момент отправки данных по сети «на лету» непосредственно на рабочем компьютере сотрудника — будь то полноценная рабочая станция, мобильный лэптоп или даже удаленное BYOD-устройство в терминальной среде на базе продуктов Microsoft, Citrix или VMware. В результате работоспособность DLP-системы DeviceLock в целом никак не зависит от доступности корпоративной сети или подключения к серверам, что позволяет службам ИБ обеспечить безопасность почтовых коммуникаций сотрудников даже в условиях, когда их бизнес-функции требуют мобильности.

Модуль NetworkLock

Реализованные в модуле NetworkLock технологии анализа сетевого трафика обеспечивает контроль как открытого, так и SSL-защищенного доступа к электронной почте по используемым в корпоративных ИС протоколам SMTP и MAPI (Microsoft Exchange), а также из любого браузера через популярные web-сервисы Gmail, Outlook.com/Hotmail, Mail.ru, Яндекс-почта и др. Встроенный в NetworkLock Белый список сетевых протоколов делает контроль почты максимально гибким.

Модуль ContentLock

Другой модуль комплекса, также функционирующий непосредственно на рабочих станциях — ContentLock — реализует технологии контентного анализа. Служба ИБ может инспектировать и фильтровать информационное содержание передаваемых сообщений и вложений, тип и свойства вложенных файлов и архивов. ContentLock позволяет разрешать или запрещать передачу данных, основываясь на целом ряде контентно-зависимых критериев — по типу файла, наличию ключевых слов и фраз, соответствию содержания шаблонам регулярных выражений, а также использовать комбинации численных порогов и логических условий для проверки соответствия содержимого почты заданным параметрам и образцам детектирования.

Анализ и контроль: весь необходимый инструментарий

Сочетание функционала компонентов NetworkLock и ContentLock в комплексе DeviceLock Endpoint DLP Suite дает службам ИБ весь необходимый инструментарий для избирательного контроля, аудита и анализа передачи конфиденциальной информации в различных типах электронной и web-почты, а также других популярных сетевых приложений. Технологические решения, предлагаемые DeviceLock для DLP-защиты обычных и виртуальных сред, позволяют как уменьшить информационные риски, так и обеспечить неукоснительное исполнения сотрудниками политик безопасности как внутри компании, так и за ее пределами.

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 2012	20460
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
ПОЛЯНА НОВИНКА Произведения современных писателей	84959
БИЗНЕС-АНАЛИТИКА: РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ НОВИНКА Разработка и применение средств обработки, анализа и визуализации данных	70078

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 2012	82855

Предлагаемые журналы распространяются по подписке и в розничную торговлю не поступают.

Интернет-подписка
www.ITbook.ru

Для справок
тел.: (495) 638-5-638,
e-mail: itj@mail.ru

Информационная безопасность в СМБ-компаниях

Автор: Елена Наумова, менеджер по продуктам компании InfoWatch

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

В настоящее время в отношении вопроса ИБ в СМБ-сегменте бытуют два противоположных мнения. Некоторые аналитики утверждают, что в небольших компаниях нет даже понятия ИБ, поскольку нет информации, представляющей настолько весомый для бизнеса актив, который требовал бы внедрения систем защиты. Другие считают, что с точки зрения информационной инфраструктуры каналов передачи и форматов данных предприятия СМБ фактически идентичны Enterprise-предприятиям — дело лишь в масштабе. Соответственно, подход к ИБ должен быть аналогичен.

Мнение об отсутствии весомых для бизнеса информационных активов у СМБ-предприятий обусловлено скорее привычным, традиционным взглядом на подобные предприятия: ведение дел «по старинке», слабое внедрение IT-технологий, хранение данных в бумажном виде — все это действительно было так. Но именно было, поскольку удешевление, а значит и доступность компьютеров и средств цифрового хранения и обработки данных происходит в ускоренном режиме, да и контролирующие организации предъявляют СМБ-рынку требования, соответствующие современным тенденциям «повсеместной оцифровки». Таким образом, все бумажные активы превращаются в невесомые файлы, «разлетающиеся» через флэшки, планшеты и облачные хранилища.

Сложно отрицать, что с точки зрения информационной инфраструктуры (топологии сети, средств управления и коммуникации, операционных систем) крупные и сравнительно небольшие предприятия мало различаются. Однако основной момент, связанный именно со спецификой СМБ, — недостаточный объем финансового обеспечения этой инфраструктуры. Отсюда и распространенные последствия.

Так в чем проблемы?

Во-первых, отсутствие долгосрочной IT-стратегии. Каждый вновь приходящий IT-специалист перекраивает инфраструктуру под свое видение и уровень знаний, постепенно превращая ее в «зоопарк» систем. Как правило, финансирование IT в СМБ осуществляется по остаточному принципу, что не позволяет проводить полноценное обновление устаревших систем. В итоге Windows 8 на ноутбуке руководителя мирно соседствует с Windows 2000 на компьютере секретаря, отдел разработки обменивается данными через Dropbox, бухгалтерия — через флэшки и дискеты, а отдел продаж и вовсе использует собственные смартфоны и планшеты — и продавцам удобно, и предприятию не нужно тратиться. А ведь подобные коммуникаторы это не только средства связи и доступа к корпоративным данным, но и весьма объемные хранилища информации.

Во-вторых, дефицит обучения сотрудников элементарным навыкам безопасного хранения данных. Большинство утечек происходит вследствие невнимательности и непонимания сотрудниками правил работы с информацией. Если для крупного бизнеса единичная утечка данных — это серьезный, но приемлемый риск, то компания средних размеров может вовсе закрыться в результате такого инцидента. Даже одна утечка (например, если речь идет о клиентской базе или бизнес-образующей технологии) может стать фатальной. Репутация также является одним из ценнейших активов, инвестировать в который приходится годами, а потерять его можно в одночасье — например, допустив разглашение чувствительной для партнеров или клиентов информации.

Третий специфичный момент — это отсутствие специалиста, которого в сегменте Enterprise гордо именуют Офицером Информационной Безопасности, в обязанности которого входит определение информационных активов, уровня риска для предприятия в случае утери или разглашения информации, а также выбор DLP-систем с последующим мониторингом результатов. В небольших компаниях все возложено на плечи одного системного администратора, у которого, даже при наличии квалификации, совершенно нет времени следить за движением информации в офисе в режиме реального времени и принимать своевременные решения.

InfoWatch EndPoint Security

Что же можно предложить организациям, которые все больше погружаются в мир цифровой информации, но не имеют достаточного финансирования для обеспечения безопасности данных? Самым эффективным решением стало бы изменение подхода к ИБ, внедрение современных систем классификации и мониторинга информации, применяемых в крупном бизнесе. Но основную проблему — недостаток финансирования — преодолеть весьма затруднительно.

Поэтому при разработке решения для предприятий СМБ мы сфокусировались на обеспечении защиты цифровых активов, не требующих больших финансовых затрат и глобальных изменений в привычных бизнес-процессах. И первым таким продуктом в нашей линейке стал InfoWatch EndPoint Security, который решает весь комплекс базовых задач в области ИБ для рабочих станций и съемных носителей информации.

Философия этого продукта описывается запоминающейся аббревиатурой C.A.F.E.: Control, Audit, Filter, Encryption. Действительно, лишь обеспечивая надежный контроль движения корпоративных данных, осуществляя непрерывное протоколирование пользовательских действий и теневое копирование перемещаемых файлов, регулируя доступ к внешним ресурсам и возможность запуска локальных приложений, а также производя сквозное шифрование в рабочих каталогах и на сменных носителях, можно с уверенностью говорить о должном уровне информационного контроля на предприятии.

Предлагаемый функционал

Одна из ключевых функциональных особенностей системы — это возможность осуществлять контроль по двум принципам: по отношению к учетной записи пользователя и по отношению к рабочему месту. Модуль контроля учетных записей пользователей не привязан к определенному компьютеру и подразумевает, что сотрудник может зайти под своей учетной записью с любого компьютера. Во втором случае контроль осуществляется над определенным рабочим местом вне зависимости от того, чья учетная запись на нем активирована.

Контроль доступа предусматривает назначение настраиваемых прав (запрет/только чтение/полный доступ/по расписанию) для любого устройства или порта, включая определенные их разновидности или уникальные устройства. Возможно создание «белого» списка WiFi-сетей, к которым — и только к ним! — будет позволено подключаться данному ПК.

В InfoWatch EndPoint Security реализована возможность создания гибких настроек прав доступа к устройствам и аудита информации с помощью механизма теневого копирования данных, записываемых на эти устройства.

Аудит информации — еще один ключевой элемент. Действия пользователей протоколируются, а благодаря меха-

низму теневого копирования администратор всегда будет осведомлен об активности сотрудников, связанной с перемещением конфиденциальных данных. Фиксируется любая операция, затрагивающая ценные информационные активы (например, запись на съемные носители, печать, копирование, удаление и др.).

Кроме контроля устройств в InfoWatch EndPoint Security заложены опции контроля при обмене файлами, а именно возможность запрета скачивания файлов через Internet Explorer, доступа к облачным файловым хранилищам (Dropbox, SkyDrive и Google Drive) и передачи файлов через Skype.

Для компаний, мигрирующих на виртуальную инфраструктуру и задействующих в бизнес-процессах работу в режиме терминальных сессий, предусмотрена функция контроля доступа к терминальным дискам (поддержку Thin Client Storage и редиректа USB по RDP).

Контроль доступа к внешним ресурсам и запуска локальных приложений настраивается с применением «черного» и «белого» списков приложений. Причем для верификации исполняемых файлов используется метод контрольных сумм. В результате подмена разрешенного приложения вредоносным или шпионским, например, путем переименования его основного модуля, становится невозможной. Привязка правил контроля доступа к учетным записям гарантирует, что с какого бы компьютера (включая удаленные подключения) пользователь ни вошел бы в систему, он будет иметь возможность запускать лишь заведомо доверенные приложения.

Права доступа: варианты

Поскольку в сегменте СМБ не принята политика жесткого контроля, мы предусмотрели два режима работы, связанных с изменением уровня прав доступа к внешним устройствам: императивный, когда права доступа к устройствам задаются администратором и не могут изменяться сотрудником, и демократичный — когда через интерфейс агента сотрудник может запросить у администратора изменение прав доступа к устройствам и портам (генерация кода доступа). Это удобно в случае, если человек находится вне сети и не имеет связи с сервером управления. Опцию по достоинству оценят сотрудники, работающие удаленно или находящиеся в командировке, — в случае необходимости открыть доступ к данным на нужном носителе им достаточно ввести код, полученный от администратора по SMS.

Выделенный сервер не требуется!

Системы ИБ знамениты сложностью в установке и настройке, чтобы установить все нужное ПО и «подружить» между собой, привлекаются системные интеграторы. Мы подходили с пониманием этой проблемы, поэтому для работы InfoWatch EndPoint Security не требуется выделенный сервер, достаточно базы данных MySQL или MS SQL (любой версии, начиная с MS SQL 2005, включая бесплатный SQL Express), а на рабочих местах требуется лишь один агент, обеспечивающий работу всех систем, включенных в продукт. Достаточно активировать их одним кликом в управляющей консоли, и InfoWatch EndPoint Security начнет работу.

Аппаратные требования к продукту не выходят за рамки требований к ОС, при этом InfoWatch EndPoint Security поддерживает все системы Windows, начиная с Windows 2000. Решение может устанавливаться как на десктопные, так и на серверные системы без необходимости перезагрузки и без конфликтов с антивирусами (KIS, Bit Defender, ESET, Dr.Web и др.).

Интеграция InfoWatch EndPoint Security с Microsoft Active Directory и Novell eDirectory позволяет использовать уже установленную в организации иерархию групп пользователей и компьютеров.

«Прозрачное» шифрование

Всем известно, что шифрование — наиболее эффективный и надежный способ защиты данных. А также вызывающий головную боль у администраторов при развертывании корпоративной системы шифрования и при работе с бесчисленными жалобами сотрудников на то, что система мешает работе. Продукт InfoWatch EndPoint Security осуществляет шифрование в прозрачном режиме, т.е. абсолютно незаметно для сотрудников, пока они используют зашифрованные данные по назначению — на рабочих местах, внутри рабочей группы или всей организации (в зависимости от включенного режима). При этом используются только криптографические модули, входящие в состав ОС, что максимально снижает риски некорректной работы и невозможности восстановления зашифрованных данных.

Модульная структура

Шестикомпонентное решение InfoWatch EndPoint Security (модули Access Control, Audit, Device Encryption, Folders Encryption, Application Control, Power Management) лицензируется по количеству учетных записей пользователей, поэтому продукт позволяет при необходимости производить перераспределение лицензий между учетными записями или компьютерами. Поскольку продукт имеет модульную структуру, итоговая стоимость зависит от приобретаемых компонент и сроков подписки, количество которых заказчик определяет сам.

Мы создавали продукт для системного администратора и постарались, чтобы решение было максимально простым и удобным в использовании, решало задачи безопасности, но не требовало постоянного внимания и тем более не служило источником жалоб от сотрудников. Поэтому InfoWatch EndPoint Security — это не просто сочетание нескольких технологий, а в первую очередь их продуманная совместная работа с единой политикой управления функционалом из одной консоли.

О группе компаний InfoWatch

Группа компаний InfoWatch объединяет несколько организаций, которые разрабатывают комплексные решения в области информационной безопасности, защиты корпоративной информации на основе собственных технологий лингвистического анализа, а также инструменты для управления бизнес-рисками — InfoWatch, Kribrum, EgoSecure, Appercut.

Портфель продуктов ГК InfoWatch включает решения для крупных корпоративных заказчиков: флагманский продукт по защите от утечек информации, внутренних угроз и контролю информационных потоков InfoWatch Traffic Monitor Enterprise, технологии шифрования CryptoStorage SDK, облачный сервис мониторинга высказываний в Интернете – InfoWatch KRIBRUM, сервис для автоматизированного анализа кода бизнес-приложений InfoWatch Appercut Code Scanner. А также решения для малого и среднего бизнеса: защита от утечек – InfoWatch Traffic Monitor Standard и система для защиты рабочих станций InfoWatch EndPoint Security.

Головная компания Группы — ЗАО «ИнфоВотч» основана «Лабораторией Касперского» в 2003 году. Сегодня InfoWatch является ведущим российским разработчиком комплексных решений для защиты корпоративной информации и занимает около 50% российского рынка систем защиты конфиденциальных данных (DLP), активно выходит на международные рынки Европы, Ближнего Востока и Азии. Головной офис ЗАО располагается в Москве, где работают более 150 специалистов и экспертов в области разработки, внедрения, интеграции, продаж и продвижения собственных продуктов и технологий.

Check Point 1100
Большая безопасность для небольших филиалов

В эпоху глобального бизнеса и все большего рассредоточения трудовых ресурсов для эффективной и результативной работы необходимо иметь доступ для удаленных работников и доступ персонала филиалов к корпоративным ресурсам. Тем не менее, даже небольшая утечка данных может подвергнуть растущие компании судебным искам, штрафам и потере репутации.

Как методы взлома и развивающееся вредоносное ПО, так и угроза потери данных принуждает компании к дальнейшему ограничению доступа к конфиденциальным данным. В условиях ограниченных IT-бюджетов и ресурсов филиалам компании необходимо недорогое, но эффективное решение для обеспечения безопасного доступа к критически важным ресурсам из любого места при минимальных рисках нарушений.

Устройства Check Point 1100 — простые, доступные и удобные в развертывании полнофункциональные решения, обеспечивающие ведущий в отрасли уровень безопасности для защиты самого слабого звена в корпоративной сети — удаленных филиалов компании. Программный блейд Check Point Threat Prevention защищает от киберугроз. Устройство Check Point 1100 — полнофункциональное централизованно управляемое устройство защиты для филиалов и удаленных подразделений. Встроенная архитектура «Программные блейды» устройства 1100 обеспечивает ту же защиту корпоративного класса, которую используют все компании из списка Fortune 100, в компактном настольном исполнении.

Устройства 1100 предлагаются в 3 модификациях, в зависимости от числа защищаемых пользователей, идеально подходят для небольших офисов с количеством сотрудников от одного до пятидесяти. В наличии имеется широкий выбор вариантов сетевых интерфейсов, включая порты 1 GbE Ethernet, WiFi 802.11b/g/n, ADSL и беспроводную связь стандарта 3G. Эти компактные настольные устройства обеспечивают выдающуюся производительность межсетевого экрана 1,5 Гбит/с и пропускную способность VPN 220 Мбит/с. Для локального управления и поддержки в условиях небольшого офиса имеется простой и интуитивно понятный web-интерфейс локального управления. Предприятия, которые хотят управлять безопасностью из центрального офиса, могут использовать Управление Безопасностью от Check Point или многодоменное Управление Безопасностью для удаленного управления и настройки согласованных политик безопасности сотен периферийных устройств одновременно.

Противодействие спаму и защита почтового обмена

Программный блейд Check Point Anti-Spam & Email Security обеспечивает всесторонний, многомерный подход для защиты почтовой инфраструктуры — обеспечивает высокую точность защиты от спама и ограждает организации от широкого спектра вирусов и вредоносных программ, доставляемых с электронной почтой.

Программные блейды шлюза

	FW — межсетевой экран (только для модели 1120)	**NGTP — следующее поколение средств предотвращения угроз**
Firewall	+	+
VPN	+	+
Advanced Networking & Clustering	+	+
Identity Awareness	+	+
IPS		+
Application Control		+
URL Filtering		+
Antivirus		+
Anti-spam		+

Преимущества

- Архитектура «Программные блейды» в компактном исполнении.
- Новое оборудование оптимизировано под нужды филиалов компании.
- Гибкие варианты управления и настройки.
- Многоуровневая защита от современных изощренных киберугроз.
- Поддержка любых требований к сети с помощью нескольких сетевых интерфейсов, опционального беспроводного доступа и ADSL-соединения.
- Несколько вариантов управления для удовлетворения любых потребностей организации:
  - упрощенное локальное управление с помощью веб-интерфейса;
  - централизованное управление с помощью Управления Безопасностью Check Point.

Идеально для сетей удаленных офисов

Устройства 1100 — полноценные сетевые маршрутизаторы, которые содержат в себе коммутатор локальной сети и выделенные порты для WAN и DMZ. Опциональный встроенный ADSL-модем устраняет необходимость в отдельном внешнем ADSL-модеме.

Устройства 1100 также содержат в себе порты USB и слот для карт PCI Express, что позволяет администратору подключать совместимый 3G-модем от стороннего производителя, обеспечивая дополнительное подключение к глобальной сети для резервирования Интернет-канала, обеспечивая максимальную надежность.

Беспроводная версия устройств 1100 содержит в себе точку доступа WiFi (802.11b/g/n), поддерживающую аутентификацию стандартов WEP, WPA и WPA2.

Встроенная система GAIA

Check Point Gaia — следующее поколение защищенной операционной системы для всех устройств Check Point, открытых серверов и виртуальных шлюзов. Gaia объединяет лучшие характеристики IPSO и SecurePlatform в единой унифицированной ОС, обеспечивающей высокую эффективность и надежную производительность. Gaia защищает сети IPv4 и IPv6, поддерживая сложные сетевые среды за счет поддержки протоколов динамической маршрутизации, таких как RIP, OSPF, BGP.

Цена от $599* без стоимости техподдержки. Цены приведены в долларах США по курсу ЦБ на момент покупки.

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

UserGate Web Filter

UserGate Web Filter обеспечивает интернет-фильтрацию для любых предприятий, образовательных учреждений, интернет-провайдеров и точек публичного Wi-Fi доступа. Решение использует в работе крупнейшую базу электронных ресурсов, разделенных для удобства оперирования на 70+ категорий. Набор сайтов насчитывает более 500 млн адресов.

Функционал решения

Продукт осуществляет морфологический анализ веб-страниц на наличие определенных слов и словосочетаний. Данная технология фильтрации позволяет контролировать доступ к конкретным разделам сайта, не блокируя ресурс целиком на уровне категории или домена. Подобный подход достаточно актуален для различных социальных сетей, форумов и других порталов, в наполнении которых значительную роль играют пользователи (Web 2.0).

Существует возможность подписки на обновление базы словарей, в том числе списка материалов, запрещенных Министерством Юстиции Российской Федерации, наборов слов «Суицид», «Терроризм», «Порнография», «Плохие слова», «Наркотики», «Азартные игры». Доступны словари на русском, английском, немецком, японском и арабском языках.

Функционал решения включает возможность принудительной активации «безопасного режима» в популярных поисковых системах (Google, Yandex, Yahoo, Bing, Rambler), а также на портале YouTube.

UserGate Web Filter поддерживает работу с «черными» и «белыми» списками электронных ресурсов. Доступ к сайтам, входящим в данные наборы, блокируется/разрешается независимо от других настроек продукта.В решении реализована возможность подписки на списки сайтов, в том числе запрещенные государством на федеральном уровне.

Проблема всплывающих окон и вездесухих баннеров приобретает все большую актуальность. Зачастую переход по ссылке, скрывшейся за навязчивой картинкой, связан не с осознанным решением, а ошибочным нажатием кнопки мыши. UserGate Web Filter осуществляет блокировку подобных окон и баннеров, в том числе загружаемых с других сайтов.

Новое в версии 3.1

Контроль загрузки файлов

Продукт позволяет контролировать скачивание определенных видов файлов (EXE, DOC, MP3, AVI и т.д.).

Фильтрация HTTPS-трафика

Наряду с обычным нешифрованным трафиком UserGate Web Filter может быть настроен для фильтрации HTTPS-трафика. При этом сервер на лету осуществляет подмену сертификата и морфологическую фильтрацию.

В UserGate Web Filter Appliance функция фильтрации HTTPs-трафика доступна по умолчанию.

Веб-статистика

UserGate Web Filter предоставляет возможность получать статистику по посещенным категориям сайтов, по разрешенным и блокированным хитам. Использование данных отчетов позволяет качественно анализировать проблемы, связанные с нецелевым использованием Интернета.

Варианты поставки

Продукт доступен в качестве:

- программного решения;
- виртуального приложения;
- программно-аппаратного комплекса;
- кластерного решения.

UserGate Proxy & Firewall

UserGate Proxy & Firewall представляет собой интернет-шлюз класса UTM (Unified Threat Management), позволяющий обеспечивать и контролировать общий доступ сотрудников к интернет-ресурсам, фильтровать вредоносные, опасные и нежелательные сайты, защищать сеть компании от внешних вторжений и атак, создавать виртуальные сети и организовывать безопасный VPN-доступ к ресурсам сети извне, а также управлять шириной канала и интернет-приложениями.

UserGate обеспечивает **комплексную защиту локальной сети**, благодаря наличию двух встроенных антивирусных модулей от ведущих разработчиков антивирусных программ — Лаборатории Касперского и Panda Security. Антивирусные модули производят сканирование всех типов сетевого трафика, включая почтовый, HTTP- и FTP-трафик. В дополнение к антивирусной проверке в UserGate встроен межсетевой экран, обеспечивающий надежную защиту сети от внешних атак посредством системы предотвращения вторжений (IDPS). В решении реализован полноценный VPN-сервер с возможностью создания туннеля «сервер-сервер», маршрутизацией между подсетями и поддержкой текущих VPN-соединений.

Посредством UserGate можно **контролировать доступ в Интернет** отдельных сотрудников компании и их групп. Встроенный модуль **Entensys URL Filtering 2.0** позволяет блокировать доступ к нежелательным ресурсам, как в отдельности, так и по категориям сайтов. UserGate также контролирует запуск приложений, установленных на клиентских машинах, разрешая или запрещая той или иной программе выход в Интернет. Подробные статистические отчеты доступны как напрямую из программы, так и удаленно посредством веб-браузера.

С помощью UserGate можно **организовать доступ в Интернет** для сотрудников вашей компании через NAT или прокси-сервер, а также одновременно работать через несколько интернет-провайдеров. Поддержка протоколов IP-телефонии позволяет воспользоваться преимуществами VoIP-решений, чтобы на их основе создать современную коммуникационную инфраструктуру компании.

Функционал UserGate включает также **удаленное администрирование** из любой точки мира.

UserGate Proxy & Firewall 6.0 VPN GOST

UserGate Proxy & Firewall 6.0 VPN GOST — специальный дистрибутив, находящийся в данный момент в процессе сертификационных испытаний ФСТЭК РФ.

Особенности версии:

- двусторонняя криптографическая аутентификация удаленных пользователей и администраторов по ГОСТ Р 34.10-2001 с использованием СКЗИ КриптоПро CSP;
- шифрование/расшифрование данных, передаваемых при организации VPN-соединения, по ГОСТ 28147-89 с использованием СКЗИ КриптоПро CSP;
- система обнаружения Вторжении (СОВ) по 4 классу защиты.

Ожидаемая дата релиза: до конца года.

Продукт поддерживает обновление списков запрещенных URL от Министерства Юстиции!

ДВОЙНАЯ ВЫГОДА

При покупке бандла* MDaemon и SecurityPlus действует скидка 20% на каждый продукт!

Только с 15 сентября по 30 ноября 2013 г.!

В акции участвуют продукты:

- **Alt-N Technologies MDaemon Messaging Server — сервер обмена сообщениями**
- **Alt-N Technologies SecurityPlus for MDaemon — безопасность вашей почты**

Условия:

- При покупке бандла* MDaemon (новые лицензии) и SecurityPlus (новые лицензии) действует скидка 20% на каждый продукт.
- При покупке бандла MDaemon (продление) и SecurityPlus (новые лицензии) действует скидка 20% на каждый продукт.

Важно:

• В акции могут принять участие только юридические лица • В акции НЕ принимает участие дозакупка • Количество лицензий обоих продуктов в одном заказе должно быть одинаковым • Скидка 20% предоставляется на каждый продукт • Предложение действует только на продукты, приобретенные в компании Softline, в период проведения акции

www.MDaemon.com

softline® 20 лет в IT

Более подробная информация о продукте на:
http://store.softline.ru/alt-n-technologies-ltd

*Бандл — совместная покупка.

Kerio Control: Комплексное решение для обеспечения безопасности и мониторинга сети

Kerio Control 8 разработан специально для защиты компаний от полного спектра сетевых угроз. Автоматически обновляющийся модуль защиты обнаруживает и предотвращает возникающие опасности, одновременно давая администратору сети гибкие инструменты для управления политиками доступа пользователей, полного управления полосой пропускания и QoS, детального мониторинга сети и возможность VPN-подключения с IPSec для настольных компьютеров, мобильных устройств и удаленных серверов.

В обеспечивающем единую систему защиты приложении Kerio Control 8 появились функции IPSec для виртуальных частных сетей (VPN).

Kerio Control гарантирует превосходную защиту сети, является стабильным, безопасным и, что немаловажно, простым в управлении решением. Оно сертифицировано ICSA Labs — признанной независимой организацией, устанавливающей стандарт для продуктов защиты электронных данных. В рамках сертификации межсетевых экранов ICSA Labs тестируются возможности программ и проводится постоянная проверка на устойчивость к новым уязвимостям. Критерии, которым должны отвечать испытания программной продукции, представляемой вендорами, являются промышленным стандартом. Этот стандарт создает консорциум компаний-разработчиков, конечных пользователей и сотрудников ICSA Labs. Релиз Kerio Control 7.3.2 имеет сертификат ФСТЭК.

Всеобъемлющая защита сети

Система предотвращения вторжений (IPS) делает сигнатурный анализ пакетов передачи данных, ведет список заблокированных IP-адресов (черный список), управляет правилами безопасности.

Тестирование осуществляется по признанным индустриальным стандартам. Продукт предоставляет корпоративный уровень защиты, т.е. обеспечивает политики безопасности по умолчанию, сразу после установки.

Возможно безопасное удаленное администрирование: все изменения в политике безопасности записываются в журнал.

Брандмауэр уровня приложений помогает создавать политики для входящего и исходящего трафика, осуществлять статичный мониторинг и журналирование сетевых пакетов и протоколов.

Антивирусная защита Sophos

Интегрированный антивирус Sophos защищает от вирусов, троянов, червей, шпионских программ и других вредоносных программ:

- защита электронной почты (SMTP и POP3). Проверка входящих и исходящих почтовых сообщений, а также их вложений. Найденные во вложениях вирусы удаляются, в сообщение добавляется информационная пометка об этом;
- web (HTTP). Сканирование web-страниц, скачиваемых по HTTP объектов и прочего трафика на наличие вирусов. Осуществляется мониторинг трафика, передаваемого по защищенному каналу Kerio VPN;
- передача файлов (FTP). Проверка скачиваний и закачек файлов по протоколу FTP.

Kerio Control Web Filter

Kerio Web Filter — это опционально-активируемый модуль для Kerio Control, который разделяет сайты на 141 категорию в зависимости от содержания. Системные администраторы могут блокировать или контролировать доступ пользователей на основе определенных категорий контента.

Например, используя категорию «Вредоносное ПО» Kerio Web Filter предотвращает посещение пользователями сайтов, имеющих вредоносное содержимое, включая вирусы, программы-шпионы, трояны, web-страницы которые участвуют в фишинге или краже персональных данных.

Встроенный модуль отчетов о поведении пользователей в сети

Защита корпоративной сети от угроз имеет жизненно важное значение для бизнеса, но не гарантирует высокую производительность труда сотрудников. Каждая ссылка на YouTube или мелькающий баннер отвлекают людей от работы. Вам необходим простой и эффективный инструмент для минимизации этих отвлекающих факторов? Kerio Control позволяет разрешить или запретить доступ к определенным сайтам, и собирать статистику по конкретным видам трафика для каждого пользователя или группы пользователей.

Что такое QoS (Quality of Service) и шейпер?

QoS-инструменты Kerio Control позволяют легко определить приоритеты и контролировать сетевой трафик, чтобы гарантировать высокую скорость для наиболее важного трафика. Простые в использовании инструменты управления трафиком, DSCP-правила, а также гибкость балансировки нагрузки, встроенные в Kerio Control, дают возможность увеличивать скорость для важных служб, таких как конференции VoIP или видео, и ограничивать пропускную способность каналов YouTube. Но это больше, чем управление пропускной полосой: благодаря наличию средств переподключения при отказе, Kerio Control предоставляет полноценный доступ в Интернет с отличным качеством обслуживания.

Распределение нагрузки на каналы

- Расширение пропускной полосы сетевого канала за счет комбинирования несколько Интернет-подключений.
- Увеличение скорости загрузки и отдачи файлов.
- Повышение производительности сервисов, требующих широкой полосы пропускания, таких как VoIP и видеоконференции.

Ограничение скорости канала

- Установка дневных или месячных квот на использование пользователями пропускной полосы.
- Ограничение скорости соединения для некритических приложений.

Подключение по резервному каналу

- Поддержка связи с Интернетом для критических приложений (почта, SQL).
- Автоматическое подключение по резервному каналу в случае отсутствия связи по основному.

Встроенный модуль статистики Kerio StaR отвечает за:

- мониторинг и создание отчетов о деятельности сотрудников в Интернете, включая поисковые запросы;
- получение по электронной почте по запросу или на регулярной основе подробных и наглядных отчетов о действиях пользователей или групп в сети;
- быстрое обнаружение «узких мест» в сети и случаев злоупотребления Интернетом.

KERIO

Транскапиталбанк использует решения Netwrix для контроля IT-инфраструктуры

Система обеспечивает оперативное выявление и реагирование на инциденты, возникающие в сфере информационной безопасности, что существенно повышает управляемость IT-инфраструктуры.

Транскапиталбанк работает на рынке финансовых услуг с 1992 года и стабильно входит в ТОП-50 крупнейших и ТОП-30 самых надежных российских банков.

Ситуация

Обслуживание IT-инфраструктуры банка выполняется коллективом специалистов с разными административными полномочиями и сферами ответственности, действия которых тесно связаны между собой. Возникали ситуации, когда изменение в Active Directory, внесенное одним из администраторов, вызывало определенный сбой работы бизнес-приложений или сервисов, за которые отвечал другой технический специалист. Были попытки решить проблему на административном уровне, для чего был разработан соответствующий регламент согласования проведения технических работ. Однако потребность в автоматизированном инструменте, фиксирующем изменения в Active Directory и групповых политиках, а также оперативно оповещающем об этом, продолжала оставаться актуальной.

Решение

В ходе тестирования выяснилось, что стандартные средства аудита не предоставляют полную информацию об изменениях, а именно не отображают состояние объекта до модификации, что усложняет процесс оперативного восстановления работы приложений.

«Нас привлек тот факт, что Netwrix Auditor — Active Directory не устанавливает дополнительное программное обеспечение на контроллеры домена, полагаясь исключительно на штатные функции аудита. Недостающую информацию Netwrix Auditor получает посредством периодического создания снапшотов — моментальных снимков AD», — комментирует Олег Ржевский, заместитель начальника Управления технической поддержки Транскапиталбанка, Microsoft MVP.

На заключительном этапе был запущен пилотный проект с использованием пробной версии Netwrix Auditor — Active Directory, которая обладает всеми функциями коммерческого программного обеспечения. По окончании тест-драйва была развернута полнофункциональная версия продукта, что не потребовало больших временных и трудовых затрат.

Результат

Использование программных продуктов Netwrix позволяет получать максимально полную картину состояния IT-системы в определенные периоды. Появляется возможность не только отслеживать изменения в инфраструктуре или отдельных приложениях, но и иметь представление о доступе к корпоративной информации, отслеживать историю работы с файлами. Средства аудита Netwrix позволяют получать оповещения об изменениях в режиме реального времени, что снижает нагрузку на IT-отделы.

Безопасность персональных данных ОАО «Белгородоблгаз»

Успешно завершен проект по созданию системы защиты персональных данных (СЗПДн) для ОАО «Белгородоблгаз».

ОАО «Белгородоблгаз» — старейшее предприятие Белгородской области. Основными видами его деятельности являются: транспортировка газа потребителям, проведение единой технической политики, координация производственной деятельности и комплексное решение вопросов, связанных с эксплуатацией газораспределительных систем и газификацией региона, а также разработка прогнозов потребления газа на территории области. Штат сотрудников предприятия превышает 3000 человек.

Решение ОАО «Белгородоблгаз» о создании СЗПДн было вызвано стремлением обеспечить защиту персональных данных, а также их конфиденциальность, целостность, доступность и подотчетность при обработке. Кроме того, в соответствии с требованиями законодательства в области защиты персональных данных предприятию важно было снизить риск угроз их безопасности при помощи способов и методов, определенных нормативными и методическими документами ФСТЭК и ФСБ.

Для выбора исполнителя проекта предприятие «Белгородоблгаз» провело тендер. Предложив оптимальные условия по стоимости и подтвердив свой профессионализм обширной экспертизой в реализации аналогичных проектов, компания Softline стала победителем конкурса.

Проект был выполнен с использованием программно-аппаратных комплексов таких производителей, как Positive Technologies, Stonesoft, CryptoPro, «Код Безопасности», Aladdin. Эксперты Softline тщательно подобрали решения различных вендоров с тем, чтобы создаваемая на их основе система полностью отвечала требованиям заказчика.

В ходе проекта специалисты Softline провели обследование и разработали концепцию защиты информационных систем, осуществляющих хранение и обработку персональных данных. В рамках данной концепции был создан технический проект новой системы обеспечения информационной безопасности, а также комплект организационно-распорядительной документации, регламентирующей процессы обработки персональных данных. Далее была проведена опытная эксплуатация созданного решения, завершившаяся приемо-сдаточными испытаниями СЗПДн. Работы выполнены на 6 площадках заказчика, система ЗПДН развернута на 8 серверах и 25 рабочих местах.

Лучший партнер VMware

Компания Softline объявляет о получении звания «Лучший партнер» VMware в категории «Региональное развитие». Этой наградой, врученной в рамках партнерской конференции VMware в Москве, вендор подтвердил компетенции Softline в области продвижения решений для виртуализации инфраструктуры и обеспечения непрерывной работы бизнеса.

Благодаря тщательному обучению персонала и индивидуальному подходу к каждому клиенту Softline продемонстрировала высокий уровень профессионализма в обслуживании заказчиков решений VMware. Кроме того, Softline обладает высшим статусом Premier в программе VMware Solution Provider и полным набором компетенций по решениям VMware. С 2006 года Softline неоднократно была номинирована как лучший партнер в России, а в 2012 году была удостоена награды «Best Partner in EMEA Emerging Markets», став лидером по продажам решений вендора среди партнеров 100 стран региона. Компания Softline также стала первым российским дистрибьютором по программе VMware Service Provider Program на территории России и СНГ. С 2008 года в Softline работает авторизованный центр обучения VMware.

Softline обеспечила защиту данных администрации города Орск

Компания Softline в Оренбурге осуществила поставку программного продукта Kaspersky Endpoint Security для бизнеса в администрацию города Орск. Внедрение решения «Лаборатории Касперского» обеспечило сохранность информации организации и повысило производительность корпоративной IT-инфраструктуры.

Администрацией города Орск был объявлен открытый конкурс на поставку и техническую поддержку антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса Расширенный. Победителем тендера стала компания Softline.

«На протяжении 10 лет мы успешно используем продукты «Лаборатории Касперского». Антивирусные решения разработчика полностью удовлетворяют нашим требованиям и обеспечивают стабильную и безопасную работу организации. При выборе поставщика лицензий мы всегда уделяли особое внимание репутации реселлера. Именно поэтому мы выбрали партнером проекта компанию Softline, надежного и опытного поставщика, обладающего наивысшим партнерским статусом производителя — Enterprise Partner», — рассказывает начальник отдела по информатизации и связи администрации города Орск Валерий Воловельский.

Программное обеспечение Kaspersky Endpoint Security для бизнеса Расширенный предоставляет инструменты защиты и управления, необходимые организации для внедрения политик IT-безопасности, блокирования вредоносного ПО и предотвращения потери данных, а также для повышения производительности корпоративной IT-инфраструктуры. Решение позволяет администраторам просматривать и контролировать состояние защиты всех физических, виртуальных и мобильных устройств через единую консоль управления.

Softline и «Лаборатория Касперского» защитили данные «Конвентстройинжиниринг»

Softline обеспечила безопасность данных компании «Конвентстройинжиниринг», осуществив поставку программного продукта Kaspersky Endpoint Security для бизнеса. Решение «Лаборатории Касперского» обеспечило сохранность информации и повысило производительность корпоративной IT-инфраструктуры организации.

Компания «Конвентстройинжиниринг», существующая с 2005 года, специализируется на продаже и установке кондиционеров и вентиляционного оборудования, а также на проведении сопутствующих строительных работ.

При выборе антивирусных продуктов заказчик руководствовался возможностью сохранения высокой производительности корпоративной IT-инфраструктуры, а также надежностью ПО при защите рабочих станций, серверов и персональных данных клиентов и сотрудников от различного рода угроз. Использовавшиеся ранее продукты «Лаборатории Касперского» удовлетворяли основным требованиям компании по обеспечению безопасности информации, что также позитивно повлияло на выбор антивирусного решения. В итоге в компании было принято решение о закупке лицензий Kaspersky Endpoint Security для бизнеса Стандартный.

Благодаря внедрению решения «Лаборатории Касперского» рабочие места сотрудников, а также серверы оказались надежно защищены от попыток заражения. Это способствовало обеспечению бесперебойной работы IT-инфраструктуры компании, а значит и повышению эффективности ее бизнеса.

По итогам проекта «Конвентстройинжиниринг» получил современное решение по обеспечению многоуровневой защиты предприятия, эффективность которого подтверждена независимыми тестами. Это позволило свести к минимуму риски потери информации и простоя в работе компании. Данное решение помогло заказчику обеспечить соответствие необходимым стандартам качества, а после внедрения способствовало успешному проведению аудита IT-инфраструктуры предприятия.

«Мы вновь сделали выбор в пользу решения «Лаборатории Касперского», поскольку убедились в том, что антивирусное ПО этого производителя обеспечивает оптимальную защиту рабочих ПК и серверов компании. Продукт Kaspersky Endpoint Security для бизнеса Стандартный привлек соотношением оптимальной цены и высокого качества, простотой установки, а также удобством управления посредством соответствующей консоли. Решение было предоставлено компанией Softline в кратчайшие сроки. Также мы имели возможность получать необходимую техническую поддержку по продукту как со стороны IT-партнера, так и со стороны разработчика», — рассказывает Булат Шамсутдинов, коммерческий директор компании «Конвентстройинжиниринг».

«Внедрение программного обеспечения «Лаборатории Касперского» позволило повысить уровень соответствия информационной безопасности компании «Конвентстройинжиниринг» высоким требованиям надежности, которые предъявляются к поставщикам на конкурентном рынке. В результате проекта были минимизированы риски нарушения ИБ, что привело к повышению доверия к компании со стороны клиентов и партнеров», — комментирует Евгений Робинов, руководитель направления по информационной безопасности отдела сервисов компании Softline в Казани.

Softline помогла Салехардской ОКБ автоматизировать предоставление IT-сервисов

Компания Softline завершила проект по внедрению системы управления конфигурациями System Center Configuration Manager (SCCM) для Салехардской окружной клинической больницы.

О заказчике

ГБУЗ «Салехардская окружная клиническая больница» основана в 1893 году. Учреждение оказывает первичную медико-санитарную и специализированную медицинскую помощь населению г. Салехарда, а также жителям округа, преимущественно из сельских территорий. В настоящее время в структуру Салехардской ОКБ входят стационар и амбулаторно-поликлиническая служба, имеющая взрослую, детскую и стоматологическую поликлиники; общая численность сотрудников превышает 1500 человек.

Ситуация

В северных городах УрФО очень остро стоит вопрос нехватки квалифицированных IT-специалистов. Для Салехардской ОКБ, находящейся в Заполярье, данная проблема более актуальна, чем для коммерческих организаций. Именно поэтому больнице требовалась максимальная автоматизация предоставления IT-сервисов.

Решение

В рамках заключенного соглашения Microsoft Enterprise Agreement (EA) руководством больницы совместно с менеджерами и инженерами компании Softline было принято решение автоматизировать процесс управления парком ПК, насчитывающим около 400 единиц и более 1500 пользователей, работающих в шести зданиях больницы, с помощью системы управления конфигурациями System Center Configuration Manager (SCCM).

Процесс

Реализация проекта проходила в несколько этапов. На первом специалисты Softline провели аудит существующей IT-инфраструктуры больницы. В ходе второго этапа было проведено внедрение и настройка центрального сайта SCCM. После этого к нему были подключены рабочие места пилотной группы пользователей, а также осуществлена миграция операционной системы с Windows XP на Windows 7. На завершающем этапе для специалистов заказчика был проведен инструктаж по основам работы с системой, после чего решение было запущено в эксплуатацию.

«Роль IT в Салехардской ОКБ невозможно переоценить — автоматизированы важнейшие аспекты деятельности: исследовательские лаборатории, операционные, приемные докторов и многое другое. Поэтому отсутствие перебоев в работе IT-сервисов было самым важным условием при реализации работ по проекту. Кроме того, важно было помнить и о сохранении конфиденциальности личных данных пациентов больницы, — отмечает Дмитрий Наговицын, руководитель Центра решений компании Softline в Уральском ФО и Пермском крае. — SCCM позволяет проводить инвентаризацию используемых активов (ПК и ПО) без существенных трудозатрат. Также при использовании SCCM появилась возможность стандартизировать рабочие места пользователей. Существенным нововведением стал функционал, автоматизирующий установку операционной системы и программного обеспечения ПК и миграцию среды пользователей на новейшие операционные системы корпорации Microsoft».

Результат

Итогом проекта стала автоматизация основных процессов IT-департамента, что позволило уменьшить трудозатраты подразделения на поддержку и развитие IT-инфраструктуры, а также эффективно организовать работу удаленных подразделений с информационной системой больницы. Как следствие, снизилась и необходимость в увеличении штата IT-специалистов. «Выражаю благодарность специалистам Softline за успешное выполнение работ по развертыванию системы управления конфигурациями. Реализация задач, предусмотренных в проекте, была проведена на высоком организационном, техническом и качественном уровне. Все этапы проекта были проведены в минимально возможные сроки, без срывов и непредвиденных задержек. Большую роль в этом сыграл высокий уровень квалификации специалистов Softline. В ходе реализации проекта мы получили ценные технические консультации, благодаря которым был решен ряд важных вопросов по настройке системы и ее дальнейшей эксплуатации», — комментирует итоги проекта Анатолий Крупин, главный врач-директор территориального центра медицины катастроф ГБУЗ «Салехардская окружная клиническая больница».

***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.

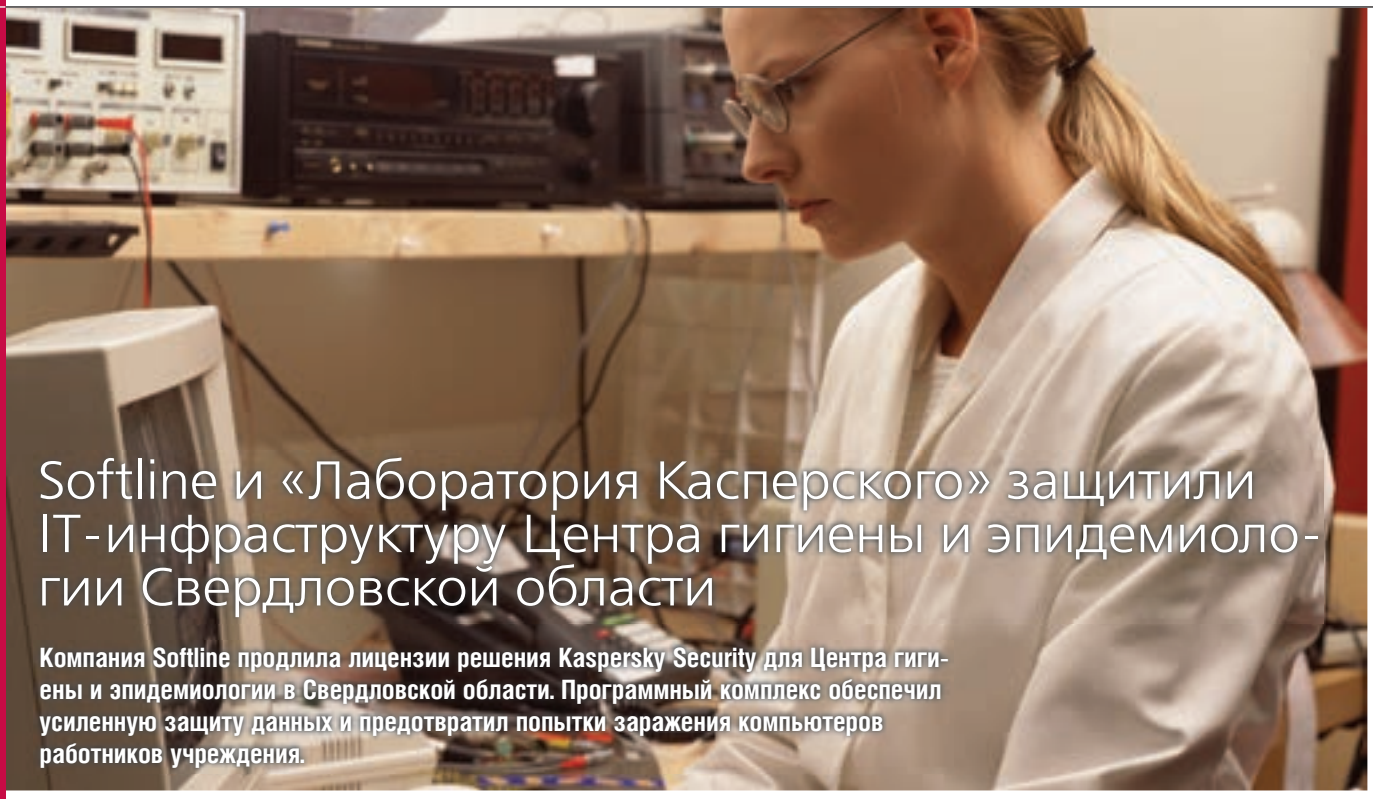
ВЕБИНАРЫ

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



Softline и «Лаборатория Касперского» защитили IT-инфраструктуру Центра гигиены и эпидемиологии Свердловской области

Компания Softline продлила лицензии решения Kaspersky Security для Центра гигиены и эпидемиологии в Свердловской области. Программный комплекс обеспечил усиленную защиту данных и предотвратил попытки заражения компьютеров работников учреждения.

Ситуация

Перед отделом информационного обеспечения учреждения стояла задача организовать надежную защиту данных и бесперебойную работу сотрудников. При этом компьютерный парк организации насчитывал 2000 устройств, размещенных в головном офисе и в 29 филиалах Центра.

Решение

Выбор был сделан в пользу программного продукта Kaspersky Security для бизнеса — комплексного решения, сочетающего инновационные «облачные» и классические антивирусные технологии. Функциональные возможности решения позволяют создать надежный механизм гибридной защиты, предназначенный для отражения как существующих, так и новых угроз. Унифицированный код модулей антивирусного ядра также способствует оптимизации использования ресурсов рабочих станций и серверов, при этом минимизируя влияние на работу других приложений.

Компания Softline, обладающая наивысшим статусом Kaspersky Enterprise Partner и имеющая успешный двадцатилетний опыт работы на рынке IT, была выбрана в качестве партнера проекта по итогам конкурса на поставку данного ПО, предложив заказчику наиболее гибкие условия.

Результат

«Мы рассматривали варианты внедрения программных продуктов ряда ведущих мировых разработчиков ПО. Выбор был сделан в пользу решения «Лаборатории Касперского» — в основном, за счет полного набора необходимого функционала, удобства настройки и эксплуатации, а также наличия надежной и доступной службы технической поддержки. Основные цели были достигнуты: рабочие места наших сотрудников надежно защищены от попыток заражения компьютеров», — отметил Алексей Лутков, заведующий отделом информационного обеспечения ФБУЗ «Центр гигиены и эпидемиологии в Свердловской области».

«Для сферы здравоохранения все мероприятия по защите информации (а это и построение защищенной виртуальной сети передачи данных, и защита от несанкционированного доступа к серверам и терминальным рабочим станциям, и антивирусная защита) являются необходимым условием работы. Причем в каждом медучреждении реализация мер по обеспечению информационной безопасности должна вестись строго с учетом требований регуляторов. Продукты «Лаборатории Касперского» соответствуют всем критериям, предъявляемым государством к работе с конфиденциальными данными, и имеют необходимые сертификаты ФСБ РФ. На наш взгляд, заказчик сделал правильный выбор, и мы были рады оказать содействие в реализации этого проекта», — подчеркнул Алексей Бутаков, директор по развитию бизнеса компании Softline в Уральском ФО и Пермском крае.

О заказчике

Федеральное бюджетное учреждение здравоохранения «Центр гигиены и эпидемиологии в Свердловской области» является некоммерческой организацией, входящей в структуру Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека. В структуру Центра входят 29 территориально распределенных филиалов. Его основной задачей является лабораторное и экспертное обеспечение надзорных мероприятий, проводимых Управлением Роспотребнадзора по Свердловской области.

УЧАСТВУЙ В АКЦИЯХ! ПОЛУЧАЙ ПОДАРКИ! УЧАСТВУЙ В АКЦИЯХ! ПОЛУЧАЙ ПОДАРКИ!

Softline дарит подарки!

Юбилейная программа «20 лет в IT – Марафон скидок»

ДО 28 ФЕВРАЛЯ 2014 ГОДА

Каждый 20 счет — выигрышный

Купи на $20 тыс. — получи подарок

Поздравь Softline с 20-летним юбилеем

До 28 февраля 2014 г. спешите воспользоваться специальными предложениями на приобретение решений от таких производителей, как **Microsoft**, **«Лаборатория Касперского»**, **Adobe**, **ESET** и многих других!

Принять участие могут только юридические лица — организации с парком ПК от 10 до 250 единиц.
Программа распространяется на следующие регионы: Екатеринбург и Свердловская область, Курган и Курганская область.

Регистрируйтесь на сайте
http://20let.softline.ru

softline® 20 лет в IT

(343) 278-53-35
620144 Екатеринбург, ул. 8 Марта, д. 194, секция И.
www.softline.ru/ekt | info.ekt@softline.ru

Коммуникации без границ

Компания Softline завершила проект по созданию корпоративной системы объединенных коммуникаций как части комплексного решения по модернизации IT-инфраструктуры нефтяной акционерной компании «Аки-Отыр» — дочернего предприятия ОАО НК «РуссНефть».

Ситуация

Имеющаяся на предприятии система коммуникаций не могла обеспечить высокую эффективность взаимодействия между подразделениями компании. В связи с этим было принято решение модернизировать существующую систему объединенных коммуникаций и тем самым снизить временные и материальные издержки на связь между сотрудниками. Партнером по данному проекту была выбрана компания Softline, обладающая обширным опытом и глубокой экспертизой в различных областях IT.

Решение

Руководством «Аки-Отыр» совместно со специалистами Softline было разработано комплексное решение на основе Microsoft Lync Server 2013 и Exchange Server 2013. Работая в тандеме, перечисленные системы значительно сокращают затраты предприятия на телефонную связь, а также предоставляют новые защищенные инструменты и возможности для эффективного взаимодействия сотрудников.

Процесс

Для подготовки к внедрению экосистемы объединенных коммуникаций специалисты Softline совместно с инженерами «Аки-Отыр» провели комплексное обследование существующей IT-инфраструктуры предприятия и спроектировали оптимальную с точки зрения функционала и обслуживания архитектуру решений.

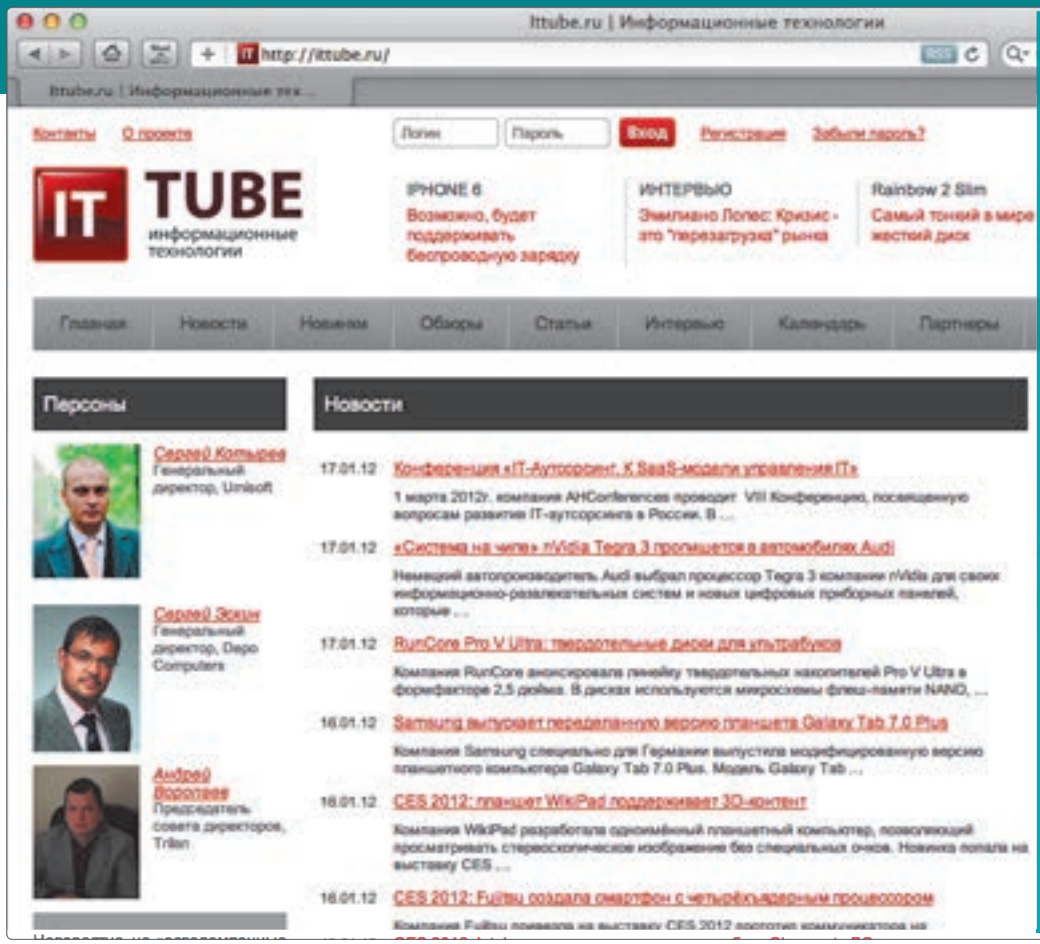
Благодаря внедрению специалистами Softline системы на основе Microsoft Lync в «Аки-Отыр» значительно выросла скорость коммуникации сотрудников.

Проведенное обследование службы каталогов показало, что она не удовлетворяет требованиям, в результате чего была предложена миграция, и все серверные компьютеры, рабочие станции и учетные записи пользователей были перенесены в новый лес Active Directory. Электронная почта была перенесена специалистами Softline на отказоустойчивый вариант на базе Exchange Server 2013, который гарантирует работу почты даже в случае выхода из строя одной из серверных площадок. Сотрудники получили систему универсальных коммуникаций на основе Lync.

Результаты

Инженеры Softline реализовали комплексную систему объединенных коммуникаций «под ключ». Работы включали в себя: детальное обследование IT-инфраструктуры, разработку оптимальной архитектуры, внедрение систем Lync Server и Exchange Server, разработку сопроводительной документации и инструкций, рекомендаций по использованию, обучение технических специалистов и длительный период технической поддержки. Теперь сотрудники могут использовать совместные календари, устанавливать задачи, а также получать дополнительные возможности планирования ресурсов. Кроме того, стала возможной блокировка отправки почтовых сообщений в зависимости от отправителя и получателя письма, а также использование других транспортных правил. Помимо этого, были значительно повышены отказоустойчивость почтового решения и безопасность доступа к среде коммуникаций за пределами корпоративной сети с любого ПК или мобильного устройства. Благодаря внедрению специалистами Softline системы на основе Microsoft Lync в «Аки-Отыр» значительно выросла скорость коммуникации сотрудников. Одним из самых удобных инструментов повседневного взаимодействия стали внутренние и внешние аудио- и видеоконференции: теперь с помощью мобильных устройств и планшетных ПК в них могут участвовать все сотрудники — вне зависимости от их местонахождения. Еще одна ключевая функция — возможность предоставлять коллегам доступ к своему «рабочему столу» и файлам для совместной корректировки различных документов и принятия оперативных решений.

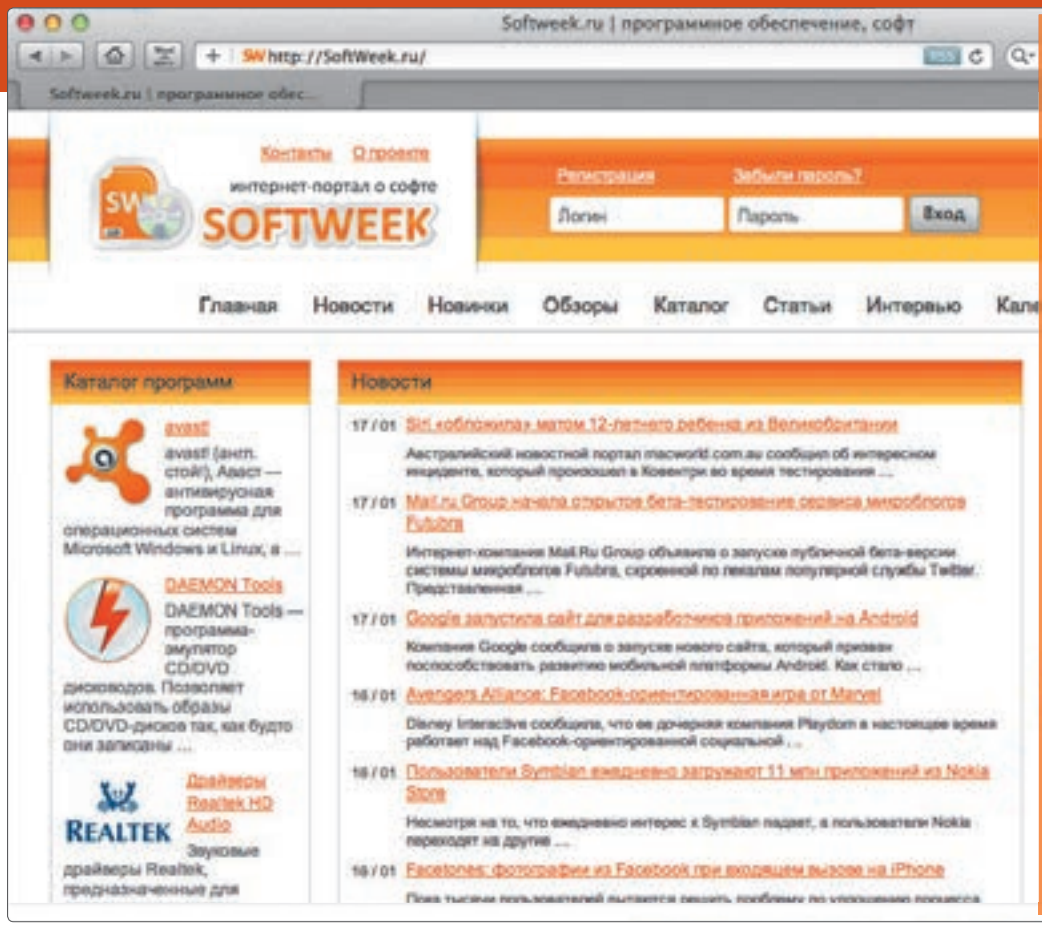
Интернет-портал гаджетов ittube.ru



- 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

Акции и скидки

Покупателям Salesforce.com — Google Apps for Business в подарок

12.09.2013 — 30.11.2013

Softline объявляет о запуске акции «Google Apps for Business в подарок при покупке 100 лицензий CRM Salesforce Enterprise Edition». В результате интеграции двух облачных решений у заказчиков появится возможность видеть историю взаимодействий с клиентами внутри CRM, использовать почту Google для проведения рассылок, синхронизировать задачи и календари пользователей, атакже многие другие преимущества.

При покупке от 100 лицензий Enterprise Edition Sales Cloud или Service Cloud с 1 сентября по 30 ноября 2013 года клиенты Softline получат в подарок 100 лицензий Google Apps for Business сроком на один год. Предложение действует для заказчиков из России и стран СНГ.

Скидка 10% на Microsoft Office Standard 2013 для государственных организаций

08.10.2013 — 24.12.2013

Стартует новое ценовое предложение от Microsoft для государственных организаций — 10% скидки на Office Standard по уровню Government A при покупке от 10 до 249 лицензий! Акция проводится по следующим условиям:

- предложение действует при покупке от 10 до 249 лицензий на одну организацию;
- предложение распространяется на лицензии по программе Open License;
- предложение распространяется на государственные организации (за исключением академических) — только на уровень OLP GOV A;
- заказы по уровню GOV A не должны превышать 149 баллов на 1 заказ. 1 лицензия Office 2013 Standard Lic only = 2 балла;
- Microsoft оставляет за собой право отказать в обработке заказов в случае нарушения условий данных специальных предложений.

Скидка 24% от Corel для госучреждений

01.10.2013 — 30.11.2013

Компания Corel сообщает о предоставлении специальных цен на все коммерческие лицензии продуктов для государственных учреждений. С 1 октября по 30 ноября государственные учреждения получают возможность закупки всех коммерческих лицензий в любом количестве на продукты Corel по ценам уровня J (от 2500 лицензий). Фактически экономия даже при покупке одной лицензии составит более 24%.

Данная акция распространяется на все типы коммерческих лицензий (включая Upgrade и Maintenance) всех продуктов Corel.

Новый этап Радминизации. Присоединяйтесь!

01.10.2013 — 31.12.2013

Компания Фаматек сообщает о старте нового этапа конкурса «Радминизация всей страны», который проводит совместно со своими партнерами. Конкурс стартует 1 октября 2013 года и продлится до 31 декабря 2013 года. Для участия в конкурсе менеджерам нужно зарегистрировать свои продажи Radmin.

Конкурс проводится уже в шестой раз и с каждым этапом количество участников возрастает, а их продажи увеличиваются. Список призов стал еще более интересным и был дополнен высокотехнологичными новинками 2013 года — новейшими смартфонами Apple iPhone 5S, Samsung Galaxy Note 3, а также Nokia Lumia 1020!

Самые активные продавцы получат следующие призы:

1 место — Apple MacBook Pro 13 with Retina display;
2 место — Apple iPhone 5S (32Gb) New;
3 место — Samsung Galaxy Note 3 (32Gb) New;
4 место — Nokia Lumia 1020 (32Gb) New;
5 место — Apple iPad 4 + cellular (32Gb);
6 место — Apple iPod touch (16Gb);
7 место — Apple iPod nano (16Gb);
8 место — Apple iPod shuffle 4 (2Gb).

Участники, занявшие 9 и 10 место, получат флэшки с символикой Radmin на 8Gb. Среди участников, занявших с 9-го по последнее место, случайным образом будет разыгран поощрительный приз: Apple iPad 4 Wi-Fi!

Подробнее ознакомиться с правилами конкурса и принять участие можно на странице акции: www.radmin.ru/partners/contest/.

Acrobat XI: купи 6 по цене 5!

16.09.2013 — 28.11.2013

Компания Adobe предоставляет клиентам, покупающим 5 и более коммерческих лицензий Adobe Acrobat XI Standard или Adobe Acrobat XI Professional специальное предложение — 6 лицензий по цене 5! Adobe Acrobat XI — это не просто конвертер PDF, а комплексное решение, которое содержит множество интеллектуальных функций и дополнительных возможностей для взаимодействия с самыми разнообразными документами.

Самые новые приложения Adobe со скидкой 40%!

03.09.2013 — 29.11.2013

Спешите приобрести свои любимые инструменты Creative Cloud со скидкой 40%! Акция проходит для клиентов Adobe и уже существующих подписчиков Adobe Creative Cloud до 29 ноября 2013 года и действует на всей территории России. Скидка предоставляется не только на первый год покупки подписки, но и для дозакупки лицензий и их продления в 2014 году.

Список приложений, доступных по подписке:

- Photoshop CC Multiple Platforms;
- Adobe Audition CC Multiple Platforms;
- Adobe Muse CC Multiple Platforms;
- Adobe Premiere Pro CC Multiple Platforms;
- After Effects CC Multiple Platforms;
- Dreamweaver CC Multiple Platforms;
- Edge Animate CC Multiple Platforms;
- Edge Inspect CC Multiple Platforms;
- Flash Professional CC Multiple Platforms;
- Illustrator CC Multiple Platforms;
- InCopy CC Multiple Platforms;
- InDesign CC Multiple Platforms;
- Prelude CC Multiple Platforms;
- SpeedGrade CC Multiple Platforms.

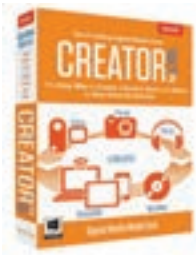
Новые продукты

TrustPort Total Protection 2014

Мультидвижковый антивирус TrustPort, постоянный лидер независимых тестов Virus Bulletin, предоставляет всестороннюю защиту ПК от вредоносных программ, шпионского ПО и утечки конфиденциальной информации. В TrustPort Total Protection 2014 используется улучшенный антивирусный сканер, пользовательские профили, пользовательский интерфейс в стиле Windows 8 и улучшена интеграция с мобильными компонентами Portunes и SkyTale (для iOS/Android). К любому из многочисленных видов сканирования теперь можно перейти непосредственно из главного интерфейса, кроме того, добавлен игровой режим.

TrustPort Security Elements 2014

TrustPort Security Elements 2014 — новая версия комплексного решения для обеспечения безопасности корпоративных сетей различного масштаба и отдельных их компонентов. Продукт предоставляет корпоративным пользователям и администраторам антивирусную защиту рабочих станций, серверов, фильтрацию интернет-трафика, а также защиту от вирусов и спама на шлюзе. В обновленной версии TrustPort Security Elements 2014 улучшены средства управления TrustPort Management (в частности, процесс установки, обновления и обслуживания в сети) и антивирусная защита рабочих мест.



Roxio Creator NXT 2

Roxio Creator NXT — лидирующий в своей отрасли программный пакет для работы с мультимедийными материалами — был обновлен до версии 2. Продукт отличается повышенной производительностью благодаря интеллектуальному кодированию AVC/H.264 и улучшенной поддержкой таких устройств, как Xbox One, PlayStation 4, iPad, iPhone. Новые библиотеки музыки предоставляют больше творческих возможностей для создания фото- и видеопроектов. Усовершенствованная конвертация аудиоданных экономит время пользователя и может использоваться при создании профессиональных мультимедиа-проектов.

MAGIX Movie Edit Pro 2014

MAGIX Software GmbH объявила об обновлении своего продукта для редактирования фильмов — MAGIX Movie Pro Edit 2014, также доступного в редакциях Plus и Premium. Версия 2014 предлагает повышенную производительность мультипоточной обработки благодаря более эффективному использованию многоядерной архитектуры. Продукт содержит много нового контента, совместимого с форматами HD и 16:9, предлагает DVD/Blu-ray и киношаблоны, образцы начала и концовки видео. Кроме того, впервые могут использоваться HDR-эффекты. Новая версия также оптимизирована для сенсорных экранов.

IObit Driver Booster Pro 1.0

Состоялся финальный релиз продукта для управления драйверами IObit Driver Booster 1.0, который теперь доступен в двух редакциях — платной и бесплатной. Версия Pro ускоряет процессы обновления до 3 раз, а также предлагает расширенную техническую поддержку. Одно из основных преимуществ ПО — в обширной и надежной базе данных драйверов. Каждый объект тщательно протестирован и всегда актуален, поскольку хранится в облаке, а не загружается на локальный ПК. Загрузка и установка осуществляется в фоновом режиме. Новая программа также поддерживает работу с игровыми драйверами.

DeviceLock Endpoint DLP Suite 7.3

Компания «Смарт Лайн» объявила о выпуске новой версии программного комплекса для защиты информации от утечек DeviceLock Endpoint DLP Suite 7.3. Очередная версия продукта предоставляет широкие возможности контроля устройств на ПК под управлением Apple OS X Lion и OS X Mountain Lion, что позволяет службам ИБ организаций любого масштаба унифицировать DLP-политики как для Windows-компьютеров, так и для Mac-компьютеров наиболее простым и удобным способом — из оснастки DeviceLock в редакторе групповых политик Group Policy Management Console для Microsoft Active Directory.

MDaemon Messaging Server

Alt-N Technologies представляет уникальное предложение для СМБ — сервер электронной почты MDaemon Messaging Server и решение для защиты от вирусов и спама SecurityPlus for MDaemon. MDaemon Messaging Server является удачной альтернативой платформе Microsoft Exchange для СМБ. Он поддерживает протоколы IMAP, SMTP, POP3 и ActiveSync, предоставляя высокую производительность и удобный интерфейс. SecurityPlus for MDaemon дополняет встроенные инструменты безопасности MDaemon Messaging Server, формируя щит, блокирующий угрозы до их попадания в IT-инфраструктуру.

F-Secure Internet Security 2014

Компания F-Secure анонсировала выпуск новых версий своей линейки продуктов, включающей F-Secure Internet Security 2014. Главные достоинства релиза — эффективная проактивная защита DeepGuard, веб-защита и родительский контроль, надежный онлайн-банкинг и безопасное посещение социальных сетей. В решении используется также новая технология для обнаружения конфликтующего программного обеспечения: установка ПО теперь будет использовать переработанные компоненты для проверки ПК на наличие конфликтующих программ, которые могут помешать нормальной работе антивируса.

20-я международная выставка и конференция

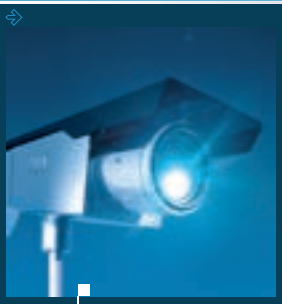
ОХРАНА, БЕЗОПАСНОСТЬ И ПРОТИВОПОЖАРНАЯ ЗАЩИТА

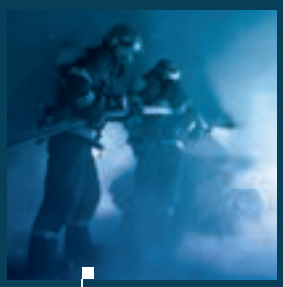
ufi Approved Event

MIPS MOSCOW

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

Нам 20 лет!




- Охранное телевидение и наблюдение
- Технические средства обеспечения безопасности
- Системы защиты периметра. Ограждения
- Пожарная безопасность. Аварийно-спасательная техника. Охрана труда
- Смарт карты

Организатор:

ITE

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

При поддержке:

МВД России

www.mips.ru

Что такое корпоративный поиск на базе Google Search Appliance?

- Поисковые технологии Google
- Индексирует 220 форматов файлов
- Знакомый пользовательский интерфейс
- Соблюдение прав доступа пользователей к информации
- Единый поиск по всем корпоративным системам
- Мультиязычный поиск и перевод
- Готовые коннекторы для популярных корпоративных систем
- Простая архитектура и масштабируемость

40 000 крупнейших компаний во всем мире выбрали решение Google Search Appliance для корпоративного поиска

softline®

Компания Softline — эксклюзивный поставщик поисковых решений Google в России

(495) 232-00-23 | www.softline.ru | google@softline.ru

Google Apps for Business –

облачные приложения для эффективной совместной работы

Пришло время Google!

Более **5 млн**
компаний по всему миру уже используют Google Apps for Business

70%
компаний Fortune 500 уже используют решения Google Enterprise

- Снижение затрат на поддержку инфраструктуры коммуникаций и офисные приложения до 70%
- Увеличение эффективности работы персонала в 2 раза
- Гарантированная доступность 99.9%
- Фактическая доступность почтового сервера 99,983% по данным за 2012 г.

Бесплатный доступ к Google Apps for Business на 30 дней

softline® 20 лет в IT

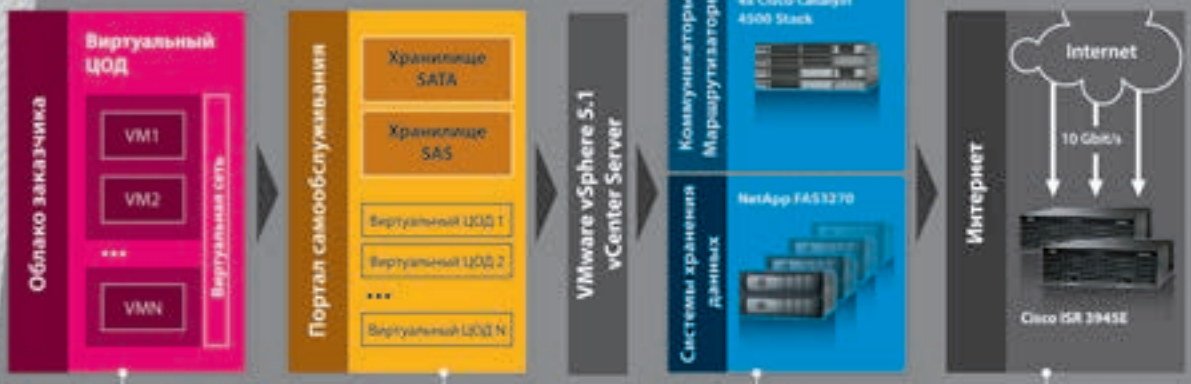
cloud.softline.ru

(495) 232-00-23 | google@softline.ru

IaaS

МОЩНОСТЬ В АРЕНДУ

Бесплатный тест-драйв на сайте softcloud.ru



Автозапуск двигателя не выходя из дома

Организация работы IT-инфраструктуры по облачной схеме

Суперкар оснащен умной электроникой

Удобное управление виртуальным ЦОД с помощью web-портала

Ездить на машине мечты

Новейшее оборудование от ведущих производителей

Разгон до 100 км/ч за секунды

Обмен данными со скоростью до 10 Gbit/s

Экономия на налогах и страховках

Не требуется покупать оборудование и лицензии

Защита от кражи авто

Обеспечение абсолютной безопасности Ваших данных

Экономия на обслуживании авто

Полное техническое обслуживание платформы включено в стоимость аренды

Экономия времени и денег на покупку машины в ограниченном бюджете

Аренда необходимых ресурсов под любые Ваши проекты

К Вашим услугам – **СОВРЕМЕННАЯ IAAS-ПЛАТФОРМА** для построения отказоустойчивой IT-инфраструктуры в облаке с возможностью **гибкого масштабирования и расширения** арендуемых вычислительных мощностей.

Для поддержки постоянной работоспособности облачной платформы Softline задействовала современный программно-аппаратный комплекс ведущих производителей серверного, а также коммуникационного оборудования и технологий виртуализации: **VMware, IBM, HP, Cisco, NetApp.** Это позволяет нам предоставлять абсолютные гарантии отказоустойчивости, надежности и безопасного использования вычислительных ресурсов облачной платформы.

softline®

Services Software Cloud

+7 (495) 232 00 23
8 800 100 00 23
cloud.softline.ru
cloud@softline.ru

ОБЛАЧНЫЕ ТЕХНОЛОГИИ

КАК ИСПОЛЬЗОВАТЬ ОБЛАКО

- **Вынести в него любые данные и сервисы, интегрировать их между собой и с Вашей инфраструктурой**

- 1С
- файл-сервер
- корпоративную почту
- корпоративный портал
- CRM-системы
- ERP-системы
- сервисы для управления проектами
- средства совместной работы
- сервисы Helpdesk
- антиспам и антивирусные решения
- инфраструктурные решения

- **Организовать резервный ЦОД**

Публикация **приложений**

ActiveCloud by Softline предлагает проектирование и внедрение оптимальной архитектуры служб удаленных рабочих столов

Ключевые преимущества для бизнеса:

01 Доступ к многофункциональным приложениям с помощью веб-страниц или портала **SharePoint**

02 Ускорение внедрения новых бизнес-приложений и обновления существующих

03 Полная интеграция опубликованных на сервере приложения **RemoteApp** с локальным рабочим столом

04 Исключение риска хищения данных в случае потери или кражи мобильного устройства

05 Однократное развертывание приложения на сервере вместо установки на каждом компьютере

06 Подключение к внутренним приложениям по **протоколу HTTPS** с SSL-шифрованием без необходимости использования VPN

07 Удобство работы для пользователей

Полную информацию об услуге вы можете получить у наших менеджеров

8 800 100-22-50
sales@activecloud.ru
activecloud.ru

ActiVe CLOUD by softline

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

Active CLOUD

by softline

Аренда Symantec Backup Exec 2012

Резервирование становится доступнее!
Комплексный подход к резервированию и восстановлению данных

Доступны агенты для Microsoft Windows Server, SQL Server, Exchange, SharePoint, Active Directory, VMware, ORACLE, SAP и др.

Microsoft Windows Server
Microsoft Office SharePoint Server
SAP
Microsoft Exchange
Microsoft SQL Server
vmware
ORACLE

Symantec Backup Exec

- **Новейшие разработки**

  Инновационная технология выборочного восстановления для сред Exchange и Active Directory.

- **Мировое признание**

  Сертифицированные корпорацией Microsoft средства резервного копирования и восстановления для новейших продуктов компании.

- **Оптимизация ресурсов**

  Снижение затрат на хранение и оптимизация использования сетевых ресурсов за счет технологии устранения дублирования данных и архивирования.

- **Оперативность и безотказность**

  Сокращение времени на резервное копирование и обеспечение требований к точкам восстановления для непрерывной защиты данных.

- **Простота использования**

  Простые функции обновления и управления. Лёгкое добавление и восстановление резервных копий.

- **Широкие возможности**

  Расширенные дисковые системы хранения для новейших физических и виртуальных серверных систем, включая системы VMware и Microsoft Hyper-V.

+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**

Radmin 3.5

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 буд то 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 3.5 Стандартная лицензия (на 1 компьютер)	11-13-FAMATECH-SL	1250
Radmin 3.5 Пакет из 50 лицензий (на 50 компьютеров)	11-14-FAMATECH-SL	38000
Radmin 3.5 Пакет из 100 лицензий (на 100 компьютеров)	11-15-FAMATECH-SL	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, включая Kerberos, и службы каталогов Active Directory.
- IP-фильтрация.
- 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 8.

softline®

Premier Business Partner IBM

В два раза больше виртуальных машин. Меньше затрат на организацию работы. И никаких компромиссов

Вы ищете ИТ-решения, которые отвечали бы все более и более сложным требованиям, предъявляемым к ИТ-инфраструктуре? IBM Flex System™ на базе процессоров Intel® Xeon® – это простота, гибкость и контроль в одной системе, с которой не придется идти на компромиссы.

По сравнению с предыдущим поколением блейд-серверов эта система позволяет создавать в два раза больше виртуальных машин[1]. А благодаря IBM Flex System Manager™ можно сократить расходы на организацию работы систем за счет возможности из одной точки видеть и контролировать все реальные и виртуальные компоненты[2].

Вы сможете выбрать отдельные элементы и интегрировать их самостоятельно либо с помощью бизнес-партнера IBM. Другой вариант – выбрать систему IBM PureFlex™ и воспользоваться преимуществами экспертной интеграции от IBM, что будет еще проще. Подробнее — на ibm.com/systems/no_compromise/ru.

Узнайте, почему эксперты исследовательской компании Clubby Analytics выделяют IBM Flex System среди других предложений на рынке блейд-серверов. Скачайте статью на ibm.com/systems/no_compromise/ru.

Реклама

intel inside Xeon

[1] Согласно тестированию, проведенному IBM, и документации по консолидации серверов с помощью возможностей виртуализации IBM System x®. По сравнению с сервером предыдущего поколения BladeCenter® HS22V система IBM Flex System x240 поддерживает в 2,7 раза больше виртуальных машин с максимальной загрузкой. [2] По материалам подготовленной аналитической компанией IDC статьи «Экономические аспекты виртуализации: шаг к модели затрат, основанной на использовании приложений», Мишель Бейли, ноябрь 2009 года, http://www.vmware.com/files/pdf/Virtualization-application-based-cost-model-WP-EN.pdf. Дополнительный узел IBM Flex System для хранения данных доступен в четвертом квартале 2012 года.

IBM Notes 9.0

Первый релиз «социальной» корпоративной почты без приставки Lotus

Компания IBM выпустила первый новый релиз своей почтовой платформы Notes and Domino 9.0 после отказа от марки Lotus, сопровождавшей все предыдущие версии Notes и Domino.

«Социальная» почта

Главная особенность этого релиза заключается в его социальной направленности. В платформе Notes 9.0 компания IBM стремится воспроизвести среду социальных сетей, включая сторонние приложения, которые теперь доступны прямо в почтовом клиенте.

«Социальная» почта IBM Notes 9.0 призывает пользователей проводить больше времени в электронной почте. По оценке самой компании IBM, сегодня работники интеллектуального труда проводят до 80% своего рабочего времени, разбираясь с почтой. Внедрение приложений в почту имеет определенный смысл, поскольку помогает избавить пользователя от постоянного переключения между приложениями, сохраняя больше времени на продуктивную работу.

Встроенные приложения

Встроенные приложения для IBM Notes and Domino 9.0 Social Edition внедряются в почтовую платформу с помощью набора программных интерфейсов OpenSocial API. Эти приложения предлагают выполнение различных операций с элементами почты и календарей, как развлекательные (по большей части) сторонние приложения в социальных сетях. В результате появляется возможность выстроить документооборот таким образом, что основным носителем останется электронная почта, но сторонние приложения не придется глубоко интегрировать с сервером электронной почты и коллективной работы. По мнению разработчиков из IBM, в будущем в почту Notes можно будет встраивать даже такие «тяжелые» промышленные приложения, как SAP.

Абстракция вложений

Еще одна новая функция Notes 9.0 — это абстракция вложений. Это значит, что вложения электронной почты теперь будут храниться отдельно, вне рамок почтового клиента. Внутри компании IBM с использованием этого метода уже хранится 6 ПБ вложений. Все вложения находятся в единственной копии в централизованных хранилищах, где обеспечивается контроль версий и работа множества пользователей с одним файлом в реальном времени. При этом на клиентских машинах не создаются локальные копии вложений, засоряющие жесткий диск, а вот администраторам систем хранения данных явно прибавится работы.

Компания IBM отдельно отметила, что предыдущий 2012 год был исключительным для платформы Notes/Domino, поскольку в этот год более 1600 заказчиков вернулись к использованию этого продукта после того, как ранее перешли на другие платформы. Дополнительное преимущество обновленной платформе IBM Notes обеспечивает и тот факт, что уже выпущена локальная версия облачного офисного пакета — IBM Docs on Premise.

IBM Notes 9.0 Social Edition: что нового?

Решение находилось в разработке чуть более 18 месяцев. Основная цель — сделать Notes более современным, в едином тематическом стиле, с полностью переработанным упрощенным интерфейсом. При этом важной особенностью остается использование самых последних и стабильных web-технологий.

IBM Notes 9.0 Social Edition легок в использовании, за счет того, что:

- улучшена производительность;
- помощь «на лету» оказывает дополнительное меню Discover для поиска решений;
- появилось много расширений и удобных новшеств (ссылки в режиме редактирования, сортировка по критериям использования и др.);
- в основе — новая технологиия для платформ OpenSocial.

Обновленный интерфейс

1. Оптимальное проектирование и однородность пользовательского интерфейса и взаимодействия по всему портфелю продуктов.
2. Знакомые и стандартные шаблоны.
3. Снижение расходов на обучение и ускорение внедрения продуктов.
4. Упрощение управления и цветовой гаммы интерфейса — главное видно сразу.
   - Цветовая палитра стала спокойнее.
   - Уменьшена плотность текста, улучшена читаемость тем.
   - Больше слов, меньше значков.
   - Упрощенная графика.

Лучшие новые функции

- Новая страница «Discover».
- Ссылки в режиме редактирования.
- Быстрый поиск.
- Группировка по дате.
- Автоматическая сортировка по дате.
- Быстрый доступ к почте, календарю, контактам и т.д.
- Прокрутка в календаре.
- Настройка вида для недели Weekly Planner.
- Категоризация по цветам Color Pallete.
- Добавление автора в контакты.
- Функция «Ответить всем» в папке исходящих писем.
- Вставка в режиме Plain Text.
- Подержка Mac Cocoa.
- Новые горячие клавиши:
  - Ctrl+R — «Ответить»;
  - Ctrl+Shft+R — «Ответить всем»;
  - Ctrl+Alt+V — «Специальная вставка»;
  - Ctrl+Shft+V — «Вставить без форматирования».

Команда «Ответить всем» из папки «Исходящие» теперь удаляет имя отправителя из поля «Кому». Окно диалога «Проверить Календарь» можно перемещать. Оно отображается поверх всех окон Notes. Поиск осуществляется в почте и архивах одновременно.

Notes Browser Plug-in

Разработан для того, чтобы просматривать из браузера приложения, ранее доступные только для пользователей Notes.

Этот мощный инструмент в дополнение к возможностям XPages позволяет запускать приложения в браузере без каких-либо изменений! Он легок в установке и конфигурировании.

Local Mail Delivery Failover

Новинка в Domino 9.0 Social Edition — функция, поддерживающая Local Failover — доставку сообщения, даже если почтовый файл назначения в данный момент недоступен. Если база данных работает в автономном режиме, в режиме обслуживания или была по каким-либо причинам удалена, почта будет маршрутизироваться на сервер с копии реплики.

Контакты

Оформить заказ вам поможет Анна Курьянова.

Пишите: annakuri@softline.ru

Решения Softline на базе IBM Lotus Domino

DirectoryCatalog/Ru

Единый корпоративный справочник

Решение DirectoryCatalog/Ru основано на встроенном средстве Lotus Domino — Directory Catalog. После регистрации сотрудника в системе Lotus Domino он автоматически добавляется в единый корпоративный справочник, в котором сами сотрудники или автоматизированные программные средства импорта заполняют всю необходимую информацию о сотрудниках.

В стандартной конфигурации Lotus Domino/Notes пользователь имеет возможность использовать только системный справочник сервера Lotus Domino (Domino Directory или NAB). Для пользователя Lotus Notes он имеет ряд неудобств:

- справочник содержит большой объем системной информации;
- англоязычный интерфейс;
- пользователь не имеет возможности изменять контактную информацию о сотрудниках;
- нельзя вносить дополнительную информацию о сотрудниках (ICQ, Skype, Facebook и т.д.);
- безопасность системы Lotus Domino подвергается существенной уязвимости, если справочник NAB пользователь выносит на ноутбуке из офиса;
- отсутствие единого корпоративного справочника при использовании нескольких NAB.

Решение DirectoryCatalog/Ru избавляет от перечисленных выше проблем и упрощает работу пользователя. Данное решение основано на встроенном средстве Lotus Domino — Directory Catalog — и является открытым, при необходимости оно может быть расширено под дополнительные потребности компании.

Каковы результаты?

- В организации создается единый корпоративный справочник, который заполняется в автоматическом или полуавтоматическом режиме.
- Справочник автоматически подключается к почте Lotus Notes или любому другому почтовому клиенту с помощью протокола LDAP.
- Появляется возможность быстрого доступа к контактной информации о сотруднике, используя удобный русифицированный интерфейс Lotus Notes или web-браузер, а также заполнения любой дополнительной информацией, которая соответствует корпоративному стандарту компании.
- Повышается безопасность сервера Lotus Domino. Справочник содержит только краткую информацию о сотруднике, что позволяет избежать утечки системной информации сервера при использовании справочника вне офиса, иметь у пользователя корпоративный справочник, работая в offline-режиме вне офиса.

Система корпоративного информирования

Любой сотрудник крупной компании ежедневно помимо персональной корреспонденции получает большое количество различный внутрикорпоративных рассылок: новости, объявления, приказы и т. д. Такие сообщения на несколько минут отвлекают внимание людей от важных текущих дел, что в масштабах компании приводит к большим временным потерям. Подобные рассылки оказывают дополнительную нагрузку на почтовые сервера и сетевое оборудование, ощутимо повышают размеры корпоративных почтовых ящиков. Наше решение призвано устранить обозначенные проблемы и создать единый информационный раздел.

Вместо организации групповой рассылки сотрудник компании заполняет форму, в которой указываются:

- название новости;
- категория новости;
- получатели;
- анонс новости;
- текст с картинками.

Ежедневно в установленное время (например, 8:00 — до начала рабочего дня) сотрудникам компании приходит единое новостное письмо, которое содержит в себе анонсы всех рассылок.

Полный текст каждой новости можно посмотреть в Lotus Notes или web-интерфейсе, кликнув на ссылку после анонса. Каждую новость сотрудники компании могут обсудить на форуме и оставить свои комментарии к ней.

Любой желающий может опубликовать свое объявление в разделе «частные объявления».

Work group: общие ресурсы для совместного пользования

Решение «Рабочая группа» позволяет пользователям без привлечения IT-специалистов создавать собственные виртуальные информационные пространства для совместного пользования общими ресурсами. В данных информационных областях автор может сам определять, кому предоставить доступ к документу в качестве редакторов и читателей.

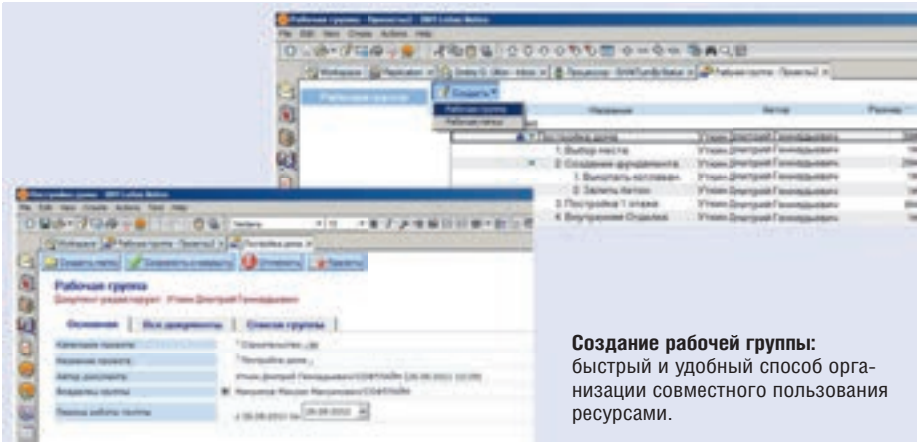
В созданной рабочей группе пользователи могут помещать в совместное пользование файлы, форматированный текст и картинки.

Для работы в модуле Рабочая группа (Work group) необходима платформа IBM Lotus Domino / Notes. Используя данный модуль, пользователи могут создавать управляемую информационную область, в которой у них будет возможность:

- сохранять ограниченную информационную область для совместной работы;
- размещать и совместно работать с файлами документов в доступных им областях;
- определять редакторов документа;
- группировать рабочие файлы по папкам и сопровождать их текстовым комментарием и картинками;
- создавать 5 последних версий редактирования документа;
- создавать обсуждения к папкам документов (мини-форум).

Кроме того, система контролирует возможность одновременного редактирования документа.

Функционал Softline Work Group дополняет и расширяет возможности Lotus Domino и интегрируется с сервисами, предоставляемыми Lotus Social, облегчая их использование и внедрение в рабочий процесс сотрудников.



Создание рабочей группы: быстрый и удобный способ организации совместного пользования ресурсами.

Auslogics BoostSpeed 6

Продукт включает более 15 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 всевозможного файлового «мусора», дубликатов файлов и ненужных программ. Дефрагментация диска с помощью популярного инструмента Auslogics Disk Defrag повышает скорость доступа к данным и оптимизирует файловую систему. Модуль Disk Doctor проверяет диск на ошибки и помогает избежать потери данных, а Disk Explorer выявляет папки и файлы, занимающие больше всего места, чтобы вы могли перенести или удалить их при критическом заполнении дискового пространства.

Настройка системы. Программа включает утилиту с более чем 280 различными опциями для быстрой и удобной настройки Windows согласно нуждам и предпочтениям пользователя. Модуль Locked Files Manager позволяет производить операции с файлами, доступ к которым закрыт системой или приложениями. Отдельные утилиты дают возможность управлять запланированными задачами, системными службами и программами, настроенными на автозапуск.

Оптимизация интернет-соединения. Встроенный Internet Optimizer позволяет настраивать параметры интернет-соединения как автоматически, так и вручную для увеличения скорости 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.

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.
- Автоматическая оптимизация использования памяти и процессора в режиме реального времени.

Новые возможности

- **Удобная навигация.** Новый интерфейс упрощает работу с программой.
- **Управление браузерами из общей панели.** Новая уникальная утилита позволяет настраивать все популярные веб-браузеры, установленные в системе, из одной удобной панели, устанавливая поисковую систему по умолчанию, управляя домашними страницами и удаляя ненужные плагины и надстройки.
- **Планирование очистки и оптимизации.** Теперь еще легче настроить автоматическое поддержание системы в оптимальном состоянии с помощью удобно расположенной вкладки планировщика.

Автоматизация управления договорами в представительстве Philips в России и СНГ

Компания Philips с большим вниманием относится к эффективной организации рабочего процесса. Именно поэтому на уровне российского руководства компании было принято решение о создании выделенной группы по оформлению и согласованию контрактов и автоматизации данного процесса.

Олег Зупник

Сергей Давыдов

В качестве партнера по проекту была приглашена команда Департамента разработки информационных систем компании Softline. Одним из требований Заказчика, обусловленных внутренней политикой, было использование исключительно штатных возможностей SharePoint 2010. Работы по организации системы электронного документооборота были разделены на несколько этапов. На текущий момент успешно завершен первый этап, в рамках которого был настроен базовый функционал системы, обеспечивающий автоматизацию процесса подачи и обработки запросов по договорам для офиса, в котором работает более 700 человек. Подробнее о проекте нашему изданию рассказали Олег Зупник, руководитель отдела по управлению и сопровождению контрактов Philips в России и СНГ, и Сергей Давыдов, IT-менеджер по операционной работе компании Philips в России.

— Господа, сотрудничали ли вы с Softline ранее, до начала проекта?

Сергей Давыдов: Да, закупали программное обеспечение. Сотрудничество началось задолго до начала текущего проекта, и уже тогда мы с коллегами из Softline обсуждали пути дальнейшего взаимодействия, касающегося, например, разработки портала, сайтов, инфраструктурных решений.

Олег Зупник: На рынке не так много квалифицированных специалистов, способных качественно реализовывать действительно сложные бизнес-задачи на базе динамично развивающегося продукта SharePoint. Нам нравится конструктивный настрой проектной команды департамента разработки Softline, сотрудники не отказывают и всегда стараются решить поставленную задачу, какой бы трудной она ни была.

— Каковы, на ваш взгляд, особенности данного проекта?

С.Д.: Большая часть инфраструктуры нашей компании находится на аутсорсинге у крупных сервис-провайдеров, которые предоставляют нам облачные решения. С одной стороны, это позволяет нам добиться необходимого уровня масштабирования и качества сервиса в масштабах всей компании, а с другой — накладывает некоторые ограничения на возможности изменения стандартных решений и сервисов на локальном уровне. Вот и в данном случае, в качестве платформы используется облачная версия MS SharePoint, работа с которой, в отличие от локального продукта, предполагает применение нетривиальных подходов, с чем команда Softline хорошо справляется. Есть и еще ряд сложностей, связанных с настройкой системы с точки зрения ее производительности: сложные расчетные процессы «выедают» ограниченную квоту процессорного времени в системе, но проектной команде Softline пока удается найти «резервные возможности» системы, чтобы выполнить наши требования. Этот проект — уникальная практика для всей рабочей группы.

О.З.: Стоит добавить, что еще одной ключевой особенностью этого проекта является тот факт, что все работы осуществляются без прерывания и замедления текущих бизнес-процессов. Это как операция на живом сердце, когда нельзя сделать ни одной ошибки.

— Расскажите, как была организована работа с контрактами ранее и ощутили ли вы изменения с внедрением первого блока системы?

О.З.: До того, как был сформирован отдел по управлению и сопровождению контрактов, в котором сейчас трудится порядка восьми специалистов, в процесс согласования документации были вовлечены около 60 ассистентов из различных отделов компании. При формировании данного отдела требовалась исключительная гибкость ИТ-инструментов, чтобы новые сотрудники могли оперативно подхватить всю работу по договорам различных видов, сильно отличающихся друг от друга по бизнес-процессам. Нам было необходимо новое простое решение, обладающее гибкостью Excel и мощностью хорошей базы данных. SharePoint значительно облегчил жизнь специалистам и позволил минимизировать возможные ошибки. Теперь мы можем работать с масштабными файлами и тратить на обработку документа не более 5 минут, а коллеги из Softline дают нам подробные инструкции, позволяющие делать тонкую настройку системы под конкретные бизнес-процессы, что в свою очередь способствует увеличению производительности труда сотрудников отдела.

Главной целью проекта для нас всегда была и есть максимальная автоматизация процессов документооборота. Поскольку контракты и запросы поступают к нам тысячами, каждая операция, выполняющаяся автоматически, экономит массу времени и усилий.

С.Д.: Раньше, чтобы запустить процесс обработки договоров, сотрудникам приходилось переписываться по электронной почте, а теперь процесс находится под контролем: портал дает возможность создавать заявки и отслеживать статус согласования контракта. Кроме того, электронная почта — не лучший вариант для аудиторов компании, так как согласование документов по почте неизбежно сопровождается ошибками. Общение через SharePoint — более надежное в этом плане. Система позволяет оставлять комментарии в процессе утверждения документов, и мы активно пользуемся этим функционалом. В настоящее время, мы создаем полноценный архив документов на базе SharePoint, со всеми сопутствующими комментариями, заметками и подтверждениями, чтобы в любой момент времени можно было вернуться к документу и отследить историю его изменений. SharePoint в этом плане хорошо решает задачу хранения всех промежуточных версий документа.

Реализация полноценной системы документооборота с использованием базовых возможностей SharePoint в отделе по управлению и сопровождению контрактов московского офиса Philips уже заинтересовала коллег из других стран, что говорит об очевидной практической пользе внедренного решения и возможности его тиражирования.

Заинтересовались проектом?

Обращайтесь в Департамент разработки Softline.

Пишите: webdev@softline.ru

Звоните: +7 (495) 232-00-23, доб. 2085, Александр Суханов

О компании

Royal Philips (Нидерланды) — это международная компания, работающая в индустрии «здоровья и благополучия» и нацеленная на улучшение жизни людей путем внедрения значимых инноваций. На российском рынке Philips присутствует с 1898 года, в московском офисе компании трудится порядка 700 человек.

22 миллиона человек

в России использует мобильный интернет и мобильные приложения через смартфоны.

Они могут использовать и Ваше приложение!

А оно у вас есть?

По данным проведенного исследования FDT Lesson & Sons

Разработка мобильных приложений

softline®

Сайты и информационные порталы / Интернет - магазины / Мобильные приложения
Геоинформационные системы / Корпоративные порталы / Решения по учету IT–активов / Биллинговые системы
Решения на базе SalesForce CRM / Электронный документооборот / Решения для управления архивом документов
Поисковые технологии / Интеграция информационных систем / Разработка заказного ПО

http://webdev.softline.ru

+7 (495) 232–00–23, доб. 2085

Выбор профиля для стелс-антенны

Авторы статьи: Франческа Де Вита, Симоне Ди Марко, Фабио Коста и Паоло Турчи, компания Altran Group, Италия.

Перевод: Владимир Цветков, Евгений Кузнецов

Частотно-избирательная поверхность, состоящая из набора геометрических объектов, может выступать в качестве радиочастотного фильтра и позволяет сократить эффективную площадь рассеяния для антенн. Существуют, в буквальном смысле, тысячи возможнных вариантов профиля подобной поверхности и тестирование физического прототипа каждого из них займет огромное количество времени. Моделирование позволяет отобрать наиболее перспективные конфигурации в считанные минуты.

На протяжении почти 30 лет компания Altran Group является одним из мировых лидеров в области инноваций, высокотехнологичных инженерных проектов и консалтинга, предоставляя свои услуги на всех стадиях разработки проектов: от стратегического планирования до запуска в производство. Ее клиентами являются ключевые игроки в таких отраслях, как аэрокосмический комплекс, машиностроение, энергетика, железнодорожная промышленность, финансы, здравоохранение и телекоммуникации.

Антенна — самое уязвимое место

Наша команда работает в первую очередь в аэрокосмической и оборонной промышленности, и некоторые из проектов посвящены изучению наилучшего расположения антенны, а так же определению эффективной площади рассеяния и ее снижению. Один из таких проектов занимается одной из самых инновационных областей оборонной промышленности последних лет — стелс-самолетами и кораблями, способными быть малозаметными для радаров. Подобный результат достигается путем комбинирования различных технологий, включая подбор специальной формы поверхности, отражающей сигнал заданным образом, а также использование поглощающих излучение материалов. В то же время, для корректной работы антенны корабля или самолета, покрывающая ее поверхность должна обладать достаточным уровнем радиопрозрачности. Как следствие, антенна становится одним из компонентов с наибольшей площадью эффективного рассеяния (ЭПР), что может поставить крест на общей радарной малозаметности самолета или корабля.

Эффективная площадь рассеяния зависит от поляризации и частоты воздействующей радиоволны. Под воздействием электромагнитной волны, в объекте-цели индуцируются электрические токи, порождающие вторичное излучение и ответную рассеянную волну. Последняя частично отражается непосредственно на источник воздействующей волны, на чем и основывается принцип функционирования радаров. Пиковая интенсивность отраженной волны зависит от коэффициента направленного действия антенны и от пиковой эффективной площади ее поверхности. Как следствие, конструкторы сталкиваются с противоречием: при стремлении максимизировать коэффициент направленного действия (КНД) антенны, необходимо также уменьшить площадь эффективной поверхности рассеяния, что в свою очередь требует уменьшения КНД.

Одним из методов обойти это противоречие является использование частотно-избирательной поверхности. Последняя представляет из себя узор, из отверстий или поверхностей специальной формы на подложке, который, по существу, действует как полосно-пропускающий фильтр. В заданном диапазоне частот, например, где ведется прием и передача сигнала радиооператорами, антенна функционирует привычным образом; в то время как в других диапазонах частотно-избирательная поверхность больше поглощает, чем рассеивает воздействующее излучение. Как правило, антенны размещаются в защитном кожухе, который называется куполом радиоантенны: в самолетах он обычно расположен в носовой части. Применение частотно-избирательной поверхности позволяет значительно уменьшить ЭПР корпуса на всех частотах, за исключением рабочих.

Геометрические узоры в качестве фильтра

Частотно-избирательные поверхности, как правило, представляют из себя периодически чередующийся набор упорядоченных металлических пластин произвольной геометрической формы. Они напоминают «заплатки» на металлическом экране (см. рисунок 1). Рабочие характеристики частотно-избирательной поверхности зависят от ее формы, толщины, выбора подложки и зазора между отдельными элементами. Мы сосредоточились на физических конфигурациях и резонирующих частотах в пределах заданных диапазонов. При изучении этих вопросов, бесценную помощь нам оказал продукт COMSOL Multiphysics.

Как показано на рисунке 1, частотно-избирательная поверхность состоит из группы геометрических объектов. По сравнению с длиной волны, размер поверхности может оказаться очень большим, равно как и число геометри-

Металлические полоски, окруженные воздухом

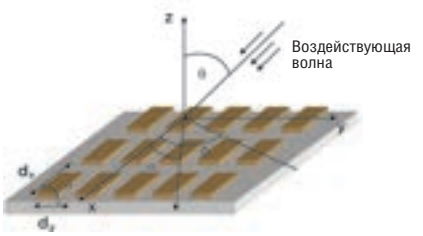


Рисунок 1. Пример частотно-избирательной поверхности, сделанной из множества металлических полосок.

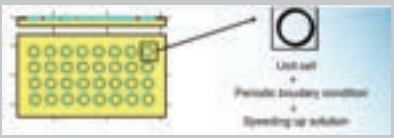


Рисунок 2. Функция задания периодических граничных условий, доступная в COMSOL, значительно ускоряет поиск оптимальной формы частотно-избирательной поверхности, позволяя свести задачу к моделированию одного блока ячеек.

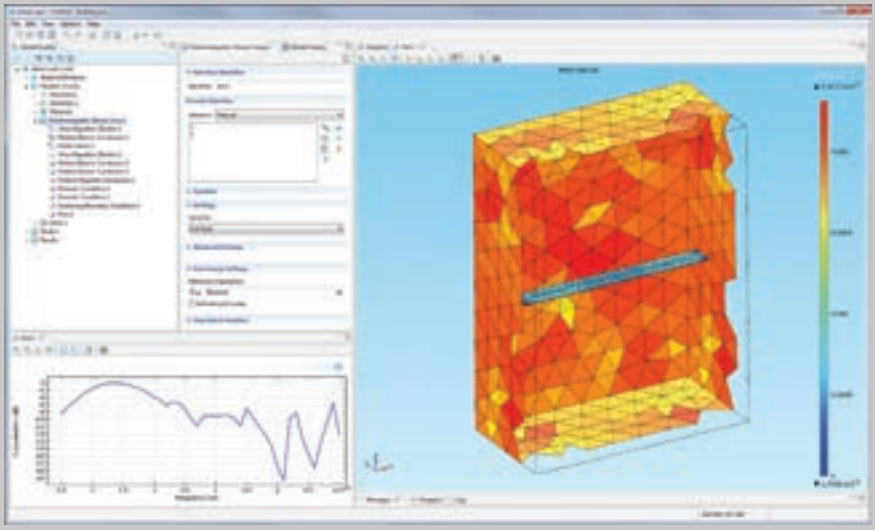


Рисунок 3. Пример простой частотно-избирательной поверхности, основанной на массиве металлических полосок, окруженных воздухом (правая часть) с расчитанной кривой частотной характеристики (левая нижняя часть). Кривая отображает параметр S11 в децибелах в масштабе 1010 с резонансной частотой в районе 40 ГГц. Углубление соответствует максимальной излучаемой мощности.

ческих объектов-«заплаток». Как следствие, моделирование поведения полной поверхности становится весьма громоздким и затратным с точки зрения как вычислительных мощностей, так и времени. К счастью, среди набора доступных в COMSOL Multiphysics инструментов, есть очень удобный способ разрешения этой проблемы - использование «Периодических граничных условий» (Periodic Boundary Condition, PBC). Использование PBC позволяет свести задачу к моделированию одного блока ячеек (или одной ячейки) и тем самым приводит к значительной экономии временных затрат (см. рисунок 2). Этот способ также гарантирует сохранение непрерывности электрических и магнитных полей, благодаря чему мы получаем результаты, эквивалентные решению полной задачи, с учетом поведения всех блоков ячеек на поверхности.

Нас очень впечатлила экономия по времени и оперативной памяти, полученная при использовании PBC, при одновременном сохранении уровня точности, необходимого для изучения поведения заданных геометрий поверхностей. Так, при моделировании простой структуры без диэлектрической подложки, время моделирования сокращается в 100 раз; а для более сложных электрических структур возможно сокращение времени в 1000 раз или даже больше.

Рисунок 3 (верхняя правая часть) демонстрирует пример частотно-избирательной поверхности, сделанной из простых металлических полос, окруженных воздухом. Моделирования для одной из полос показало наличие прозрачности в районе 40ГГц, как это видно из частотной диаграммы (нижняя левая часть).

Для подтверждения правильности решения и проверки модели, мы начали с анализа доступного в литературе примера и повторения результатов расчетов в пакете COMSOL Multiphysics.

Отладив модель, мы перешли к следующей стадии, на которой уже провели исследование влияния выбора формы и материала на характеристики частотно-избирательной поверхности.

Мы использовали программное обеспечение для углубленного исследования частотных характеристик множества объектов простой формы и небольшого размера, а также всевозможных способов их распределения по поверхности. Также, мы получили возможность усложнить конструкцию, комбинируя два типа «заплаток», поведение которых дополняет друг друга. Это позволяет, например, разрабатывать системы с множеством резонирующих частот.

> «Возможность моделирования произвольного количества объектов различной формы в очередной раз подчеркивает эффективность COMSOL Multiphysics как инструмента, позволяющего нам осуществлять эффективный поиск оптимального решения»

Возможность моделирования произвольного количества объектов различной формы в очередной раз подчеркивает эффективность COMSOL Multiphysics как инструмента, позволяющего нам осуществлять эффективный поиск оптимального решения. Возможной альтернативой численному моделированию является изготовление и физическое тестирование различных прототипов частотно-избирательных поверхностей, что связано с ощутимо большими затратами по времени и материальным ресурсам. Используя моделирование, мы можем в течении нескольких минут определить, заслуживает ли исследуемый образец более детального изучения или нет.

В настоящий момент мы начинаем работу над улучшением нашей модели путем добавления учета влияния эффектов от диэлектрической подложки. Также, мы планируем начать работать с алгоритмами оптимизации, которые помогают в решении задачи с дополнительными ограничениями, например, на максимальный размер блока ячеек.

Группа сотрудников Altran, занимающаяся моделированием (слева направо): Фабио Коста, Симоне Ди Марко, Франческа Де Вита и Паоло Турчи.

Wolfram SystemModeler™

В преддверии выхода четвертой версии Wolfram SystemModeler рассмотрим ее основные возможности и отличительные черты, позволившие ей занять одно из лидирующих мест на современном рынке программного обеспечения для моделирования физических систем.

На сегодняшний день существует несколько основных требований к системам физического моделирования. Они должны поддерживать возможность моделирования задач, включающих в себя разнородные физические системы, поддерживать иерархическую структуру моделей, иметь возможность заготавливать компоненты для многоразового пользования. Но прежде всего модели должны быть достоверными и точными на столько, чтобы заменить создание прототипов и натурных экспериментов. Пакет WSM был разработан с учетом всех этих требований. Он предлагает инженерам проектировщикам мощные средства для моделирования физических систем с помощью гибкой рабочей среды и обширной библиотеки готовых физических и логических компонентов. Пакет поддерживает как статическое, так и динамическое моделирование систем с возможностью пошаговой визуализации.

WSM создан на базе технологий Modelica компонентно-ориентированного моделирования компании MathCore Engineering AB, которая была поглощена компанией Wolfram Research в 2011 году. Modelica является открытым языком, специально созданным для моделирования физических систем, а компонентно-ориентированный подход дает существенные преимущества по сравнению с блочно-ориентированным моделированием. Он также позволяет пользователям эффективно работать над крупномасштабными проектами, создавая индивидуальные компоненты и библиотеки многократного пользования. SystemModeler — это результат более чем десятилетнего тесного сотрудничества со специалистами из автомобильной, медико-биологической, корабельной и тяжелой промышленности, что делает его легким в использовании инструментальным средством. В то же время знание самого языка Modelica не является необходимым для успешной работы в системе.

Возможности Wolfram SystemModeler

SystemModeler позволяет легко создавать реалистичные модели в различных предметных областях. Благодаря встроенным численным решателям можно проводить точный анализ модели в различных условиях. SystemModeler предусматривает автоматическую визуализацию трехмерных механических элементов. В качестве особенностей системы отметим следующие функции.

- **Drag & Drop моделирование.** С помощью drag-and-drop подхода можно быстро на интуитивном уровне создать собственную модель. Выбирая, например, транзистор или пружину, вы просто перетаскиваете их на свободное пространство. Необходимо соединить выбранные элементы между собой, чтобы обозначить электрические провода или механическую связь.
- **Иерархическое моделирование.** Модель в SystemModeler представляет собой иерархическую структуру. Такая модель более понятна и более проста в разработке. Вы можете тестировать и использовать отдельно каждый подуровень Вашей модели, что способствует быстрому анализу различных сценариев и проектных решений.
- **Моделирование в различных областях.** Зачастую любая система совмещает в себе несколько подсистем из различных областей физики — механическая подсистема, электрическая подсистема или тепловая подсистема. В SystemModeler не существует ограничений на число взаимосвязанных подсистем. Анализ таких моделей позволяет выявить важные и интересные эффекты, которые могли быть пропущены в другом случае.
- **Встроенные библиотеки моделей.** В SystemModeler существует большое число встроенных библиотек языка Modelica, которые содержат модели поступательных, вращательных двумерных и трехмерных механических компонентов, электрических и логических блоков и т.д. Библиотеки содержат документацию и полные коды.
- **Визуализация.** При помощи одного щелчка мыши можно получить график любой интересующей переменной. Можно строить несколько графиков, создавать параметрические графики и настраивать их внешний вид. Существует возможность совместного использования SystemModeler компонентов CAD-систем для создания трехмерных визуализаций. Для более тонких

настроек можно использовать интеграцию с системой Mathematica.

- **Моделирование биологических реакций.** SystemModeler предоставляет уникальную возможность проводить численные эксперименты с процессами метаболизма. Библиотека BioChem включает в себя модели разнообразных реактивов, набор различных физических условий для проведения экспериментов, а также примеры стандартных биохимических реакций.

Wolfram SystemModeler и Mathematica

Интеграция SystemModeler с системой Mathematica позволяет полностью управлять процессом моделирования, осуществляя любые виды анализа. Совместное использование двух систем существенно облегчает проектирование, управление моделями, создание анимации и визуализацию. Mathematica позволяет быстро создавать интерактивные отчеты или презентации для представления результатов проведенных исследований.

Вместе SystemModeler и система Mathematica предоставляют полный программный контроль над численным моделированием, делая возможными все виды проектирования и анализа.

Можно полностью контролировать процесс моделирования из документа системы Mathematica. Используя различные функции, можно задавать начальные условия, значения параметров и входные сигналы, проводить параллельно моделирование с различными наборами параметров.

Есть возможность проводить калибровку моделей на основе экспериментальных данных, подбирать значения параметров модели так, чтобы она наилучшим образом соответствовала эксперименту. Затем из документа системы Mathematica вы можете запускать процесс заново уже с оптимизированными параметрами.

Также существует возможность проводить анализ чувствительности системы по отношению к различным параметрам. Из наглядных графиков легко определяются параметры, оказывающие наибольшее влияние на модель.

Рабочая среда системы Mathematica спроектирована так, чтобы обеспечить максимальную эффективность рабочего процесса. При моделировании в системе автоматически создается документ, в который записывается вся последовательность команд. Такой документ можно распространять среди коллег или использовать в дальнейших разработках. Необходимо помнить, что любой документ, содержащий в себе разнообразные данные, результаты вычислений, а также элементы визуализации и анимации можно превратить в свободно распространяемый и платформонезависимый файл формата CDF.

Конкурентные преимущества

Основными конкурентами компании продукта WSM являются, безусловно, MapleSim и Simulink. Первым и наиболее важным преимуществом WSM над этими системами является его автономность. Приобретение системы Mathematica — лишь возможная опция, а не необходимое условие работы системы. В то время как для работы двух последних продуктов обязательно необходимо приобретение Maple и MATLAB, соответственно. Среди прочих преимуществ отметим возможность сочетания кода Modelica с концепцией drag-and-drop моделирования, а также возможность использования внешних функций языка Си. Еще одной существенной особенностью является возможность моделирования биохимических реакций. С более подробным описанием различий между данными системами можно ознакомиться по адресу http://www.wolfram.com/system-modeler/modeling-tools-comparison/#product-comparison.

Intel Cluster Studio XE 2013

Пакет Intel Cluster Studio XE содержит полный набор параллельных стандартов программирования на языке C / C++ и средств разработки Fortran, а также модели программирования, которые позволяют разработчикам эффективно разрабатывать, анализировать и оптимизировать HPC-приложения для масштабирования, ускорения и повышения производительности IA-совместимых процессоров, включая сопроцессоры Intel Xeon Phi.

Основные характеристики

- Интегрированный набор инструментов для разработки кластерных приложений.
- Высокопроизводительная библиотека MPI.
- Высокопроизводительные компиляторы C++ и Fortran и мощные модели параллельности для многоядерных процессоров.
- Анализ корректности и инструменты профилирования для приложений общего доступа и для распределенных и гибридных приложений.

Инструменты

Intel Cluster Studio XE включает в себя инструменты для разработки программ нового поколения, среди которых:

- Intel MPI Library — коммутационно-независимая MPI-библиотека с высоким уровнем масштабируемости и малым временем задержки;
- Intel Trace Analyzer and Collector — профилировщик производительности MPI-коммуникаций;
- компиляторы Intel C, C++ и Fortran — самые лучшие в отрасли компиляторы;
- Intel MKL и Intel IPP — высокопроизводительные библиотеки для математических примитивов и мультимедиа;
- Intel Threading Building Blocks и Intel Cilk Plus — модели параллельного программирования на основе потоков;
- Intel Advisor XE — помощник в организации многопоточности для разработчиков приложений на языках C/C++, C# и Fortran с использованием потоковой параллельности главного узла кластера;
- Intel VTune Amplifier XE — профилировщик производительности и потоков с возможностями MPI для каждого узла;
- Intel Inspector XE — средство для проверки памяти и потоков с возможностями MPI для каждого узла;
- Static Analysis — средство для поиска труднообнаруживаемых дефектов;
- Intel MPI Benchmarks — набор открытых программных кодов MPI и ядер тестовых программ кластера.

Комплект Intel Cluster Studio XE помогает разработчикам, работающим с высокопроизводительными кластерами, решать стоящие перед ними задачи, предлагая первый в своем роде всеобъемлющий пакет программных средств, дающий возможность разработчикам увеличить производительность и надежность кластерных приложений. Он сочетает в себе проверенные практикой наборы инструментов Intel для кластерных приложений и передовые средства компании Intel для анализа корректности организации потоков/памяти и профилирования производительности, что дает пользователю возможность разработки масштабируемых приложений для современных и будущих высокопроизводительных кластерных систем.

Основные характеристики

1. Интегрированный набор инструментов для разработки кластерных приложений

Великолепная производительность совместно используемых, распределенных или гибридных приложений обеспечивается ведущими в отрасли компиляторами, параллельными моделями и библиотеками компании Intel, обладающими передовыми оптимизациями производительности для систем высокопроизводительных кластеров с мультиядерными (на сегодняшний день) и многоядерными (в будущем) процессорами.

2. Ведущая в отрасли библиотека MPI

Библиотека Intel MPI Library обеспечивает новые уровни производительности, масштабируемости и гибкости приложениям, исполняемым на кластерах платформ Intel.

- Масштабирование до 120 тыс. процессов.
- Высокая производительность, малое время задержки.
- Независимость межкомпонентных соединений.
- Интеллектуальный выбор коммутируемой матрицы.
- Возможность настройки приложения и кластера.
- Поддержка Multirail InfiniBand.
- Поддержка Berkeley Labs Checkpoint Restart (BLCR).

3. Intel Trace Analyzer and Collector

Intel Trace Analyzer and Collector представляет собой мощный инструмент для определения корректности и режима работы MPI-приложения.

- Вывод на экран и описание поведения параллельных приложений.
- Оценка статистических данных профилирования и балансировка нагрузки.
- Анализ производительности подпрограмм или блоков кода.
- Изучение коммуникационного обмена и выявление «горячих» точек.
- Снижение времени на рабочую нагрузку.

4. Высокопроизводительные компиляторы и библиотеки языков C/C++ и Fortran

Компиляторы Intel C/C++ и Fortran имеют встроенные технологии оптимизации и поддержку многопоточности, что помогает создавать код, максимально эффективно работающий на новейших мультиядерных процессорах Intel и многоядерных архитектурах.

- Мультиядерные и многоядерные оптимизации.
- Поддержка распределенной памяти CAF (Co-Array Fortran).
- Расширенные возможности поддержки оптимизации, многопоточности и процессоров.
- Поддержка гибридных моделей параллелизма с MPI и моделей многопоточности, таких как OpenMP, Intel Cilk Plus и методов Intel TBB для повышения производительности приложений на кластерах.
- Передовые библиотеки Intel MKL и Intel IPP содержат множество процедур для повышения производительности и сокращения времени разработки.

Что нового

Повышенный уровень масштабируемости MPI. Intel MPI Library теперь масштабируется до 120 тысяч процессов, а Intel Trace Analyzer and Collector теперь масштабируется до 6000 процессов в целях поддержки разработки и развертывания приложений для дальнейшего роста производительности кластерных систем.

Библиотека Intel MPI Library теперь поддерживает версию 2.2 стандарта MPI. Поддержка Berkeley Labs Checkpoint Restart (BLCR) была реализована для повышения надежности длительных кластерных приложений в случае восстановления после сбоя, планирования и переноса процесса.

Получение воспроизводимых результатов. Преодолейте неассоциированные по своей природе характеристики результатов арифметических действий с плавающей запятой с помощью библиотеки Intel Math Kernel Library, а также специальных средств поддержки Intel для OpenMP и Intel Threading Building Blocks.

Intel System Studio

Углубленный анализ систем для разработчиков встраиваемых и мобильных приложений

Intel System Studio является исчерпывающим набором инструментов, который предоставляет в распоряжение разработчиков самые мощные средства для ускорения разработки систем следующего поколения.

Ключевые особенности

- Интегрированный набор программных инструментов.
- Отладчики и анализаторы, компиляторы и библиотеки.
- Проверенные инструменты и технологии для разработки и доставки встраиваемых и мобильных решений следующего поколения.

> «Intel Inspector (один из компонентов Intel System Studio) отличается интуитивно понятным пользовательским интерфейсом, который дал мне возможность обнаружить утечки памяти, ошибки доступа к данным, а также ошибки при работе с потоками, такие как гонки данных, используя всего один инструмент».
>
> Эшли Драйвер, разработчик решений и приложений, Altech Multimedia

Intel System Studio — это продукт, предназначенный для разработчиков встраиваемых систем, работающих на платформе Linux. Он поддерживает системы, основанные на процессорах Intel Atom, Intel Core и Intel Xeon и предоставляет следующие возможности:

- уменьшение времени, затрачиваемого на разработку и тестирование, благодаря углубленному анализу поведения программного и аппаратного обеспечения;
- улучшение стабильности кода с использованием инструментов отладки и анализа, дающих детальное представление о функционировании системы;
- увеличение энергоэффективности системы и ее производительности благодаря анализаторам, компиляторам и библиотекам.

Инструменты разработки Intel System Studio, сочетаемые с процессорными платформами Intel Atom, Intel Core и Intel Xeon, предоставляют разработчикам дополнительные конкурентные преимущества при разработке надежных встраиваемых и мобильных решений для широкого спектра рынков.

Компоненты Intel System Studio

Компонент	Описание
Intel VTune	Углубленный анализ ЦП с помощью компонента Amplifier и анализ систем на кристалле (SoC) для профилировки и настройки производительности и энергопотребления.
Intel JTAG Debugger (опционально)	Системный отладчик для систем на кристалле Atom, трассировка событий, вызывающих затраты системных ресурсов, ведение журналов, отладка на уровне исходного кода для прошивки UEFI, загрузчиков операционных систем и драйверов. Доступен в редакции Intel System Studio for Linux with JTAG Debugger.
GDB Debugger	Программный отладчик для быстрого поиска проблем на уровне приложений, позволяющий увеличивать стабильность системы, трассировать выполнение команд на уровне приложений и обнаруживать гонки данных.
Intel Inspector	Динамический и статический анализатор позволяет обнаруживать труднонаходимые ошибки работы с памятью и потоками.
Intel C++ Compiler	Ведущий в отрасли компилятор C/C++, включающий библиотеку параллельных вычислений Intel Cilk Plus для оптимизации производительности. Двоичный и исходный код совместим с компиляторами и кросс-компиляторами GCC.
Intel Integrated Performance Primitives	Библиотека с широчайшим набором программных компонентов для обработки сигналов, данных и мультимедиа.
Intel Math Kernel Library	Высоко оптимизированная линейная алгебра, быстрое преобразование Фурье (FFT), векторная математика и статистические функции.

Основные компоненты

Профилировщик энергопотребления Intel VTune Amplifier:

- обеспечивает углубленное исследование событий на уровне систем на кристалле, а также анализ операций центрального и графического процессоров;
- идентифицирует причины пробуждения процессора, таймеры, активированные приложением, а также прерывания на уровне аппаратного обеспечения;
- отображает частоты ядра центрального процессора, и события, которые пробуждают процессор на уровне исходного кода.

Профилировщик производительности Intel VTune Amplifier:

- анализирует события на уровне системы и SoC;
- отображает аппаратные события с помощью стеков вызовов, обеспечивает понижение затрат вычислительных ресурсов, а также обнаруживает «узкие места» в коде;
- предоставляет статистику по количеству вызовов и развернутую информацию для принятия решения об использовании параллельного либо линейного кода;
- демонстрирует результаты в исходном коде или в ассемблере без необходимости применения диагностического или тестового оборудования.

Отладчики GDB Debugger и Intel JTAG Debugger (опционально):

- многофункциональная отладка на системном уровне и уровне приложений для быстрого обнаружения проблем;
- углубленная отладка на уровнях процессоров, чипсетов и систем на кристалле с предоставлением полного описания содержимого регистров;
- отладка программного обеспечения ядра операционной системы, BIOS, UEFI, прошивок и драйверов на уровне исходного кода;
- инструменты для сверхбыстрой программной трассировки событий;
- усовершенствованный отладчик приложений, основанных на GDB.

Инструмент динамического и статического анализа Intel Inspector:

- улучшает надежность кода;
- отмечает ключевые ошибки в коде при работе с памятью и с потоками;
- быстро находит утечки памяти, некорректный доступ, а также гонки данных и взаимные блокировки;
- с большой скоростью и эффективностью выполняет статический анализ и анализ роста кучи для выявления критических дефектов кода;
- поддерживает удаленный сбор данных, точки останова для отладчика, а также прерывание при выбранных ошибках.

Контакты

За дополнительной информацией обращайтесь к менеджеру компании Softline Анне Курьяновой.

Пишите: AnnaKuri@softline.ru

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

Docflow Best Practice: отличный маркетинг с Adobe Creative Cloud

Docflow Best Practice существует на российском рынке уже более 7 лет. Компания занимается разработкой программных решений для управления электронными документами на платформе SAP, предоставляет услуги по внедрению и сопровождению своих продуктов. Программные решения создаются в специальном диапазоне имен /DFS/, зарегистрированном в SAP. С недавних пор разнообразные маркетинговые материалы Docflow Best Practice создаются при помощи инструментов Adobe Creative Cloud. Подробнее об этом нам рассказал Александр Тихомиров, специалист по маркетингу ООО «Докфлоу Бест Практис».

Бизнес-инструмент Adobe CC

В круг моих профессиональных обязанностей входит подготовка печатных материалов о разработках Docflow Best Practice, а также вывесок, баннеров для выставочных стендов и всевозможной сопутствующей продукции, например, визиток, фирменных пакетов и многого другого.

С подпиской Adobe Creative Cloud мы работаем совсем недавно. В мае этого года подписка была приобретена через компанию Softline, и мы очень довольны этим выбором.

> В Creative Cloud все приложения устанавливаются на ваше рабочее место и работают как обычно, просто скачиваются из облачного хранилища и активируются через Интернет. Каждые 30 дней ваш компьютер на сервере лицензирования будет проверять, действует ли Подписка, ведь она ограничена по времени.

Правда, пока мы используем не весь пакет приложений. Но это только вопрос времени, ведь чтобы полноценно пользоваться решением, важно для начала его хорошенько изучить. Сейчас, когда появляется свободная минута, я осваиваю новый для меня функционал.

Великолепная тройка

Самые часто используемые приложения — это Adobe Photoshop CC, Adobe Illustrator CC и Adobe InDesign CC. Кроме того, незаменимым инструментом для меня стал Adobe Flash Professional CC — приложение с простым пользовательским интерфейсом и широкими новыми возможностями.

Все сами

Наша компания не всегда готовила маркетинговые материалы самостоятельно «от и до». Ранее мы делали частичную верстку в Illustrator, а затем передавали ее на окончательную доработку сторонним дизайнерам. Такая организация процесса не всегда была удобна, т.к., например, часто приходится дополнять или исправлять информацию для листовок и буклетов, причем внести изменения требуется срочно.

Именно поэтому руководство компании приняло решение о том, что все задачи, связанные с печатной продукцией, мы будем решать сами. Так что теперь мы напрямую высылаем в типографию готовые макеты!

Красиво и информативно

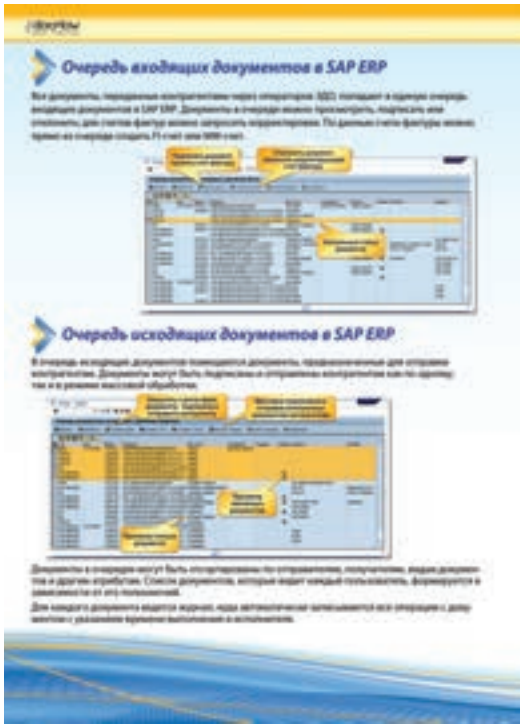
Я пока единственный сотрудник, ответственный за сегмент дизайнерских работ. Справляюсь в одиночку благодаря знанию решений Adobe. А работы достаточно, ведь у компании уже много разработанных программных продуктов, и каждый мы сопровождает набором печатных материалов. В каталоге Docflow Best Practice находятся 18 решений, которые успешно используются в более чем 30 компаниях в России, Украине, Казахстане, Белоруссии.

Материалы активно распространяем на специализированных выставках, демонстрируем на переговорах, всегда берем с собой в командировки. Поэтому качество продукции должно быть на высоте. Мы стараемся делать буклеты не только максимально информативными, но и красивыми, хорошо иллюстрированными.

Все просто!

Глубокое освоение функционала приложений — задача не всегда простая. К счастью, Adobe Photoshop CC мне знаком, так как уже много лет я использовал программу для собственных нужд, как любитель. Практически таким же привычным кажется и Adobe Illustrator CC, и только с Adobe Flash Professional CC возникают трудности, которые, я уверен, в скором времени будут полностью преодолены. А пока время от времени приходится изучать обучающие материалы от Adobe, например, видео о продуктах на русском языке, а также читать форумы пользователей. Я занимаюсь веб-дизайном сайта компании, и приложение Adobe Flash Professional CC нужно для создания всевозможной анимации. Сайт обновляется постоянно, и фронт работ непрерывно расширяется. Веб-контент должен быть привлекательным и запоминающимся — это неоспоримый факт — и анимация

docflow BEST PRACTICE
www.sapdocflow.ru



в этом отношении может удачно разнообразить интернет-страницу.

На будущее

Облачным хранилищем мы пока не пользуемся, такой необходимости нет, но вполне вероятно, что оно нам пригодится в будущем — точно так же, как приложение Adobe Premiere Pro CC, с помощью которого планируем монтировать видеоролики.

Если у вас возникнут вопросы, пожалуйста, обращайтесь в Центр компетенций Adobe: adobe@softline.ru

Наш сайт: http://adobe.softline.ru

CERTIFIED RESELLER Gold

CERTIFIED RESELLER Education Gold

Adobe Creative Cloud для рабочих групп

Выбирай:

Подписка на отдельные приложения

Ps Ai Id Ic Dw Mu Fl An In Pr Ae Au Sg Pl

Скидка 40%
до 31 декабря 2013 г.

Подписка на полный набор

Скидка 30%
до 31 декабря 2013 г.

Записи вебинаров Adobe ищите здесь:

Наслаждайся творчеством с Adobe® Creative Cloud™

http://adobe.softline.ru

MapInfo Professional 12.0

75 500 руб.

MapInfo Professional — полнофункциональная геоинформационная система (профессиональное средство для создания, редактирования и анализа пространственной информации). Интегрируется в качестве клиента в распределенные информационные системы на базе серверов: Microsoft SQL, Oracle, PostgreSQL/PostGIS и других. 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. Поддерживаются картографичесие web-сервера тайлов и сервера WFS и WMS.

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

MapInfo Spectrum Spatial

ЗВОНИТЕ

Spectrum — новая технологическая платформа для создания корпоративных геоинформационных систем, управления пространственными данными, оценки качества данных, решения различных аналитических и геоинформационных задач. Spectrum Spatial — один из компонентов платформы Spectrum, сервер инфраструктуры пространственных данных предприятия, предназначенный для совместной работы с картографической информацией неограниченного числа пользователей.

Платформа Spectrum, кроме пространственного модуля, может включать модули геокодирования, решения транспортных задач, интеллектуальной верификации данных и др.

Все компоненты платформы могут быть объединены в последовательности связанных процессов (Dataflow). Для создания dataflow, jobs и сервисов используется графический дизайнер.

Основанный на современной сервис-ориентированной архитектуре (SOA), Spectrum Spatial включает в себя все необходимые операции для создания, визуализации, анализа и редактирования пространственных данных в различных форматах (пространственные СУБД Oracle, MS SQL, PostGis и др., широкий набор файловых источников).

Большинство возможностей платформы Spectrum доступно через набор готовых web-сервисов SOAP и REST: Tile, Map, Feature, Geometry, UserManagment, сервисы по стандартам OGC (WFS, WFS, CSW).

Spectrum позволяет:

- создать и централизованно управлять инфраструктурой пространственных данных предприятия;
- с минимальными затратами интегрировать геоинформационные возможности в существующие системы предприятия (CRM, BI, ERP и др.), что поможет добиться совершенно нового уровня анализа и визуализации бизнес-информации;
- обеспечить доступ к пространственным данным широкому кругу пользователей посредством геопортала, с возможностью настройки и добавления собственной функциональности.

Компания ЭСТИ МАП

Официальный представитель Pitney Bowes Software Inc. в России и СНГ

Тел.: +7 (495) 627-76-37, +7 (495) 627-76-49

E-mail: sales@esti-map.ru, esti-m@esti-map.ru;
http://www.mapinfo.ru

Русская версия MapBasic 12.0

MapInfo MapBasic — 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 MapXtreme .NET

ЗВОНИТЕ

Программное обеспечение MapInfo MapXtreme 7.1 предназначено для создания настольных ГИС-приложений и геоинформационных систем в Интернете/интранете. Серверы пространственных данных, разработанные с помощью MapInfo MapXtreme 7.1, обеспечивают обслуживание неограниченного количества сетевых пользователей.

Единая платформа для разработки настольных, а также Интернет/интранет-приложений — одно из основных достоинств MapXtreme 7.1, существенно упрощающее разработку и сопровождение программного продукта.

MapXtreme 7.1 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 7.1 и возможности платформы .NET Framework, можно создавать картографические web-сервисы и интегрировать их в распределенную архитектуру своей системы. Для работы с пространственными данными MapXtreme 7.1 содержит готовые web-сервисы, взаимодействующие по протоколам WMS/WFS. MapXtreme 7.1 обеспечивает генерацию тайлов, работу с картами Google и Bing. Применение стандартных IT-протоколов, таких как OpenLS, GML, Microsoft.NET, ASP.NET, ADO.NET, SQL3 и др. позволяет существенно сократить затраты на внедрение и интеграцию приложений, разработанных на основе MapXtreme 7.1, в существующую IT-инфраструктуру компании.

MapXtreme 7.1 поддерживает работу с широким набором атрибутивных и пространственных источников данных, в качестве которых могут выступать СУБД (такие как Oracle и Microsoft SQL Server) и файлы различных форматов (например, MapInfo TAB, Shapefile).

SCAD Office®
www.scadsoft.com

ИНТЕГРИРОВАННАЯ СИСТЕМА **АНАЛИЗА КОНСТРУКЦИЙ**

SCAD

Система нового поколения, разработанная инженерами для инженеров и реализованная коллективом опытных программистов. Единая графическая среда синтеза расчетной схемы и анализа результатов обеспечивает широкие возможности моделирования расчетных схем от самых простых до самых сложных конструкций, удовлетворяя потребностям опытных профессионалов и оставаясь при этом доступной для начинающих.

Высокопроизводительные прямые и итерационный алгоритмы разложения матрицы жесткости позволяют решать задачи большой размерности (несколько миллионов степеней свободы) в линейной и геометрически нелинейной постановке. Расчеты на различные виды динамических воздействий включают решение таких задач как сейсмика, пульсация ветра, гармонические колебания, импульс, удар, а также прямое интегрирование уравнений движения.

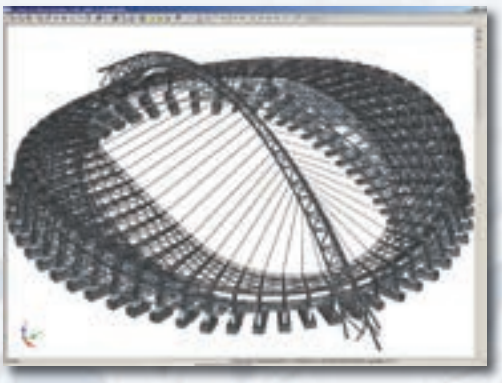
В состав комплекса включены модули анализа устойчивости, формирования расчетных сочетаний усилий, проверки напряженного состояния по различным теориям прочности, определения реакций от взаимодействия фрагмента схемы с остальной конструкцией, вычисления перемещений и усилий от комбинаций загружений, определения напряженно-деформированного состояния конструкции с учетом очередности возведения сооружения (монтаж), анализа амплитудно-частотных характеристик, учета усилий преднапряжения в элементах конструкции и др. Для совместного анализа нескольких вариантов расчетной модели реализован режим вариации моделей.

Библиотека конечных элементов позволяет учесть широкий диапазон свойств проектируемых конструкций при моделировании стержневых, пластинчатых, твердотельных и комбинированных систем.

Графические средства формирования расчетных схем включают наборы параметрических прототипов конструкций, позволяют автоматически сгенерировать сетку конечных элементов на плоскости, задать описания физико-механических свойств материалов, условий опирания и примыкания, а также нагрузок. Предусмотрена возможность сборки расчетных моделей из различных схем, а также широкий выбор средств графического контроля всех характеристик схемы. Реализован импорт геометрии расчетных схем из систем ALLPLAN, Revit Structure, ArchiCAD, Advance Steel, StruCAD, AutoCAD, 3D Studio, и др.

ООО "АВТОМАТИЗАЦИЯ ПРОЕКТНЫХ РАБОТ"

Модули подбора арматуры в элементах железобетонных конструкций учитывают требования различных нормативных документов (СНиП 2.03.01-84*, СНиП 52-01-2003, СП 63.13330.2012). Экспертиза и подбор сечений элементов стальных конструкций выполняется согласно СНиП II-23-81*, СП 16.13330.2011 и ДБН В.2.6-163:2010.



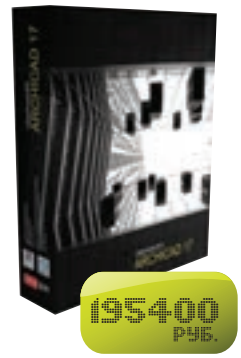
Сертификат соответствия:
РОСС RU.СП15.Н00276

Результаты расчета могут экспортироваться в табличном виде в редактор MS Word или электронные таблицы MS Excel. Графический анализ результатов расчета реализован в многооконной среде с возможностью одновременного анализа как различных фрагментов одной модели, так и различных моделей. Вывод перемещений включает реалистичное (с учетом профиля стержней и толщин пластин) отображение деформированной схемы, схемы прогибов, цветовую и цифровую индикацию значений перемещений в узлах, изополя и изолинии перемещений для пластинчатых и объемных элементов. Выполняется анимация форм колебаний для динамических и процесса деформирования — для статических загружений. Усилия в стержневых элементах представляются в виде эпюр и цветовой индикации с возможностью отображения на элементах максимальных значений выбранного силового фактора. Усилия и напряжения в пластинчатых и объемных элементах выводятся в виде изополей и изолиний в указанном диапазоне цветовой шкалы с возможностью одновременного отображения числовых значений факторов.

Адрес: 105082, Россия, г. Москва, Рубцовская набережная, 4, корп. 1, помещение VII. Тел/факс: +7 (499) 267 40 76; тел.: +7 (499) 940 88 27/29
E-mail: scad@scadsoft.ru

Graphisoft ArchiCAD 17

BIM — в каждой детали



Наиболее популярная среди архитекторов система автоматизированного проектирования, базирующаяся на технологии информационного моделирования здания (BIM), и предоставляющая все преимущества принципа открытого межплатформенного взаимодействия (OpenBIM). Работая с объемной моделью здания, проектировщики получают возможность детально прорабатывать свои проектные решения и свести число ошибок к нулю.

В любой момент можно получить согласованные между собой чертежи поэтажных планов, разрезы, фасады и спецификации, передать задания на разработку смежных разделов проектирования, подготовить презентационные материалы, включая виртуальное представление модели здания, облегчающее процесс согласования с клиентом проектных решений. ArchiCAD — это современные технологии, работающие на вас.

Новые возможности

Использование Строительных материалов дает возможность создавать виртуальную модель здания, максимально приближенную к реальным строительным процессам, а технология автоматического соединения элементов, базирующаяся на приоритете пересечения материалов, избавляет от рутины и позволяет генерировать узлы и детали непосредственно при работе над моделью. Все соединения автоматически учитываются в интерактивных каталогах и спецификациях, что позволяет существенно повысить их точность.

Реализация новой технологии создания 3D-сечений позволяет динамически изменять отображение модели в трехмерном пространстве без каких-либо ограничений.

ArchiCAD 17 демонстрирует существенный прирост производительности в сравнении со всеми предыдущими версиями, что особенно сильно проявляется при работе с большими моделями.

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. При этом изменения, вносимые на любом этапе, отображаются во всех частях проекта, что позволяет разработчику контролировать его целостность.

Новое слово в проектировании радиоэлектронных устройств

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.

Управление проектными данными и выпуск документации

«Интеллектуальное» управление данными, управление компонентами нового поколения, выпуск проектов с высоким уровнем интеграции благодаря использованию хранилища Satellite Vault или хранилищ, расположенных на AltiumLive.

Возможности 3D-проектирования

3D-визуализация позволяет получать в реальном времени реалистичные изображения платы, обеспечивает поддержку машиностроительных САПР, прямую связь с моделями в формате STEP и оперативную проверку зазоров и расстояний, просмотр конфигурации в режимах 2D и 3D, получение ортогональных проекций, а также наложение текстур двумерных и трехмерных моделей печатных плат.

Altium Designer 2013. Новые возможности

Предварительный просмотр документов проекта. Для удобства работы файлы проектов теперь можно объединять в рабочие группы (Workspace). В Altium Designer 2013 рабочая группа графически отображается в виде отдельной страницы.

Настройки прозрачности для слоев и объектов Редактора плат. При работе в Редакторе плат часто возникает необходимость отключить отображение некоторых объектов и наиболее загруженных слоев. Теперь вы можете в окне View Configuration раздела Transparently установить индивидуальные настройки прозрачности для всех примитивов каждого слоя платы.

Настраиваемая таблица отверстий. Эта таблица будет доступна всем подписчикам в одном из ближайших обновлений Altium Designer 2013. Данные в ней будут отображаться не только при выводе на печать, но и при просмотре платы в PCB-редакторе. Для добавления таблицы на лист чертежа будет использоваться специальная команда Drill Table.

Управление размерами и текстом для портов. Ранее размер порта в Редакторе схем был недоступен для редактирования, а при изменении шрифта для названия вывода надпись выходила за пределы графики порта. Это не позволяло оформлять схему в соответствии с ГОСТ. В Altium Designer 2013 оба параметра внесены в ряд пользовательских настроек.

Пользовательские настройки надписей выводов. В Altium Designer 2013 решены некоторые проблемы с Редактором схем, связанные с соответствием требованиям ГОСТ.

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 15 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.

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 проектирования молниезащиты зданий.

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 Технологические схемы — программный комплекс для создания принципиальных, технологических и монтажно-технологических схем установок и производств.

Model Studio CS Трубопроводы — программный комплекс, предназначенный для трехмерного проектирования внутриплощадочных, внутрицеховых и межцеховых систем трубопроводов, в том числе технологических трубопроводов, систем водо- и газоснабжения, отопления, канализации и других.

Model Studio CS Кабельное хозяйство — 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.

Корпоративный портал DeskWork 2013
Простой способ работать вместе

Корпоративный портал DeskWork — это готовое коробочное решение для организации коллективной работы на базе платформы Microsoft SharePoint 2013. Продукт объединяет традиционные инструменты управления информационным пространством, такие как работа с документами, обмен сообщениями и информирование, с новейшими коммуникативными технологиями — интерактивным общением, видеоконференциями. Это современное решение, которое организует внутреннее информационное пространство компании, решает конкретные бизнес-задачи и тем самым повышает производительность труда сотрудников за счет сокращения времени поиска и оптимизации рутинных процессов.

В сентябре 2013 года вышла очередная версия корпоративного портала DeskWork на платформе Microsoft SharePoint 2013. Пользователям представлены удобные и простые инструменты для коллективной работы и достижения различных бизнес-целей организации, таких как хранение информации, знаний и документов, средства удаленной работы сотрудников, создание и управление рабочими процессами компании, организация документооборота, эффективные корпоративные коммуникации и видеоконференции. В новой версии DeskWork 2013 Q3 завершен перевод продукта на платформу SharePoint 2013, работающую в классическом режиме, — на собственных серверах заказчиков. В DeskWork 2013 Q3 множество дополнений, направленных на повышение удобства работы пользователей и упрощение администрирования. Следующим шагом в развитии портала станет создание нового решения, которое будет работать на платформе Microsoft Office 365, в соответствии с современными тенденциями — повышением мобильности и ростом популярности облаков.

Корпоративный портал DeskWork служит единой точкой входа к информационным ресурсам компании и делает работу сотрудников более результативной за счет совместной работы с информацией, размещенной на портале, эффективной организации ее хранения и средств поиска. Автоматизация рутинных бизнес-процессов позволяет значительно сократить время на выполнение повседневных задач. Социальные модули DeskWork помогают организациям укреплять и развивать корпоративный дух.

В основе портала DeskWork лежит принцип логического распределения информации на функциональные блоки, каждый из которых выполняет полный цикл определенной бизнес-задачи. Такое разделение делает портал значительно доступнее для тех организаций, которым не требуется сразу сложный продукт. Компании могут приобретать блоки постепенно, наращивая функционал в соответствии со стоящими перед ними задачами.

Базовый блок как основа портала

Базовый блок DeskWork состоит из нескольких обязательных частей: Платформы, блока Информационных модулей и Справочника сотрудников. Его использование дает компаниям возможность быстро и просто начать использование средства коллективной коммуникации у себя в организации. При этом решается одна из первых задач портала — непрерывное и оперативное информирование сотрудников компании о важных мероприятиях, собраниях или событиях, о структуре компании и о сотрудниках, предоставление справочной информации, хранение документов.

Управляйте ресурсами и обязанностями

Блоки «Центр задач» и «Управление заявками» вместе и по отдельности реализуют задачи автоматизации рабочих процессов. «Управление заявками» позволяет ускорить и упростить выполнение ежедневных задач, такие как заполнение бланков, отправка запросов и заявок на рассмотрение и их исполнение. «Центр задач» — это система управления поручениями и задачами. Здесь в одном блоке можно видеть все задания и поручения исполнителя и контролировать их выполнение. Для руководителя или менеджера проектов это удобный инструмент постановки и отслеживания заданий.

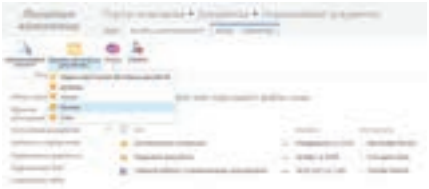
Эффективные коммуникации: соберите свою команду вместе!

Задачу эффективных коммуникаций успешно решают блоки «Универсальные сообщения» и «Видеоконференции». С их помощью можно существенно упростить деловое общение и взаимодействие сотрудников, провести дистанционное обучение, организовать семинары или презентации, виртуальные встречи с возможностью показа слайдов или других материалов.

Система позволяет проводить аудио- и видеопрезентации в режиме реального времени на 600 участников, планировать конференции в календаре, использовать текстовый чат, функции голосования или трансляции рабочего стола, поддерживает работу с современным кодеком h.264. Кроме того, в новой версии портала в Видеоконференции добавлены возможности работы на отдельном узле, просмотра записи при слабом интернет-канале, сделана более удобная навигация конференций из общего меню продукта.

Блок «Универсальные сообщения» помогают разослать сообщения сотрудникам по самым различным каналам связи — электронной почте, телефону, сообщением через сайт. Сообщение можно выслать одному человеку, группе или всем пользователям портала.

Экспресс-документооборот: все в строгом порядке



Экспресс-документооборот предоставляет для организаций функции регистрации и экспресс-согласования документов. Модули электронного документооборота безошибочно контролируют всю цепочку движения документов от создания до завершения, что предотвращает дублирование их обработки и позволяет значительно экономить время.

Кроме того, портал дает возможность использовать потоковый ввод документов в библиотеки SharePoint путем интеграции со сторонними системами. Это существенно упрощает и облегчает дальнейшую работу с документами.

Функция управления заместителями позволяет пользователю портала назначить при необходимости себе заместителя или секретаря и переложить на него часть задач или их контроль — на время отпуска, командировки или для экономии времени.

Постройте бизнес по своим правилам

Графический построитель бизнес-процессов — универсальная система автоматизации рабочих действий компании в удобном графическом редакторе в виде блок-схем. Для их создания не надо обладать навыками программирования или проходить специальную подготовку. Этот функционал можно использовать для задания произвольных маршрутов согласования, утверждения, сбора подписей, рассылки оповещений и так далее. В очередной версии портала многие механизмы теперь удобнее, а активности типа JOIN и SPLIT стали более «интеллектуальными», в том числе научились предсказывать некоторые возможные действия пользователей. Кроме того, в списке пользовательских рабочих процессов добавлены фильтры «Отображать рабочие процессы для текущего списка или сайта», а также добавлена возможность создания рабочего процесса для текущего списка.

Схема продажи

Любой из представленных блоков может быть использован на платформе SharePoint 2013 как самостоятельно, так и в комбинации с другими или в комплекте (Standard или Enterprise). Такая схема продажи блоков позволяет клиентам оптимизировать расходы, экономить материальные и временные ресурсы, подходить к решению конкретной бизнес-задачи, не распыляя силы и время на установку и адаптацию больших и часто сложных продуктов.

DeskWork Standard состоит из блоков DeskWork Base + «Управление заявками» + «Экспресс-документооборот» + «Универсальные сообщения». Комплект отлично подходит для максимально эффективной совместной работы, организации экспресс-документооборота и коммуникаций между сотрудниками, позволяющий управлять всем информационным пространством компании на современном уровне. К нему также можно докупить дополнительные блоки «Видеоконференции», «Бизнес-процессы» и «Центр задач». В состав каждой лицензии на DeskWork Standard входят пробные версии данных блоков: «Видеконференции» с 10 участниками, «Центр задач» с 20 первыми задачами и «Бизнес-процессы» с 10 активностями.

Комплект предназначен для Microsoft SharePoint Foundation 2013. Для работы достаточно иметь только Windows Server 2008R2/2012 (в состав этих лицензий Windows Server входит бесплатная платформа Microsoft SharePoint Foundation 2013), лицензии на другое ПО не требуются.

DeskWork Enterprise работает на дополнительно приобретаемой платформе Microsoft SharePoint Server 2013. Также предусмотрена возможность установки на бесплатную платформу Microsoft SharePoint Foundation 2013. DeskWork Enterprise включает в себя те же блоки, что и DeskWork Standard, но адаптированные и доработанные для обеспечения эффективной совместной работы с Microsoft SharePoint Server 2013.

Существует возможность использования корпоративного портала DeskWork как коробочного решения, так и удаленной работы в режиме облачного сервиса (SaaS).

Контакты

По вопросам функционала, состава комплектов продукта DeskWork, лицензированию и приобретению пишите на: deskwork@softline.ru или звоните: +7(495) 232-0023, доб. 0590

Скачать бесплатную версию на 25 пользователей на неограниченный срок или триал-версию на 30 дней можно на сайте www.deskwork.ru

Разработчик корпоративного портала DeskWork — ООО «Дэскворк», стратегическим партнером в вопросах продаж и продвижения корпоративного портала DeskWork является компания Softline.

Программа корпоративного лицензирования Nero 2014 Volume Licensing

Компания Nero удовлетворяет уникальным потребностям клиентов, предлагая инновационные и экономичные мультимедийные решения для записи дисков, архивирования, обеспечения безопасности и сохранности данных, а также контроля над ними. Возможности обеспечения защиты данных, а также суперсовременные инструменты для творчества делают продукты Nero лучшими для максимизации безопасности, эффективности и креативности вашего бизнеса.

Возможности корпоративных лицензий Nero 2014 для вашей организации

- Надежное и безопасное архивирование важных файлов без лишних трудозатрат.
- Обеспечение сохранности данных при помощи инструментов защиты, электронных цифровых подписей и дисков, защищенных паролем при помощи Nero SecurDisc.
- Восстановление потерянных или поврежденных данных с жестких дисков, компакт-дисков, DVD и флеш-карт, а также возвращение к их предыдущей версии.
- Быстрое получение высококачественных результатов при редактировании видео (инструмент Express & Advanced Video Editing).
- Воспроизведение DVD и Blu-ray для Windows 8 и 8.1.

Основные преимущества программы корпоративного лицензирования

- Легкий и экономичный способ лицензирования программного обеспечения Nero для вашей организации
- Снижение стоимости обновлений вплоть до 50%
- Регулярные бесплатные обновления гарантируют безопасность инфраструктуры
- Удобное администрирование на уровне организации с использованием одного лицензионного мастер-ключа (через средства MSI Package)
- Для международных организаций — поддержка 22 языков

Nero SecurDisc 3.0

SecurDisc 3.0 — это высокотехнологичное комплексное решение для защиты информации на дисках CD, DVD и Blu-ray, которое предоставляет многоуровневую защиту данных, музыки, фотографий и видеофайлов. С SecurDisc вы можете быть уверены в том, что ваши конфиденциальные данные пребывают в сохранности. Извлечь данные из поврежденного диска становится гораздо легче; защита паролем позволяет предотвратить несанкционированный доступ; функция проверки надежности источника данных благодаря верификации ЭЦП.

Функционал семейства продуктов Nero		Platinum	Premium	Standard
Запись дисков	Безопасная и надежная запись дисков	✔	✔	✔
	Легкое и удобное копирование дисков	✔	✔	✔
	Эффективное распределение данных между несколькими дисками	✔	✔	✔
Безопасность	Надежное хранение данных: восстановление случайно удаленных файлов на жестких дисках и флеш-картах или на поцарапанных оптических дисках.	✔	✔	✔
	Защита паролем: предотвращение несанкционированного доступа.	✔	✔	✔
	Электронная цифровая подпись: проверка надежности источника данных благодаря верификации ЭЦП.	✔	✔	✔
	Сканирование поверхности дисков: увеличение надежности при записи оптических дисков.	✔	✔	✔
Управление	Значительно усовершенствованное управление мультимедиа	✔	✔	-
	Быстрый поиск и систематизация фотографий, видео и музыки	✔	✔	-

Корпоративная лицензия Nero 2014 Standard — Burning ROM

- Запись и копирование файлов и папок на логические диски
- Флагманское приложение — Nero Burning ROM
- SecurDisc 3.0
- Защита паролем для корпоративных файлов и папок
- Добавление электронной цифровой подписи на оптические носители
- Совместимость с Windows 8
- Эффективное распределение данных между несколькими оптическими дисками

nero2014 VOLUME LICENSING

Программа корпоративного лицензирования Nero 2014 Volume Licensing представляет собой идеальное решение класса B2B, способное выполнить требования вашего предприятия.

Корпоративная лицензия Nero 2014 Premium

- Исчерпывающий набор инструментов для записи, редактирования, извлечения, конвертирования и воспроизведения мультимедиа
- Включает все функции и возможности Nero 2014 Standard — Burning ROM
- Конвертация презентаций PowerPoint для записи на диски DVD или Blu-ray и воспроизведения в формате HDTV
- Воспроизведение DVD для Windows 8
- Импортирование и конвертация цифрового или аналогового видео в формат Blu-ray Disc, DVD-Video и в большую часть файловых форматов
- Создание диско Blu-ray и DVD-Video профессионального качества, содержащих меню, подразделы, заголовки и многое другое

Корпоративная лицензия Nero 2014 Platinum

- Включает все функции корпоративных версий Nero 2014 Standard — Burning ROM и Nero 2014 Premium
- Возможность просмотра любых дисков Blu-ray, в том числе Blu-ray 3D
- Конвертация Blu-ray 3D в форматы видеофайлов 2D HD и SD
- Экспорт содержимого дисков Blu-ray в практически любой формат видео
- Поддержка стандарта 4K Ultra HD
- Создание потрясающего видео с возможностью добавления более чем 800 высококачественных эффектов и фильтров, в том числе, новых эффектов стабилизации видео и замедленного/ускоренного движения

ufi Approved Event

XIX МЕЖДУНАРОДНАЯ СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА

ВОЛГАСТРОЙЭКСПО

22-25 АПРЕЛЯ 2014 КАЗАНЬ

ВЫСТАВОЧНЫЙ ЦЕНТР ISO - 9001

КАЗАНСКАЯ ЯРМАРКА

Россия, 420059, г. Казань, Оренбургский тракт, 8,
Выставочный центр "Казанская ярмарка"
тел./факс: (843) 570-51-07, 570-51-11 (круглосуточный)
e-mail: d4@expokazan.ru
www.volgastroyexpo.ru, www.expokazan.ru

12+

SAP Sybase PowerDesigner

Инструмент моделирования архитектуры предприятия

Тот, кто хотя бы раз в жизни решал задачу проектирования базы данных, начиная с концептуальной модели, реализовывая логическую структуру, приводя модель к третьей нормальной форме, а затем создавая скрипты создания физических объектов базы данных, наверняка знаком с Sybase Power Designer, в первую очередь, как с инструментом именно моделирования баз данных, поддерживающим более 60 промышленных СУБД. Однако функциональные возможности этого инструмента гораздо шире, и область его применения — это реализация всей архитектуры предприятия.

PowerDesigner поддерживает все уровни проектирования архитектуры предприятия: стратегический, информационный, прикладной и инфраструктурный.

Стратегический уровень описывается с помощью организационных диаграмм, карт процессов, диаграмм градостроительного планирования и диаграмм бизнес-коммуникаций. Информационная составляющая традиционно состоит из концептуальных, логических и физических моделей, которые могут быть созданы для всех источников информации, существующих в организации. Прикладной уровень — это, прежде всего, диаграммы архитектуры приложений и сервис-ориентированные диаграммы. На инфраструктурном уровне реализуются диаграммы технической инфраструктуры.

Входящие в состав PowerDesigner средства моделирования архитектуры предприятия поддерживают стандартные методологии и нотации (имитационное моделирование с поддержкой BPMN, объектное моделирование UML 1.x и 2.0, нотации IE и IDEF1/x, методологии TOGAF, TODAF, ZACHMAN, ArchiMate), обеспечивают автоматизированное воссоздание моделей на основе кода, а также генерацию кода посредством настраиваемых шаблонов.

Цикл моделирования архитектуры предприятия в Sybase PowerDesigner.

Для повышения эффективности коммуникаций в PowerDesigner реализован корпоративный глоссарий, позволяющий вводить и определять единые термины для всех моделей и артефактов организации. Благодаря хранению и синхронизации определений в репозитории обеспечивается единообразное именование объектов и согласованность терминологии для всех участников процесса. Так же мастер составления отчетов, уже готовые шаблоны отчетов, отчеты в виде списка, мультимодельные RTF- и HTML- отчеты с полной поддержкой ссылок позволяют пользователям, не участвующим в моделировании, иметь непосредственный доступ к моделям и метаданным. Это упрощает взаимодействие между всеми участниками проектной группы, а синхронизация с продуктами Microsoft Office позволяет непосредственно ввести бизнес-пользователей в жизненный цикл анализа и проектирования.

StatSoft®
STATISTICA

Цикл выездных семинаров Академии Анализа Данных

Открытый семинар «Аналитические методы *STATISTICA*: ключ к повышению эффективности бизнеса»

- Эффективный анализ данных: основные подходы и передовые технологии
- Прогнозирование: технологии решения реальных задач
- Методы анализа больших объемов информации: технологии Data Mining
- Специальные решения для промышленности

Санкт-Петербург: 6 ноября, 10.00-15.00.

Участие **бесплатное**. Количество мест ограничено.
Предварительная регистрация обязательна.

Двухдневный курс «Искусство анализа данных: уникальный опыт StatSoft»

- Введение в анализ данных: сбор и организация данных, элементарные понятия статистики, основные статистические критерии, сравнение групп и др.
- Вероятностные распределения
- Визуализация: одномерный, многомерный, интерактивный визуальный анализ данных
- Основные методы анализа данных: построение зависимостей, регрессия, классификация, временные ряды и прогнозирование
- Case Studies
- Вопросы и ответы

Санкт-Петербург: 7-8 ноября, 10.00-14.00.

Roadshow StatSoft

Аналогичные мероприятия пройдут в других городах:

***Минск**: 18-20 ноября*
***Казань**: 3-5 декабря*

http://www.statsoft.ru

Регистрация

Полное расписание вебинаров и курсов смотрите на сайте:
www.statsoft.ru

Узнать стоимость курса, а также задать все интересующие вопросы можно, отправив запрос на адрес **academy@statsoft.ru** или позвонив по нашим телефонам.

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

Лицензирование SPLA в рамках программы по развитию cloud-сервисов Stack Data Network

Став SPLA-партнером Softline в 2011 году, компания Stack Data Network (ООО «СДН») обеспечивает своим клиентам доступ к виртуальным решениям на базе продуктов Microsoft и готовится активно использовать решения Microsoft при создании корпоративных облаков своих клиентов после запуска своей технологической площадки в Санкт-Петербурге.

Stack Data Network, специализирующаяся на эксплуатации и развитии отказоустойчивых дата-центров, предлагает своим клиентам комплекс экономически эффективных высококачественных услуг, обеспечивающих оптимальную IT-среду для стабильной работы и успешного развития бизнеса. Зарекомендовав себя в предоставлении услуг colocation и dedicated, Stack Data Network в ноябре 2011 года приняла решение включить в линейку своих бизнес-предложений услугу доступа к программным продуктам Microsoft и решениям на их основе по облачной модели лицензирования.

В соответствии с этой моделью конечный клиент получает доступ к продуктам Microsoft и решениям на их основе без привязки к конкретному рабочему ПК, без необходимости затрат на приобретение ПО в собственность и без издержек на внедрение и техподдержку решений. Именно такую модель потребления ПО позволяет предлагать конечным заказчикам программа лицензирования SPLA, официальным реселлером которой с 2010 года является Softline.

Нововведение, доступное благодаря SPLA, по достоинству оценили представители всех категорий клиентов Stack Data Network: от крупных компаний, специализирующихся на предоставлении бухгалтерских, банковских, финансовых услуг, до небольших территориально распределенных команд, разрабатывающих и сопровождающих онлайн-проекты. Наиболее востребованными продуктами из SPLA-линейки Stack Data Network среди конечных пользователей стали виртуальные сервера с удаленным доступом, реализованные на базе Windows Server и RDP, и виртуальные сервера с базой данных SQL. Кроме того, клиенты компании проявили интерес к виртуальным рабочим столам с настольным приложением Office и почте, построенной на Exchange Server.

Учитывая существующий положительный опыт работы по программе SPLA, компания Stack Data Network решила использовать SPLA-лицензирование в работе готовящейся к вводу в эксплуатацию технологической площадки в Санкт-Петербурге, которая позволит предложить клиентам компании все преимущества корпоративных облаков. Благодаря энергоэффективной инженерной инфраструктуре модульного дата-центра, гарантирующего безотказную работу практически неограниченного числа стоек, укомплектованных системами высокой плотности, клиенты получат надежную защиту от рисков и нештатных ситуаций на инфраструктурном уровне. В свою очередь, на уровне приложений качество и стабильность работы будет обеспечиваться гибким масштабированием программных решений, доступным благодаря программе SPLA.

Директор по развитию бизнеса Stack Data Network Сергей Зайцев отмечает: «Среди наших клиентов немало тех, кто заинтересован в предоставлении пользователям своей корпоративной информационной системы единого качества и доступности сервисов вне зависимости от времени и места формирования запроса. Потенциал, заложенный в cloud-решениях Microsoft, и инфраструктура модульного дата-центра позволит нам сформировать предложение, в полной мере отвечающее ожиданиям наших самых взыскательных клиентов».

«На наш взгляд, центральную роль в работе современного ЦОДа играет не только высокопроизводительное ИКТ-оборудование, но и соответствующие запросам клиента программные продукты и модели их лицензирования. Становясь SPLA-партнером, ЦОД может предложить своим клиентам наиболее гибкую и прогрессивную на сегодня модель потребления ПО: оплачивая только фактическое использование продукта в фиксированный период, клиент получает полноценное IT-решение с высокой масштабируемостью и возможностью доступа из любой точки, где есть Интернет. Подобное предложение, очевидно, повышает конкурентоспособность ЦОДа и его привлекательность для заказчиков, не требуя при этом начальных вложений в ПО и не предполагая обязательств по минимуму продаж», — комментирует партнерство Softline и Stack Data Network Игорь Балашов, директор по развитию бизнеса Softline.

SPLA-программа Microsoft для лицензирования ваших облаков

Благодаря программе лицензирования Microsoft Services Provider License Agreement (SPLA) вы сможете предлагать своим клиентам облачные сервисы на базе ПО Microsoft на основе помесячной оплаты. Программа SPLA — это единственная программа Microsoft, которая позволяет партнеру реализовать модель Pay-as-you-go, то есть оплачивать только то ПО, которое действительно использовалось конечным пользователем в тот или иной момент времени. Тем самым SPLA помогает зарабатывать партнеру и экономить конечному пользователю.

Как стать SPLA-партнером?

1. Зарегистрироваться в программе Microsoft Partner Network, а также на ресурсах Microsoft Pinpoint и Microsoft Hosting Community.
2. Заключить партнерское соглашение с корпорацией Microsoft по программе SPLA с помощью специалистов Softline.
3. Заключить договор с компанией Softline.

Квалифицированные специалисты Softline помогут вам пройти все этапы регистрации, оказав консультационную поддержку и выслав необходимые подробные инструкции.

Как это работает?

Заключив SPLA-соглашение, компания-партнер имеет право разворачивать необходимое ПО Microsoft на своем (или взятом в аренду) оборудовании и оказывать на его основе услуги своим клиентам. Оплата ПО производится помесячно.

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. 2500

Пишите: spla@softline.ru

Наш сайт: http://softline.ru/spla/

Программа SPLA подходит вашей компании, если вы:

- IT-подразделение холдинга, поддерживающее работу дочерних неаффилированных структур;
- телекоммуникационная компания;
- оператор связи;
- интернет-провайдер;
- поставщик услуг web-хостинга и аренды приложений;
- поставщик услуг ЦОДов;
- системный интегратор;
- независимый разработчик программного обеспечения, продающий свои решения по модели SaaS.

ИНФОКОММУНИКАЦИИ ОНЛАЙН

iTMan Desktop License Control

Инструмент учета, надзора и инвентаризации IT-инфраструктуры для крупных компаний

iTMan Desktop License Control — эффективное решение для инвентаризации IT-активов, надзора и управления лицензиями вне зависимости от размеров, географии филиалов и сложности структуры организации.

С помощью iTMan Desktop организация формирует ценную базу знаний о своих IT-активах, автоматизирует процессы управления, получает инструмент сбора, сведения и анализа данных, оптимизирует распределение лицензий и минимизирует расходы. Решение интегрирует данные используемых в организации систем учета активов, управления инфраструктурой (SCCM) и собственного агента, который устанавливается на компьютеры сети компании.

iTMan Desktop License Control — комплексное решение, содержащее необходимый функционал для инвентаризации программ и компьютеров компании и автоматизации управления лицензиями. iTMan Desktop может работать как самостоятельно, так и поддерживать интеграцию с различными системами инвентаризации и управления компании (1С, HelpDesk, системы документооборота и др.). iTMan Desktop License Control дорабатывается под специфические потребности заказчика. iTMan Desktop — идеальный выбор для тех компаний, которым не подходят стандартные решения и необходим индивидуальный подход.

Решение iTMan проводит инвентаризацию установленного программного обеспечения, осуществляет контроль и управление лицензиями, внесение данных о лицензиях на основе правоустанавливающих документов с информацией о сроках, типах, стоимости и с возможностью хранения электронных копий документов.

Особое внимание в решении уделяется автоматизации управления лицензиями. Учет, рациональное распределение, своевременное обновление лицензий обеспечивает стабильную работу подразделений и сотрудников компании, оптимальное расходование денежных ресурсов и положительно сказывается на финансовых результатах. iTMan Desktop License Control — платформа для организации управленческого учета компании. iTMan обеспечивает сбор всей необходимой информации для оптимизации управления и минимизации расходов на IT.

В настоящее время решение iTMan Desktop License Control успешно развернуто у ряда крупных российских компаний из различных отраслей (телеком, ТЭК, госсектор и др.). iTMan обеспечивает своевременное обновление версий решения. Ведутся новые проекты по внедрению и доработке iTMan Desktop у клиентов.

Есть вопросы? Обратитесь к Евгению Кирюшину, менеджеру по развитию проекта iTMan.
Пишите: Evgeniy.Kiryushin@softline.ru

федеральный деловой журнал

ТСР

тренды. события. рынки

Журнал который читают!

Только важные события

Нефть и газ
Энергетика
Строительство
Оборудование
Технологии
Услуги

www.tsr-media.ru

Бесплатная подписка на журнал по тел. (343) 371-19-18

Расписание курсов в Учебном центре Softline

Дистанционные курсы

Вендор	Код	Название курса	Даты
Citrix	CNS-205	Citrix NetScaler 10 Essentials and Networking (Основы и сетевая архитектура Citrix NetScaler 10)	25-29 ноября
Microsoft	20414	Реализация продвинутой серверной инфраструктуры	25-29 ноября
Microsoft	10751	Настройка и развертывание частного облака с использованием System Center 2012	25-29 ноября
VMware	VI5.1 ICM	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.1)	2-6 декабря
Microsoft	20336	Базовые решения Microsoft Lync Server 2013	2-6 декабря
Microsoft	20331	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря
Microsoft	10747	Администрирование System Center 2012 Configuration Manager (SCCM)	2-6 декабря
Microsoft	10750	Мониторинг и обслуживание частных облачных решений с использованием System Center 2012	2-6 декабря
Microsoft	10775	Администрирование баз данных Microsoft SQL Server	2-6 декабря
Microsoft	20411	Администрирование Windows Server 2012	2-6 декабря
Oracle	11gAPLS	Oracle Database 11g: Advanced PL/SQL	2-4 декабря
VMware	VW ICM 5.1	VMware View: Установка, настройка, управление (VMware View: Install, Configure, Manage v.5.1)	1-4 декабря
VMware	VC1-ARC	Vmware vCloud: Проектирование инфраструктуры облака Vmware Cloud (Vmware vCloud: Построение облака Vmware Cloud)	5-7 декабря
Microsoft	6234	Внедрение и управление Microsoft SQL Server2008 Analysis Services	2-4 декабря
Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Microsoft		Продажи Office 365	4 декабря
ITIL	ITILv3	ITIL — введение и основы управления IT-сервисами	2-4 декабря
Microsoft	10774-дист	Создание запросов в SQL Server 2012	2-6 декабря
Microsoft	20410-дист	Установка и конфигурирование Windows Server 2012	2-6 декабря
Microsoft	6419-дист	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	2-6 декабря
Cisco	ICND2-дист	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Citrix	CNS-300I-дист	Advanced Administration for Citrix NetScaler 9.0 Platinum Edition (Расширенное администрирование Citrix NetScaler 9.0)	2-6 декабря
Microsoft	20331-дист	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря

Еще больше баллов от Microsoft!

Вы можете получить дополнительные 100 баллов в свой актив на бесплатном образовательном портале MVA, сдав сертификационный экзамен или пройдя обучение в одном из авторизованных учебных центров Microsoft!

Как получить баллы за экзамен?

1. Выберите сертификационный экзамен, который вы хотите сдать. Для этого:

- ознакомьтесь с текущими спецпредложениями, чтобы пройти сертификацию по наиболее выгодным условиям;
- скачайте «Пути сертификации» с сайта Microsoft, чтобы узнать о самых современных сертификатах.

2. Зарегистрируйтесь на экзамен в центре тестирования Prometric.

3. Успешно сдайте экзамен! После этого по электронной почте вы получите ваш номер MCP ID, если у вас раньше его не было, и пароль для доступа к защищенному сайту для сертифицированных специалистов.

4. Зайдите на сайт https://mcp.microsoft.com/mcp и в разделе Transcript -> Share your transcript получите два кода: TranscriptID и AccessCode.

Если вы забыли или не получили свой MCP ID и не можете войти на защищенный сайт, обратитесь в Региональный Сервисный Центр Microsoft по тел.: 8-10-800-21591049 (звонок бесплатный, поддержка осуществляется на русском языке, звоните со стационарного телефона).

5. Перешлите эти два кода по адресу: mvarussite@microsoft.com.

6. В течение трех рабочих дней вам будет выслан ваучер MVA на 100 баллов, которым вы можете воспользоваться через персональную панель мониторинга, выбрав пункт «Воспользуйтесь своими ваучерами».

Как получить баллы за официальный курс?

1. Скачайте «Путеводитель по официальным курсам Microsoft», чтобы выбрать курсы по нужным технологиям.

2. Пройдите обучение в одном из авторизованных учебных центров.

3. Получите сертификат об окончании курса Microsoft международного образца и пришлите скан этого сертификата по адресу: mvarussite@microsoft.com.

4. В течение трех рабочих дней вам будет выслан ваучер MVA на 100 баллов, которым вы можете воспользоваться через персональную панель мониторинга, выбрав пункт «Воспользуйтесь своими ваучерами».

Microsoft

Вендор	Код	Название курса	Даты
Microsoft		Трехлетние контракты	5 декабря
Oracle	11gDBA1	Oracle Database 11g: Administration Workshop I	2-6 декабря
Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Microsoft	10774	Создание запросов в SQL Server 2012	2-6 декабря
Microsoft	10534	Планирование и проектирование решения Lync Server 2010	2-6 декабря
Microsoft	6419	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	2-6 декабря
Citrix	CNS-300I	Advanced Administration for Citrix NetScaler 9.0 Platinum Edition (Расширенное администрирование Citrix NetScaler 9.0)	2-6 декабря
Symantec	DP0157	Symantec Backup Exec 2012: Администрирование	2-6 декабря
Microsoft	20415	Внедрение инфраструктуры рабочих столов	2-6 декабря
Microsoft	20410	Установка и конфигурирование Windows Server 2012	2-6 декабря
Microsoft	20331	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря
Cisco	VPN V.2.0	Внедрение виртуальных частных сетей средствами Cisco ASA v.2.0 (Virtual Private Networks)	2-6 декабря
Microsoft		Трехлетние контракты	9 декабря
Microsoft	CCNAX	Создание сетей на базе оборудования Cisco: Ускоренный курс (Interconnecting Cisco Networking Devices: Accelerated)	9-13 декабря
Microsoft	6421	Конфигурирование и устранение неполадок сетевой инфраструктуры Windows Server 2008	9-13 декабря
Microsoft	6425	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	9-13 декабря
Cisco	ROUTE	Маршрутизация с использованием оборудования Cisco (Implementing Cisco IP Routing)	9-13 декабря
Oracle	11gSQL	Oracle Database 11g: SQL Fundamentals	9-13 декабря
Red Hat	RH-124	Red Hat Системное администрирование I	9-13 декабря
Microsoft	20411-веч	Администрирование Windows Server 2012	9-20 декабря
Microsoft	6419	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	9-13 декабря
Microsoft	10775-дист	Администрирование баз данных Microsoft SQL Server	9-13 декабря
Citrix	CXA-206I-дист	Citrix XenApp 6.5 Administration (Администрирование Citrix XenApp 6.5)	9-13 декабря
Microsoft	6425-дист	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	9-13 декабря
Microsoft	20411-дист	Администрирование Windows Server 2012	9-13 декабря
Microsoft	20416-дист	Создание инфраструктуры клиентских приложений	9-13 декабря

Бесплатное обучение от Microsoft

УЦ Softline проводит бесплатное обучение корпоративных клиентов в Москве и регионах на курсах Microsoft по программе Software Assurance.

Используйте ваучеры на обучение (Training Vouchers) по программе Software Assurance на любые курсы по Microsoft, за исключением курсов по Microsoft Office и продуктам Microsoft Dynamics. Software Assurance — это программа технической поддержки Microsoft, которая призвана помочь заказчикам корпоративных лицензий максимально эффективно использовать приобретенное программное обеспечение.

Компании, заключившие соглашение Software Assurance, получают ряд преимуществ и возможностей, которые можно использовать для бесплатного обучения своих сотрудников на официальных учебных курсах Microsoft в Учебном центре Softline.

Обучение будет оплачено Microsoft, если в вашей компании:

- есть не менее 50 лицензий Software Assurance по программам корпоративного лицензирования Open Value/Open Value Subscription или
- есть не менее 250 лицензий Software Assurance на Windows Pro или Office Pro в рамках программ Enterprise Agreement/Enterprise Agreement Subscription.

Как пройти обучение?

- Зарегистрируйтесь на портале Microsoft Volume License Services (MVLS). Укажите себя в качестве основного контактного лица при подписании лицензионного соглашения, в которое входит подписка на Software Assurance, и вы получите электронное письмо с приглашением.
- Зарегистрируйтесь на сайте MVLS с использованием Windows Live ID, а также создайте учетную запись MVLS.
- Введите код, указанный в приглашении, или номер соглашения из письма-уведомления и следуйте инструкциям по созданию учетной записи. В случае ввода номера соглашения вам потребуется ввести фамилию основного контактного лица на английском языке, как она была указана в соглашении.
- Перейдите в раздел «Преимущества Software Assurance» и выберите преимущество «Ваучеры на обучение». Нажмите кнопку «Активировать преимущество».
- Выберите курс, по которому хотите пройти обучение в УЦ Softline, а также слушателей, которые будут их проходить.
- После активации преимущества создайте на MVLS ваучеры для тренингов на необходимое количество дней с указанием слушателя, центра обучения и курса.
- Слушатель получает электронное письмо с подтверждением и ваучером, после чего регистрируется на тренинге. Ваучер используется для оплаты тренинга.

Расписание курсов в Учебном центре Softline

Москва

Вендор	Код	Название курса	Даты
Citrix	CNS-205	Citrix NetScaler 10 Essentials and Networking (Основы и сетевая архитектура Citrix NetScaler 10)	25-29 ноября
Microsoft	20414	Реализация продвинутой серверной инфраструктуры	25-29 ноября
VMware	VI5.1 ICM	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.1)	2-6 декабря
Microsoft	20336	Базовые решения Microsoft Lync Server 2013	2-6 декабря
Microsoft	20331	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря
Microsoft	10747	Администрирование System Center 2012 Configuration Manager (SCCM)	2-6 декабря
Microsoft	10750	Мониторинг и обслуживание частных облачных решений с использованием System Center 2012	2-6 декабря
Microsoft	10775	Администрирование баз данных Microsoft SQL Server	2-6 декабря
Microsoft	20411	Администрирование Windows Server 2012	2-6 декабря
Oracle	11gAPLS	Oracle Database 11g: Advanced PL/SQL	2-4 декабря
VMware	VW ICM 5.1	VMware View: Установка, настройка, управление (VMware View: Install, Configure, Manage v.5.1)	1-4 декабря
VMware	VC1-ARC	VMware vCloud: Проектирование инфраструктуры облака Vmware Cloud (VMware vCloud: Построение облака Vmware Cloud)	5-7 декабря
Microsoft	6234	Внедрение и управление Microsoft SQL Server2008 Analysis Services	2-4 декабря
Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
ITIL	ITILv3	ITIL — введение и основы управления IT-сервисами	2-4 декабря
Microsoft	10774-дист	Создание запросов в SQL Server 2012	2-6 декабря
Microsoft	20410-дист	Установка и конфигурирование Windows Server 2012	2-6 декабря
Microsoft	6419-дист	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	2-6 декабря
Cisco	ICND2-дист	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Citrix	CNS-300I-дист	Advanced Administration for Citrix NetScaler 9.0 Platinum Edition (Расширенное администрирование Citrix NetScaler 9.0)	2-6 декабря
Microsoft	20331-дист	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря
Oracle	11gDBA1	Oracle Database 11g: Administration Workshop I	2-6 декабря
Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Citrix	CNS-300I	Advanced Administration for Citrix NetScaler 9.0 Platinum Edition (Расширенное администрирование Citrix NetScaler 9.0)	2-6 декабря
Symantec	DP0157	Symantec Backup Exec 2012: Администрирование	2-6 декабря
Cisco	VPN V.2.0	Внедрение виртуальных частных сетей средствами Cisco ASA v.2.0 (Virtual Private Networks)	2-6 декабря

УЦ Softline возобновил авторизацию по обучению АСКОН

Более 5000 предприятий используют программное обеспечение АСКОН в России и за рубежом. Учебный центр Softline предлагает своим слушателям обучение основным программным продуктам компании. Мы снова рады обучать слушателей по направлению «Машиностроение».

- Курс «Трехмерное моделирование деталей и сборочных единиц в системе КОМПАС-3D». Цель курса — изучить основные понятия, инструменты и приемы работы в системе автоматизированного проектирования КОМПАС-3D, являющейся мощным средством создания трехмерных моделей деталей и сборок, с последующим построением сборочных и рабочих чертежей, созданием спецификаций, связанных с моделями и другими чертежами проекта.
- Курс «Проектирование и разработка конструкторской документации в системе КОМПАС-График». Позволит слушателям получить первоначальные навыки работы в программе, научиться использовать ее основные возможности. Вы получите необходимые знания, которые позволят немедленно приступить к самостоятельной работе и повысить эффективность своего труда.
- Курс «Администрирование системы трехмерного твердотельного моделирования КОМПАС-3D». Данный курс позволит слушателям получить представление о возможностях применения технологии адаптации КОМПАС-3D, об эффективных способах и приемах настройки системы под стандарты предприятия и собственные предпочтения пользователя.

Регионы

Город	Вендор	Код	Название курса	Даты
Новосибирск	Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	25-29 ноября
Новосибирск	Microsoft	2778	Создание запросов в Microsoft SQL Server 2008 с использованием языка Transact-SQL	25-27 ноября
Хабаровск	Microsoft	20412	Дополнительные службы Windows Server 2012	25-29 ноября
Хабаровск	Cisco	ROUTE	Маршрутизация с использованием оборудования Cisco (Implementing Cisco IP Routing)	25-29 ноября
Минск	VMware	VI5.1 ICM	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.1)	2-6 декабря
Новосибирск	Microsoft	20336	Базовые решения Microsoft Lync Server 2013	2-6 декабря
Новосибирск	Microsoft	20331	Базовые решения Microsoft SharePoint Server 2013	2-6 декабря
Новосибирск	Microsoft	10747	Администрирование System Center 2012 Configuration Manager (SCCM)	2-6 декабря
Новосибирск	Microsoft	10750	Мониторинг и обслуживание частных облачных решений с использованием System Center 2012	2-6 декабря
Нижний Новгород	Microsoft	10775	Администрирование баз данных Microsoft SQL Server	2-6 декабря
Нижний Новгород	Microsoft	20411	Администрирование Windows Server 2012	2-6 декабря
Пермь	Oracle	11gAPLS	Oracle Database 11g: Advanced PL/SQL	2-4 декабря
Екатеринбург	VMware	VW ICM 5.1	VMware View: Установка, настройка, управление (VMware View: Install, Configure, Manage v.5.1)	1-4 декабря
Екатеринбург	VMware	VC1-ARC	Vmware vCloud: Проектирование инфраструктуры облака Vmware Cloud (Vmware vCloud: Построение облака Vmware Cloud)	5-7 декабря
Омск	Microsoft	6234	Внедрение и управление Microsoft SQL Server2008 Analysis Services	2-4 декабря
Омск	Cisco	ICND2	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.2.0 Part 2)	2-6 декабря
Санкт-Петербург	Microsoft		Продажи Office 365	4 декабря
Хабаровск	ITIL	ITILv3	ITIL — введение и основы управления IT-сервисами	2-4 декабря
Екатеринбург	Microsoft		Трехлетние контракты	9 декабря
Екатеринбург	Microsoft	CCNAX	Создание сетей на базе оборудования Cisco: Ускоренный курс (Interconnecting Cisco Networking Devices: Accelerated)	9-13 декабря
Екатеринбург	Microsoft	6421	Конфигурирование и устранение неполадок сетевой инфраструктуры Windows Server 2008	9-13 декабря
Нижний Новгород	Microsoft	6425	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	9-13 декабря
Нижний Новгород	Cisco	ROUTE	Маршрутизация с использованием оборудования Cisco (Implementing Cisco IP Routing)	9-13 декабря
Новосибирск	Oracle	11gSQL	Oracle Database 11g: SQL Fundamentals	9-13 декабря
Новосибирск	RedHat	RH-124	Red Hat — Системное администрирование I	9-13 декабря
Новосибирск	Microsoft	20411-веч	Администрирование Windows Server 2012	9-20 декабря
Омск	Microsoft	6419	Конфигурирование, управление и поддержка серверов на базе Windows Server 2008 R2	9-13 декабря
Екатеринбург	Microsoft	6425	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	16-20 декабря

Microsoft Second Shot Бесплатная пересдача экзамена

Акция Microsoft «Второй шанс» возобновлена! Если вы не сдали экзамен, не расстраивайтесь! Пересдайте его бесплатно.

Акция действует до 31 мая 2014 года. Все подробности — у менеджеров УЦ Softline. Мы ждем вас!

Чтобы записаться на обучение, необходимо прислать запрос на edu@softline.ru или обратиться в отдел продаж Учебного Центра, позвонив по телефону: +7 (495) 232-00-65.

Адреса представительств в других городах России и странах СНГ вы можете найти на нашем сайте: www.edu.softline.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

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**

IT 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.

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.

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.

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.

@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**

ПОДПИШИСЬ НА ЖУРНАЛ LINUX FORMAT!

2013 LINUX FORMAT
Главное в мире Linux

Оформи в редакции подписку на печатную версию журнала и получи в подарок диск с архивом номеров, а также подписку на электронную версию издания в формате PDF.

ПОЛУГОДОВАЯ ПОДПИСКА 1230 РУБ.

Стоимость подписки Годовая — **2280 руб.**, полугодовая — **1230 руб.** без учета стоимости доставки.

Адреса и телефоны редакции **Санкт-Петербург**, Лиговский пр., 50, корп. 15, тел. **(812) 309-06-86**.
Москва, Красноказарменная ул., 17, тел. **(499) 271-49-54**.

Варианты доставки Почтой по России простой бандеролью — журнал доставляют прямо в почтовый ящик » Почтой по России заказной бандеролью — в почтовый ящик приходит извещение, номера выдают на почте » Курьером «ГНУ/Линуксцентра» по Москве и Санкт-Петербургу » Курьерской службой СПСР по России » В виде PDF-файлов для подписчиков электронной версии.

shop.linuxformat.ru

ZERO NIGHTS

2013 0x03

ZERONIGHTS

EPISODE 0x03

Международная
техническая конференция
по информационной
безопасности

Москва
7-8 ноября 2013

www.zeronights.ru

TWO DAYS
OF TECHNICAL SATURNALIA!

XXIII

Международная

КОНФЕРЕНЦИЯ

ВЫСТАВКА

ИТО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

2013

Место проведения:

Москва

Ленинские горы

Московский государственный университет имени М. В. Ломоносова

2-й учебный корпус
д. 1, стр. 52

6–7 ноября

Оператор конференции:
ООО НПП «БИТ про», тел.: +7 499 408-55-86
http://ito.su email: info@ito.su

— Ждем вас на ИТО-2013. Посещение бесплатное!
— Анонс программы размещен на сайте http://ito.su

ФОРУМ

БЕЗОПАСНОСТИ И СВЯЗИ

Казань

2013

4-6 ДЕКАБРЯ

Выставочный центр "Казанская ярмарка"
Россия, 420059, г. Казань, Оренбургский тракт, 8
Тел./факс: (843) 570-51-16, 570-51-11-круглосуточно
E-mail: pdv@expokazan.ru

16+

II Санкт-Петербургская
практическая конференция
и Фестиваль мобильных решений

TOP Mobile Conference 2013

Организаторы:

COMNEWS CONFERENCES, CIO, СоДИТ

Park Inn Pribaltiyskaya
20 ноября 2013 г.
Санкт-Петербург

«Зависимость бизнеса от ИТ становится больше, а значит, ответственность и значимость ИТ-директора выше. Задумывая два года назад TOP Mobile, мы уже находились в состоянии дефицита информации о возможностях рынка мобильных решений. Первая же конференция собрала большое количество участников и экспертов, доказав таким образом свою важность и актуальность на ИТ-рынке Северо-Запада».

Максим Белоусов,
председатель правления СоДИТ

Ключевые темы конференции 2013:

- Enterprise 2.0. в России и в мире. Взгляд CIO в будущее мобильного предприятия.
- BYOC-BYOD-BYOID-BYOIT. Эволюция задач CIO при переходе на BYOx-концепцию.
- Преимущества BYOD для корпоративного заказчика. Что делать с рисками?
- Как грамотно оценить эффективность реализации BYOD-стратегии в компании?
- Корпоративное vs. Гибридное облако. Выбор за CIO.
- Виртуализация данных. Как оптимизировать расходы на ИТ?
- Корпоративные облачные сервисы: что предлагает рынок? Как минимизировать затраты и риски?
- Механизмы контроля информационных потоков в облаках.
- Практика управления Big Data в корпорации. Готовы ли компании к работе с «большими данными»?
- MDM, EMM, MAM. Защита и управление мобильными устройствами в корпоративной среде.

Генеральный спонсор: МегаФон

Платиновый спонсор: Билайн Бизнес

Серебряный спонсор: SAPRUN

Бронзовый спонсор: ЛАНИТ

Спонсор регистрации: 1С-Битрикс

При поддержке: Альют, РАЭК, RUS+SOFT, Wireless, Отечественный софт

При участии: ARUBA networks

Официальный эксперт в области корпоративной информационной безопасности: eset

Участник выставки: CORTADO

Аналитический партнер: J'son & Partners Management Consultancy

HR-партнер: mozg.ru

Событийный партнер: Айти-Событие.рф

Мультимедийный партнер: digit

Стратегический партнер: Telecom Daily

Информационные партнеры: COMNEWS, СТАНДАРТ, Broadband & Satellite Newsletter, softline, ГЛОНАСС, Apps4All, CIO CLUB, ADVISER, Time of Cloud, Бизнес, IT talk, Mobile Info, Wireless, Mobile info, LINUX Format, Терра Daily, WP7 Geeks, iguides, ICT Online, SPB.RU, Деловой контакт

Для регистрации: +7 495 933 5483, conf@comnews.ru, www.comnews-conferences.ru/top2013

XIX Международный

ТБ ФОРУМ®

Технологии Безопасности

ВИДЕОНАБЛЮДЕНИЕ
CCTV, IP-РЕШЕНИЯ
ИНТЕГРИРОВАННЫЕ
СИСТЕМЫ

КОНТРОЛЬ ДОСТУПА
ОХРАНА ПЕРИМЕТРА
ОХРАННО-ПОЖАРНАЯ
СИГНАЛИЗАЦИЯ

АНТИТЕРРОР
ОХРАНА ГРАНИЦЫ
БЕЗОПАСНОСТЬ
НА ТРАНСПОРТЕ

ЗАЩИТА СВЯЗИ
И ИНФОРМАЦИИ
БИОМЕТРИЯ
СПЕЦТЕХНИКА

ПОЖАРНАЯ ЗАЩИТА
ПОЖАРОТУШЕНИЕ
БЕЗОПАСНОСТЬ
И ОХРАНА ТРУДА

11–14.02.2014

КРОКУС ЭКСПО / МОСКВА

КОНФЕРЕНЦИИ И СТРАТЕГИЧЕСКИЕ САММИТЫ ПРИ УЧАСТИИ ПРЕДСТАВИТЕЛЕЙ ФЕДЕРАЛЬНЫХ И РЕГИОНАЛЬНЫХ ОРГАНОВ ЗАКОНОДАТЕЛЬНОЙ И ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, **ЭКСПЕРТЫ МИРОВОГО КЛАССА** НА ТЕХНИЧЕСКИХ МАСТЕР-КЛАССАХ, НОВЫЕ СИСТЕМЫ И РЕШЕНИЯ В **ДЕМО-ЗОНАХ, СЕМИНАРЫ И ПРЕЗЕНТАЦИИ** НА СТЕНДАХ ВЕДУЩИХ РОССИЙСКИХ И ЗАРУБЕЖНЫХ **ПРОИЗВОДИТЕЛЕЙ И ПОСТАВЩИКОВ** ОБОРУДОВАНИЯ И РЕШЕНИЙ, КОЛЛЕКТИВНЫЕ ЭКСПОЗИЦИИ **ФСТЭК** РОССИИ И **ФСБ** РОССИИ

БЕСПЛАТНАЯ РЕГИСТРАЦИЯ НА WWW.TBFORUM.RU

Организатор Groteck Business Media

softline® 20 лет в IT

ЛУЧШИЕ МИРОВЫЕ ПРАКТИКИ
для эффективности вашего бизнеса

SAM
- Оптимизация стоимости лицензий
- Минимизация юридических рисков
- Соответствие ISO 19770-1

ITAM
- Автоматизация учета ИТ активов
- Сокращение совокупной стоимости владения TCO
- Обоснование инвестиций в ИТ

ITSM
- Объективная оценка качества ИТ-услуг и работы службы ИТ по ключевым показателям эффективности
- Качественное снижение бизнес-рисков, связанных с ИТ
- Оценка затрат на ИТ в зависимости от уровня ИТ-услуг

BI
- Прозрачность корпоративных данных для руководства
- Превращение массивов данных в полезную информацию
- Управление бизнес рисками

ИТ стратегия
- Обоснование направлений и бюджета развития ИТ
- Согласование ИТ с бизнесом
- Повышение эффективности и управляемости сотрудников ИТ службы

sam-info@softline.ru

+7 (495) 232 00 23 | www.softline.ru | info@softline.ru

115114, Москва, Дербеневская набережная д. 7, стр. 9 «Новоспасский двор»

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?

1-С: 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.

ABBYY

ABBYY Lingvo x5 Английский язык	
Домашняя версия (коробка)	1 100
ABBYY Lingvo x5 9 языков	
Домашняя версия (коробка)	2 200
ABBYY Lingvo x5 20 языков	
Домашняя версия (коробка)	3 870
ABBYY Lingvo x5 Английский язык	
Профессиональная версия	1 750
ABBYY Lingvo x5 9 языков	
Профессиональная версия	3 870
ABBYY Lingvo x5 20 языков	
Профессиональная версия	6 650
ABBYY FineReader 11	
Professional Edition (коробка)	4 790
ABBYY FineReader 10 Home Edition (коробка)	1 790
ABBYY PDF Transformer 3.0	1 490

ACDSYSTEMS

ACDSee 17 Single Unit	2 600
ACDSee Pro 7 Single Unit	6 500
ACDSee Photo Editor 6 Single Unit	1 950
FotoSlate v4.0 Single Unit	975
Canvas 14 Single Unit	19 500

ADOBE

Acrobat Standard 11 Russian	10 331
Acrobat Professional 11 Russian	15 496
Adobe InCopy CS6 8 Russian	10 905
Adobe Media Svr Professional 5 English	166 030
Adobe Media Svr Standard 5 English	36 732
Adobe Prelude CS6 1 English	14 758
Adobe Premiere Professional CS6 6 English	29 517
Adobe SpeedGrade CS6 6 English	36 896
Adobe TechnicalSuit 4 English	71 660
After Effects CS6 11 English	36 896
Audition CS6 5 English	12 913
Authorware 7 English	110 646
Coldfusion Builder 2 English	9 839
ColdFusion Enterprise 10 English	313 613
ColdFusion Standard 10 English	55 343
Contribute 6.5 English	7 379
Contribute Pub Servr 1.1 English	3 362
CS6 Adobe Design Standard 6 Russian	47 964
CS6 Design and Web Premium 6 Russian	70 102
CS6 Master Collection 6 Russian	95 929
CS6 Production Premium 6 English	70 102
Director 12 English	36 896
Dreamweaver CS6 12 Russian	14 758
FB Premium for PHP 4.5 English	27 877
FB Standard for PHP 4.5 English	13 938
Fireworks CS6 12 Russian	11 069
Flash Builder Premium 4.7 English	24 392
Flash Builder Standard 4.7 English	8 691
Flash Professional CS6 12 Russian	25 827
Framemaker 11 English	37 716
Framemaker Server 11 English	565 733
Freehand 11 English	14 717
Illustrator CS6 16 Russian	22 137
InDesign CS6 8 Russian	25 827
PageMaker Plus 7.0.2 English	19 514
Photoshop CS6 13 Russian	25 827
Photoshop Elements 11 Russian	2 132
Photoshop Extended CS6 13 Russian	36 896
Photoshop & Premiere Elements 11 Russian	3 157
Premiere Elements 11 Russian	2 132
RoboHelp Office 10 English	37 716
RoboHelp Server 9 English	75 431
Visual Communicator 3 English	14 717

AGNITUM

Outpost Firewall Pro Персональная (Single)	
1 лицензий в пакете 12 месяцев	
первая подписка (за лицензию)	899
Outpost Security Suite Pro Персональная (Single)	
1 лицензий в пакете 12 месяцев	
первая подписка (за лицензию)	1 199
Outpost Antivirus Pro Персональная (Single)	
1 лицензий в пакете 12 месяцев	
первая подписка (за лицензию)	899

ALTIUM

Altium Designer 2013 -	
Perpetual Standalone Licence	212 000
TDD (1 рабочее место) с локальным ключом	34 055
TDD (1 рабочее место) с активацией кодом	28 380
Altium Designer 2013 -	
Perpetual Standalone Licence ESD	180 000

ALT LINUX

Альт Линукс 6.0 Кентавр	3 000
Альт Линукс 5.0 Школьный Коробочная версия	3 500
Свободный офис. Выпуск 9 для Linux и Windows	
Коробочная версия	780
Simply Linux	300

AREALCONSALTING

ИКС Стандарт до 10 пользователей программа	7 500
ИКС Стандарт до 50 пользователей программа	32 800
ИКС Стандарт до 100 пользователей программа	51 500
ИКС для образовательных учреждений	
до 100 пользователей программа	5 500
Программный межсетевой экран ИКС	
(сертифицированная версия ФСТЭК)	
до 10 пользователей программа	14 000
Программный межсетевой экран ИКС	
(сертифицированная версия ФСТЭК)	
до 50 пользователей программа	51 100
Программный межсетевой экран ИКС	
(сертифицированная версия ФСТЭК)	
до 100 пользователей программа	81 300

ATTACHMATE

Reflection Standard Suite 2011 Licensed Unit	27 777
EXTRA! X-Treme Licensed Unit	27 777
Reflection Enterprise Suite 2011 Licensed Unit	41 173

AUTODESK

AutoCAD LT 2014 SLM	45 430
AutoCAD 2014 SLM	147 972
AutoCAD Architecture 2014 SLM	160 952
AutoCAD Civil 3D 2014 SLM	186 912
AutoCAD Design Suite Premium 2014 SLM	176 528
AutoCAD Design Suite Standard 2014 SLM	160 952
AutoCAD Electrical 2014 SLM	171 336
Autodesk Inventor LT 2014 SLM	37 642
AutoCAD Inventor LT Suite 2014 SLM	51 920
AutoCAD Map 3D 2014 SLM	160 952
AutoCAD Mechanical 2014 SLM	160 952
AutoCAD MEP 2014 SLM	160 952
AutoCAD Raster Design 2014 SLM	62 304
Autodesk 3D Studio Max 2014 SLM	109 032
Autodesk 3D Studio Max Design 2014 SLM	109 032
Autodesk Alias Automotive 2014 SLM	2 076 800
Autodesk Alias Design 2014 SLM	124 608
Autodesk Building Design Suite	
Premium 2014 SLM	207 680
Autodesk Building Design Suite	
Standard 2014 SLM	171 336
Autodesk Factory Design Suite	
Premium 2014 SLM	207 680
Autodesk Factory Design Suite	
Standard 2014 SLM	171 336
Autodesk Factory Design Suite	
Ultimate 2014 SLM	311 520
Autodesk Infrastructure Design Suite	
Premium 2014 SLM	207 680
Autodesk Infrastructure Design Suite	
Standard 2014 SLM	171 336
Autodesk InfraWorks 2014 SLM	155 760
Autodesk Inventor 2014 SLM	145 376
Autodesk Inventor Professional 2014 SLM	228 448
Autodesk Maya 2014 SLM	109 032
Autodesk MotionBuilder 2014 SLM	124 608
Autodesk Mudbox 2014 SLM	23 364
Autodesk Navisworks Manage 2014 SLM	186 912
Autodesk Navisworks Simulate 2014 SLM	62 304
Autodesk Product Design Suite	
Premium 2014 SLM	249 216
Autodesk Product Design Suite	
Standard 2014 SLM	176 528
Autodesk Product Design Suite	
Ultimate 2014 SLM	311 520
Autodesk Revit Architecture 2014 SLM	171 336
Autodesk Revit MEP 2014 SLM	171 336
Autodesk Revit Structure 2014 SLM	171 336
Autodesk Robot Structural	
Analysis Professional 2014 SLM	186 912
Autodesk Showcase 2014 SLM	31 152
Autodesk Simulation Mechanical 2014 SLM	480 260
Autodesk SketchBook Pro	
for Enterprise 2014 SLM	6 230
Autodesk Softimage 2014 SLM	93 456
Autodesk Product Design Suite Standard Product	
Visualization Tools 2014 SLM	145 376

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)

КОМПАС-3D V14

Простая в работе САПР с мощным функционалом, поддерживающая российские стандарты

93 000 руб.

Altium Designer 2013

Комплексная система автоматизированного проектирования электронных устройств

от 212 000 руб.

ABBYY Lingvo x5

Надежный помощник для профессионального перевода и изучения языков

1 750 руб.

DeskWork Standard

Максимально эффективная совместная работа, организация документооборота и коммуникаций

Звоните!

Panda Internet Security 2013

Защита от вирусов, шпионов, руткитов, хакеров, сетевого мошенничества

1 600 руб.

Intel C++ Composer XE

Набор компиляторов и библиотек для ускорения разработки многопоточного ПО

22 718 руб.

Microsoft Office 2013

Популярнейший офисный пакет с богатыми возможностями персонализации и доступа к «облаку»

9 417 руб.

Nero 12

Набор разнообразных программ для полноценной работы с мультимедиа

3 300 руб.

Corel Draw Graphics Suite X6

Надежное и универсальное программное решение для графического дизайна

18 560 руб.

Serif WebPlus X6

Легкий редактор для разработки профессиональных web-сайтов

2 925 руб.

Kaspersky Small Office Security

Высочайший уровень защиты от современных интернет-угроз для малого бизнеса

3 900 руб.

TrustPort Total Protection 2014

Мультидвижковый антивирус, предоставляющий всестороннюю защиту ПК от вирусов и утечек

Звоните!

Kerio Connect

Работа с почтой, календарями, адресной книгой в офисе и дома

19 316 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?

C-I: 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.

CA

CA ARCserve Backup r16.5 for Windows - Product plus 1 Year Value Maintenance	16 295

CAMBRIDGE SOFT

ChemBioOffice Ultra	139 425
ChemOffice Professional	116 675
ChemBioDraw Ultra	97 175
ChemDraw Professional	54 925
ChemBio3D Ultra	54 925
Strcut = Name Professional	54 925
ChemDraw Standard	35 425

CITRIX

Citrix XenApp Advanced Edition	11 148
Citrix XenApp Enterprise Edition	14 333
Citrix XenApp Platinum Edition	19 110
Citrix XenDesktop Enterprise Edition	7 166
Citrix XenDesktop Platinum Edition	11 148
Citrix XenDesktop VDI Edition	3 026

COREL

AfterShot Professional	3 977
CorelCAD 2013 ML (DVD Case)	23 290
CorelDRAW Technical Suite X6 ML (DVD Case)	42 369
CorelDRAW Graphics Suite X6 Russian	18 560
CorelDRAW Graphics Suite X6 - Small Business Edition Russian	33 408
PaintShop Professional X5 Russian	3 181
Painter 12	17 817
Corel PDF Fusion 1 Mini box	2 783
Photo & Video Bundle Professional X5	5 170
VideoStudio Professional X6 IE Mini-Box	2 757
VideoStudio Professional X6 Ultimate IE Mini-Box	3 447
VideoStudio Professional X5 Mini-Box	2 757
WinDVD Professional 11 Mini-Box	3 181
WinZip 17 Professional ML DVD	1 598
WinZip 17 Standard ML DVD	1 214

CSOFT DEVELOPMENT

Программное обеспечение MechaniCS 9, локальная лицензия	21 945
Программное обеспечение MechaniCS 9 Оборудование, локальная лицензия	32 965
Project Studio CS Архитектура v.1.8, локальная лицензия	32 965
Project Studio CS Конструкции v.5.1, локальная лицензия	49 400
Project Studio CS Фундаменты v.5.1, локальная лицензия	49 400

DESKWORK

DeskWork/foundation Base 100users	43 200
DeskWork Base	138 900
DeskWork/foundation Standard 100users	99 500
DeskWork/foundation Standard	320 000
DeskWork Enterprise	394 800
DeskWork/foundation RequestManagement for Base 100users	23 600
DeskWork RequestManagement	75 900
DeskWork/foundation DocumentFlow for Base 100users	46 300
DeskWork DocumentFlow	148 900
DeskWork/foundation UnifiedMessaging for Base 100users	16 100
DeskWork UnifiedMessaging forBase	51 900
DeskWork/foundation TaskManagement forBase/ Standard 100users Promo	12 400
DeskWork/foundation BusinessProcesses forBase/ Standard 100users Promo	37 300

ДОКТОР ВЕБ

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
Dr.Web Desktop Security Suite Комплексная защита 1...9 (за 1 лицензию в диапазоне на год)	644
Dr.Web Server Security Suite Антивирус 1...9 (за 1 лицензию в диапазоне на год)	666
Dr.Web Mail Security Suite Антивирус 1...9 (за 1 лицензию в диапазоне на год)	503

EMBARCADERO

RAD Studio XE5 Professional	58 468
RAD Studio XE5 Enterprise	97 468
RAD Studio XE5 Ultimate	129 968
RAD Studio XE5 Architect	146 218
Delphi XE5 Professional	32 468
Delphi XE5 Enterprise	81 218
Delphi XE5 Ultimate	113 718
Delphi XE5 Architect	129 968
C++Builder XE5 Professional	32 468
C++Builder XE5 Enterprise	81 218
C++Builder XE5 Ultimate	113 718
C++Builder XE5 Architect	129 968
InterBase XE3 Server	6 500
DB Power Studio XE, DEV Edition - Workstation	81 088

ENTENSYS

KinderGate Родительский Контроль одна лицензия на один компьютер	490

ESET

ESET NOD32 Антивирус Platinum Edition - лицензия на 2 года на 1ПК (BOX)	1 620
ESET NOD32 Smart Security - лицензия на 1 год на 3ПК (CARD3)	1 790
ESET NOD32 Smart Security Platinum Edition - лицензия на 2 года на 1ПК (BOX)	2 535
ESET NOD32 Smart Security - лицензия на 2 года на 1ПК (KEY)	2 535
Антивирус ESET NOD32 SMALL Business Pack newsale for 5 User (BOX)	5 500
Антивирус ESET NOD32 Business Edition newsale for 5 User	10 087

ESTIMAP

ГИС MapInfo Professional 12.0 для Windows (русская версия)	75 500
MapBasic 11.5 (русская версия) (язык программирования для среды MapInfo)	15 200
MapInfo Runtime 11.0 (рус..) (для разработчиков приложений в среде MapInfo)	41 700
MapXtreme 7.1 SDK (библиотека разработчика ГИС приложений, включая техническую поддержку на 1 год)	142 000
MapInfo MapX 5.01 (библиотека разработчика ГИС приложений и 1 пользовательская лицензия)	114 800
Vertical Mapper (англ.) 3.7 (трехмерное моделирование для ГИС MapInfo)	71 600
ПП АКО 4.2 Расширенный - 1 рабочее место	32 900

FAMATECH

Radmin 3.5 1 лицензия	1 250
Radmin 3.5 50 лицензий	38 000
Radmin 3.5 100 лицензий	63 500
Radmin 3.5 150 лицензий	90 000

FAST REPORTS

FastReport FMX Single	7 990
FastReport FMX Team	23 990
FastReport FMX Site	149 990
FastReport.Mono Single License	7 990
FastReport4 VCL Basic Edition Single License	690
FastReport4 VCL Standard Edition Single License	2 590
FastReport4 VCL Professional Edition Single License (Lazarus +)	3 590
FastReport4 VCL Enterprise Edition Single License (Lazarus +)	6 990
FastCube 2 VCL Standard Edition Single Licese	5 390
FastCube 2 VCL Professional Edition Single Licese	7 490
FastReport.Net Basic Edition Single License	2 990
FastReport.Net WinForms Edition Single License	9 590
FastReport.Net Win+WebForms Edition Single License	11 190
FastReport.Net Professional Edition Single License	15 990

FILEMAKER

FileMaker Professional 12.0 RTL	10 010
FileMaker Professional 12.0 ADV	16 705
FileMaker Server 12.0 RTL	33 443
FileMaker Server 12.0 ADV RTL	100 393

GFI

GFI FAXmaker including 1 year SMA from 5 to 9 Seats (per Seat)	5 175
GFI MailArchiver including 1 year SMA from 10 to 24 Seats (per Seat)	1 440
GFI MailDefense Suite including 1 year SMA from 10 to 24 Seats (per Seat)	1 373
GFI WebMonitor 2009 for ISA - UnifiedProtection for 1 year from 10 to 49 Seats (per Seat)	1 395

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?

I-N: 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.
GFI WebMonitor 2009 for ISA - WebFilter for 1 year from 10 to 49 Seats (per Seat)	810
GFI WebMonitor 2009 for ISA - WebSecurity for 1 year from 10 to 49 Seats (per Seat)	720
GFI WebMonitor 2009 - UnifiedProtection for 1 year from 10 to 49 Seats (per Seat)	1 395
GFI WebMonitor 2009 - WebFilter for 1 year from 10 to 49 Seats (per Seat)	810
GFI WebMonitor 2009 - WebSecurity for 1 year from 10 to 49 Seats (per Seat)	720
GFI LANguard including 1 year SMA from 10 to 24 Seats (per Seat)	1 440
GFI EndPointSecurity including 1 year SMA from 10 to 24 Seats (per Seat)	1 181
GFI Network Server Monitor including 1 year SMA from 10 to 24 Seats (per Seat)	4 455

GOLDEN SOFTWARE

Golden Software Didger 4 - 1 User	14 918
Golden Software Grapher 10 - 1 User	18 753
Golden Software MapViewer 7 - 1 User	9 549
Golden Software Voxler 3 - 1 User	18 370

GRAPHISOFT

ArchiCAD 17 (локальная)	195 400
ArchiCAD 17 (сетевая на 3 р.м.)	551 000

HYPERMETHOD

eLearning Server 4G версия базовая (на 1 сервер)	215 000
eLearning Server 4G (на 1 сервер)	315 000
Assessment Tools версия start-up (на 1 сервер)	255 000
eAuthor CBT v.3.3 версия базовая (на 1 рабочее место разработчика)	18 000
iNstructor v.2.0 версия базовая (на 10 рабочих мест обучаемых и 1 рабочее место преподавателя)	29 000

IDECO

Интернет-шлюз Ideco ICS Standard Edition - 10 concurrent Users	9 400
Интернет-шлюз Ideco ICS Enterprise Edition - 10 concurrent Users	17 500

INTEL

Intel Composer XE for Windows OS - Single Commercial (ESD)	38 968
Intel C++ Composer XE for Windows OS - Single Commercial (ESD)	22 718
Intel Visual Fortran Composer XE for Windows OS - Single Commercial (ESD)	27 593
Intel Cluster Studio for Windows OS - Single Commercial (ESD)	66 593
Intel Cluster Studio XE for Windows OS - Single Commercial (ESD)	95 843
Intel Integrated Performance Primitives for Windows OS - Single Commercial (ESD)	6 468
Intel Threading Building Blocks for Windows OS - Single Commercial (ESD)	16 218
Intel C++ Studio XE for Windows OS - Single Commercial (ESD)	51 968
Intel Visual Fortran Studio XE for Windows OS - Single Commercial (ESD)	61 718

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Anti-Virus 2014 Russian Edition. 2-Desktop 1 year Base Box	1 200
Kaspersky Internet Security Multi-Device Russian Edition. 2-Device 1 year Base Box	1 600
Kaspersky Small Office Security 2 for Personal Computers Russian Edition. 5-Workstation 1 year Base License Pack	3 900
Kaspersky Small Office Security 2 for Personal Computers and File Servers Russian Edition. 5-Workstation + 1-FileServer 1 year Base License Pack	5 900
Kaspersky Security для мобильных устройств Russian Edition. 10-14 PDA 2 year Base License	2 371,50
Kaspersky Security для виртуальных сред, Desktop Russian Edition. 10-14 VirtualWorkstation 2 year Base License	1 716
Kaspersky Anti-Virus for File Server Russian Edition. 1-FileServer 1 year Base License Pack	7 590
Kaspersky Anti-Virus for Windows File Server EE Russian Edition. 1-Node 1 year Base License Pack	14 490
Антивирус Касперского для систем хранения данных Russian Edition. 10-14 User 1 year Base License	737
Антивирус Касперского для систем хранения данных Russian Edition. 100-149 User 1 year Base License	475
Kaspersky Security для виртуальных сред, Server Russian Edition. 1-VirtualServer 1 year Base License	4 199
Kaspersky Security для почтовых серверов Russian Edition. 10-14 User 1 year Base License	1 385
Kaspersky Security для серверов совместной работы Russian Edition. 10-14 User 1 year Base License	1 109
Kaspersky Security для интернет-шлюзов Russian Edition. 10-14 User 1 year Base License	746
Kaspersky Security для виртуальных сред, Core Russian Edition. 1-Core 1 year Base License	13 983
Kaspersky Endpoint Security для бизнеса – Стартовый Russian Edition. 5-9 Node 1 year Base License	1 150
Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 10-14 Node 1 year Base License	1 581
Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 10-14 Node 1 year Base License	2 324
Kaspersky Total Security для бизнеса Russian Edition. 10-14 Node 1 year Base License.	4 715
Kaspersky Anti-Virus for xSP Russian Edition. 100-149 Mb of traffic per day 1 year Base Traffic Licence	295
Kaspersky Anti-Spam for xSP Russian Edition. 100-149 Mb of traffic per day 1 year Base Traffic Licence	295
Kaspersky Security for xSP Russian Edition. 100-149 Mb of traffic per day 1 year Base Traffic Licence	554
Kaspersky Systems Management Russian Edition. 10-14 Node 1 year Base License	1 937

KERIO

Kerio Connect Server (incl 5 users, 1 yr SWM) License	19 316
Kerio Control Server (incl 5 users, 1 yr SWM) License	11 007
Kerio Operator Server (incl 5 users, 1 yr SWM) License	6 230

LINUX CENTER

Звоните!

MAPLESOFT

Звоните!

MATHWORKS

Звоните!

MICROSOFT

Access 2013 Russian	4 322
Excel 2013 Russian	4 322
Exchange Enterprise CAL 2013 Russian OLP NL User CAL wo Services	1 625
Exchange Server Enterprise 2013 Russian OLP NL	137 866
Exchange Server Enterprise 2013 Single OLP NL	137 866
Exchange Server 2010 English 5 Client	56 259
Exchange Small Business 2007 Russian OLP NL	20 470
Exchange Small Business 2007 Single OLP NL	20 470
Exchange Small Business CAL 2007 Russian OLP NL User CAL	2 062
Exchange Small Business CAL 2007 Single OLP NL User CAL	2 062
Exchange Standard CAL 2010 English MLP 5 User CAL	19 547
Forefront UAG CAL 2010 Single OLP NL User CAL	509
Forefront UAG Server 2010 Single OLP NL	220 227
Forefront Identity Manager 2010R2 Single OLP NL	505 126
Forefront Identity Manager CAL 2010R2 Single OLP NL User CAL	606
InfoPath 2013 Russian OLP NL	5 997
InfoPath 2013 Single OLP NL	5 997
Lync 2013 Russian OLP NL	1 052
Lync 2013 Single OLP NL	1 052
Lync Server 2013 Russian OLP NL	124 075
Lync Server 2013 Single OLP NL	124 075
Lync Server Enterprise CAL 2013 Single OLP NL User CAL	4 205
Lync Server Plus CAL 2013 Single OLP NL User CAL	4 205
Lync Server Standard CAL 2013 Single OLP NL User CAL	1 221
DreamSpark Electronic Software Delivery (1 year)	3 282
DreamSpark Premium Electronic Software Delivery (1 year)	16 250
Office Home and Business 2013 English	9 417
Office Home and Business 2013 Russian No Skype	9 417
Office Home and Student 2013 English	3 200
Office Home and Student 2013 Russian No Skype	3 066
Office Professional 2013 English	17 107
Office Professional 2013 Russian No Skype	17 107
Office Professional Plus 2013 Russian OLP NL	17 290

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)

Autodesk Inventor 2014

Интуитивная среда для машиностроительного 3D-проектирования

от 145 376 руб.

Windows Server 2012 Standard

Серверная ОС, обеспечивающая беспрецедентную управляемость и доступность

52 184 руб.

Outpost Security Suite Pro

Проактивная комплексная защита от разнообразных угроз в сети

1 199 руб.

MathCAD 15 Professional

ПО для решения самых сложных инженерных и математических задач

54 900 руб.

Autodesk AutoCAD 2014

Система проектирования, для построения чертежей и внесения в них изменений

147 972 руб.

Norton Internet Security 2013

Интегрированный набор средств сетевой безопасности для комплексной защиты ПК

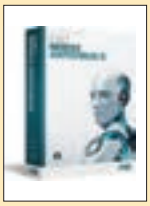
1 172 руб.

Microsoft Word 2013

Создавайте яркие документы, совместно работайте и наслаждайтесь чтением с экрана

4 322 руб.

ESET NOD32 Антивирус 6



Простое и надежное антивирусное ПО для базовой защиты домашнего компьютера.

1 080 руб.

Embarcadero RAD Studio XE5 Professional

Среда быстрой разработки native-приложений под Android и iOS для рабочих групп

Звоните!

Symantec Norton 360 v 6.0

Защита по всем направлениям: web, почта, IM-системы, P2P-сети и мобильные рабочие станции

1 546 руб.

Adobe Acrobat 11

Современное средство подготовки и распространения документов PDF

10 331 руб.

Oracle Database Standard Edition One

Доступная и многофункциональная база данных для СМБ

от 5 850 руб.

Kaspersky Anti-Virus 2014

Новейшая версия популярного решения для базовой защиты компьютера от интернет-угроз

1 200 руб.

Famatech Radmin 3.5

Быстрое и надежное ПО для удаленного управления ПК и администрирования сетей

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?

N-S: 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...

Наименование	цена, руб.
Office Professional Plus 2013 Single OLP NL	17 290
Office Standard 2013 Russian OLP NL	12 667
Office Standard 2013 Single OLP NL	12 667
OneNote 2013 Russian	2 594
Outlook 2013 Russian	4 322
PowerPoint 2013 Russian	4 322
Project 2013 Russian	24 746
Project Pro 2013 Russian	41 756
Project Server 2013 Russian OLP NL	192 809
Project Server 2013 Single OLP NL	192 809
Project Server CAL 2013 Russian OLP NL User CAL	6 598
Project Server CAL 2013 Single OLP NL User CAL	6 598
Publisher 2013 Russian	4 322
SharePoint Enterprise CAL 2013 Russian OLP NL User CAL	3 244
SharePoint Enterprise CAL 2013 Single OLP NL User CAL	3 244
SharePoint Server 2013 Russian OLP NL	231 370
SharePoint Server 2013 Single OLP NL	231 370
SharePoint Standard CAL 2013 Russian OLP NL User CAL	3 686
SharePoint Standard CAL 2013 Single OLP NL User CAL	3 686
SQL CAL 2012 Russian OLP NL User CAL	7 107
SQL CAL 2012 Single OLP NL User CAL	7 107
SQL Server Business Intelligence 2012 English 25 Client	641 076
SQL Server Business Intelligence 2012 Russian 25 Client	641 076
SQL Server Developer Edition 2012 English	1 982
SQL Server Developer Edition 2012 Russian	1 982
SQL Server Standard Edition 2012 English 10 Client	138 547
SQL Server Standard Edition 2012 Russian 10 Client	138 547
System Center Essentials Client ML 2010 English MLP	896
System Center Essentials Client ML 2010 Russian MLP	896
System Center Essentials Svr ML 2010 English MLP	5 586
System Center Essentials Svr ML 2010 Russian MLP	5 586
Visio Professional 2013 English	23 199
Visio Professional 2013 Russian	23 199
Visio Standard 2013 English	12 079
Visio Standard 2013 Russian	12 079
Visual FoxPro Professional 9.0 Win32 Single OLP NL	11 533
Visual Studio Pro 2012 English	22 839
Visual Studio Pro 2012 Russian	22 839
Visual Studio Ultimate wMSDN 2012 English Programs	608 657
Visual Studio Ultimate wMSDN 2012 Russian Programs	608 657
Win 8.1 Russian	4 762
Windows Professional 8.1 Russian	7 885
Windows Home Premium 7 English	4 762
Windows Home Premium 7 Russian	4 762
Windows Professional 7 English	7 885
Windows Professional 7 Russian	7 885
Windows Professional 8 Single OLP NL Legalization GetGenuine wCOA	5 946
Windows Ultimate 7 English	10 410
Windows Ultimate 7 Russian	10 410
Windows Server CAL 2012 English MLP 5 User CAL	9 486
Windows Server CAL 2012 Russian MLP 5 User CAL	9 486
Win Svr Essentials 2012 English	23 748
Win Svr Essentials 2012 Russian	23 748
Windows Server Standard 2012 English 5 Client	52 184
Windows Server Standard 2012 Russian 5 Client	52 184
Word 2013 English	4 322
Word 2013 Russian	4 322

NANOSOFT

nanoCAD 5.x (локальная)	20 000
nanoCAD BK 2.x (локальная)	46 200
nanoCAD Геоника 3.x (локальная)	65 000
nanoCAD Конструкции 3.x (локальная)	52 000
nanoCAD ЛЭП 1.x (локальная)	120 000
nanoCAD Механика 4.x (локальная)	23 100
nanoCAD ОПС 4.x, (локальная)	52 000
nanoCAD СКС 4.x, (локальная)	63 600
nanoCAD СПДС 4.x (локальная)	27 500
nanoCAD СПДС Железобетон 1.x (локальная)	52 500
nanoCAD Стройплощадка 3.x (локальная)	75 000
nanoCAD Схемы 2.x (локальная)	34 600
nanoCAD Фундаменты 3.x (локальная)	52 000
nanoCAD Электро 4.x (локальная)	80 800

NERO

Nero 12	3 300

ORACLE

Oracle Database Standard Edition One Named User Plus	5 850
Oracle Database Standard Edition One Processor License	188 500

Обратите внимание! Цена не включает стоимость MediaKit. Цены даны без учета стоимости поддержки. Стоимость указана за 1 лицензию. Минимальное количество лицензий уточняйте в компании Softline.

PANDA

Panda Antivirus Pro 2013 - Retail Box - на 3 ПК - (подписка на 1 год)	1 080
Panda Internet Security 2013 - Retail Box - на 3 ПК - (подписка на 1 год)	1 600
Panda Global Protection 2013 - Retail Box - на 3 ПК - (подписка на 1 год)	1 960

PRINT AUDIT

Print Audit 6 Analysis + Rules 100 лицензий	177 625
Print Audit 6 Analysis 100 лицензий	100 625
Print Audit 6 Recovery + Analysis 100 лицензий	240 625
Print Audit Suite 6 100 лицензий	402 500

ПРОМТ

PROMT 4U версия 9.0 ГИГАНТ	890
PROMT 4U версия 9.0 a-p-a + 80 словарей	720
PROMT 4U версия 9.0 ГИГАНТ + 110 словарей	970
PROMT Standard 9.0 a-p-a	3 600
PROMT Standard 9.0 ГИГАНТ	6 800
PROMT Standard 9.0 ГИГАНТ + 123 словаря	1 500
PROMT Professional 9.5 ГИГАНТ	18 000

PTC

Mathcad Professional - Individual	54 900
Mathcad Professional - Floating	Звоните!
Mathcad - Locked License 5 – Pack	Звоните!
Mathcad academic Locked License	Звоните!
Mathcad academic Floating License	Звоните!
Mathcad University Classroom - 15 Floating	Звоните!
Mathcad University Classroom – 25 Node-Locked	Звоните!

QUARK

QuarkXPress 9	32 468

SAP

Звоните!

SERIF

DrawPlus X5 English electronic License	2 730
MoviePlus X6 English electronic License	2 178
PagePlus X5 Russian electronic License	1 235
PagePlus X6 US/UK electronic License	2 925
PhotoPlus X5 Russian electronic License	2 438
WebPlus X5 Russian electronic License	2 438
WebPlus X6 US electronic License	2 925

SMARTLINE

DeviceLock Base (базовый компонент) 1-24 Licenses (per client)	1 500
DeviceLock 7.2 Компонент NetworkLock 1-24 Licenses (per client)	900
DeviceLock 7.2 Компонент ContentLock 1-24 Licenses (per client)	1 800
DeviceLock Endpoint DLP Suite 1-24 Licenses (per client)	4 200
DeviceLock Search Server 50K	11 000

SMARTSOFT

Traffic Inspector GOLD 5 Учетных записей	4 900
Traffic Inspector FSTEC 5 Учетных записей	5 900
NetPolice Office для Traffic Inspector на 1 год 5 Учетных записей	2 000
NetPolice School для Traffic Inspector на 1 год 10 Учетных записей	2 900

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?

S-Z: 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.
Kaspersky Gate Antivirus для Traffic Inspector на 1 год 5 Учетных записей	2 700
AquaInspector 2013 Server Foundation GOLD 10 Учетных записей	40 680
AquaInspector 2013 Server Foundation FSTEC 10 Учетных записей	45 480
AquaInspector 2013 Server Standard GOLD 10 Учетных записей	72 120
AquaInspector 2013 Server Standard FSTEC 10 Учетных записей	80 280

STARWIND

StarWind Enterprise CDP Edition with 1 Year Maintenance	30 721
StarWind Enterprise HA 2TB with 1 Year Maintenance	123 346
StarWind Enterprise HA 4TB with 1 Year Maintenance	185 096

STATSOFT

Statistica Base for Windows v.10 English / v.10 Russian Однопольз. версии	48 588
Statistica Advanced for Windows v.10 English / v.10 Russian Однопольз. версии	97 338
Statistica QC for Windows v.10 English / v.10 Russian Однопольз. версии	97 338
Statistica Advanced + QC for Windows v.10 English / v.10 Russian Однопольз. версии	116 838

SYMANTEC

Norton 360 6.0 Russian 1 User 3Licence 12MO 1C DRM KEY FTP	1 546
Norton 360 2013 Russian 1 User 3Licence 12MO 1C DRM KEY FTP	1 546
Norton AntiVirus 2013 Russian 1 User 3Licence	880
Norton INTERNET SECURITY 2013 Russian 1 User 3Licence	1 172
SYMC ENDPOINT Protection Small Business Edition Small Business Edition 12.0 Russian CD 5 User BNDL	
Business Pack BASIC 12 MO	3 370
SYMC Multi Tier Protection Small Business Edition 11.0.2 Russian 5User CD BNDLBP BASIC 12MO	10 613
SYMC Backup Exec 2012 Server Windows PER Server BNDL STD Licence EXPRESS Band S BASIC 12 MONTHS	26 702

TREND MICRO

Trend Micro Titanium Antivirus + 2014 1 Devices	1 353
Trend Micro Titanium Internet Security 2014 1 Devices	2 062

TRUSTPORT

TrustPort Antivirus 1 PC 1 Year	715
TrustPort Internet Security 1 PC 1 Year	975
TrustPort Total Protection 1 PC 1 Year	715
TrustPort USB Antivirus 1 User	302
TrustPort Tools 1 PC 1 Year	520
TrustPort eSign Pro 2.0 1 User	455
TrustPort Antivirus for Servers 1 Node 1 Year	6 305
TrustPort Security Elements Basic 5 Users 1 Year	5 038
TrustPort Security Elements Advanced 5 Users 1 Year	7 118
TrustPort Security Elements Premium 5 Users 1 Year	9 490
TrustPort Security Elements Ultimate 5 Users 1 Year	12 025

VENTA

VentaFax (бизнес-версия)	2 900
Venta4Net (1-линейный сервер)	3 600
Venta4Net Plus (1-линейный сервер)	5 500
На подпись! (Профессиональная версия)	2 800

VEEAM

Veeam Management Suite Standard for Hyper-V	58 143
Veeam Management Suite Enterprise for Hyper-V	72 443
Veeam Management Suite Standard for Vmware	58 143
Veeam Management Suite Enterprise for Vmware	72 443
Veeam Backup & Replication Standard for Hyper-V	31 655
Veeam Backup & Replication Enterprise for Hyper-V	47 515
Veeam Backup & Replication Standard for Vmware	31 655
Veeam Backup & Replication Enterprise for Vmware	47 515
Veeam Essentials Standard 2 socket bundle for Hyper-V	52 853
Veeam Essentials Enterprise 2 socket bundle for Hyper-V	65 826
Veeam Essentials Standard 2 socket bundle for Vmware	52 853
Veeam Essentials Enterprise 2 socket bundle for Vmware	65 826
Veeam Management Pack for Vmware	21 622
Veeam Smart Plug-In for Vmware	33 153
Veeam ONE for Hyper-V	29 055
Veeam ONE for Vmware	29 055

УСЛУГИ КОМПАНИИ SOFTLINE ПО ВИРТУАЛИЗАЦИИ

Jumpstart VMware View Upgrade (3 дня)	146 250
Jumpstart VMware vSphere (3 дня)	146 250
Jumpstart VMware View (3 дня)	146 250
Jumpstart VMware vSphere + View (5 дней)	227 500
Jumpstart VMware vCenter Site Recovery (4 дня)	323 375
Jumpstart VMware vSphere Upgrade (2 дня)	88 400
Jumpstart Business Continuity (1 день)	44 200
Jumpstart P2V Migration (1 день)	44 200
Jumpstart vCenter AppSpeed (1 день)	44 200
Jumpstart vCenter Chargeback (1 день)	44 200
Jumpstart CapacityIQ (1 день)	44 200
Jumpstart vCenter Lifecycle Manager (1 день)	44 200
Jumpstart vCenter Lab Manager (1 день)	44 200
Jumpstart vCenter Server Heartbeat	44 200

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА SOFTLINE И АРЕНДА ИНЖЕНЕРА

Аренда инженера-консультанта (стоимость за час работ)	6 500
Softline Incident Support - 10 инцидентов (на русском языке, eMail, телефон)	65 000
Softline Incident Support - 50 инцидентов (на русском языке, eMail, телефон)	260 000
Softline Premier Support - расширенная техническая поддержка по всем продуктам VMware, индивидуальные условия, eMail, телефон, выезды инженера	По запросу

VMWARE

VMware Workstation 10 for Linux and Windows, ESD	8 085
VMware ThinApp 4 Suite	173 388
VMware VirtualCenter Server 1 for VMware Server	34 678
VMware vCenter Server 5 Foundation for vSphere up to 3 hosts (Per Instance)	61 269
VMware vCenter Server 5 Standard for vSphere 5 (Per Instance)	204 708
VMware vSphere Storage Appliance (per instance)	143 234
VMware vCloud Automation Center for Desktop (25 Pack)	115 303
VMware vCloud Suite 5 Advanced	307 164
VMware vCloud Suite 5 Enterprise	471 094
VMware vCloud Suite 5 Standard	204 708
VMware vCenter Operations Manager 5.6 (Per OS Instance)	17 339
VMware vFabric Suite Advanced License for 1 VM, CPU, or AMI (Up to 2 vCPUs, Cores, or ECUs)	86 694
VMware vSphere 5 Standard for 1 processor	40 778
VMware ThinApp 4.x Client License 100 Pack	65 887
VMware View 5 Enterprise Bundle: 100 Pack	520 163
VMware View 5 Enterprise Add-on: 10 Pack	31 210
VMware View 5 Enterprise Add-on: 100 Pack	312 098
VMware View 5 Enterprise Bundle: 10 Pack	52 016

К каждой лицензии необходимо приобретать подписку\поддержку, за исключением позиций VMware Workstation 7 for Linux & Windows, ESD, VMware Fusion 3 for Mac OS X ESD

WINGATE

WinGate 7.x Standard 3 concurrent users	2 874
WinGate 7.x Professional 6 concurrent users	6 326
WinGate 7.x Enterprise 6 concurrent users	8 627

WOLFRAM RESEARCH

Звоните!

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)

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!

softline®

ДУМАЙТЕ О ЧЕМ-НИБУДЬ ПРИЯТНОМ,

ПОКА МЫ ДУМАЕМ О БЕЗОПАСНОСТИ ВАШЕЙ IT-ИНФРАСТРУКТУРЫ

СТО БР ИББС

PCI DSS

ОБЛАЧНАЯ БЕЗОПАСНОСТЬ

АУДИТ

Защита данных и коммуникаций

Тестирование на проникновение

Сетевая безопасность

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ И РИСКАМИ ИБ

Безопасность мобильных устройств и приложений

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

+7 (495) 232-00-23 | security.softline.ru | 8-800-100-00-23