КАТАЛОГ IT-РЕШЕНИЙ И СЕРВИСОВ ДЛЯ БИЗНЕСА

softline direct

МАЙ 2015

Cloud Software Hardware Services

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эффект синергии для веб-ресурсов

Аутентификация и управление доступом

Отечественная контентная фильтрация

Зачем нужен антифрод?

ДЕРЖИ ОБОРОНУ

| ГЛОБАЛЬНЫЙ ПОСТАВЩИК IT-СЕРВИСОВ И РЕШЕНИЙ | 8-800-232-00-23 | WWW.SOFTLINE.RU |

ISSN 2072-8735 (Print) ISSN 2072-8743 (Online)

T•Comm

Телекоммуникации и транспорт

Периодичность — 12 номеров в год.

Объём — от 64 полос. Формат 215 x 285 мм.

Тираж 5 000 экз.

Интернет-версия на русском и английском языках.

Журнал "T-Comm" рекомендован УМО по образованию в области телекоммуникаций в качестве дополнительного учебного материала для студентов высших учебных заведений по специальностям телекоммуникации и экономика.

Издание включено:

- **в перечень ВАК** (публикации в нём учитываются при защите кандидатских и докторских диссертаций);
- **в реферативный журнал и базу данных ВИНИТИ РАН** (сведения о нем публикуются в справочной системе по периодическим и продолжающимся изданиям Ulrich's Periodicals Directory);
- **в систему Российского индекса научного цитирования** (РИНЦ): eLIDRARY.RU.

Специальные выпуски журнала

"Информационные технологии на транспорте"

"Измерительное оборудование"

"Информационная безопасность"

"Радиочастотная идентификация"

"Цифровое телерадиовещание"

"Системы спутниковой навигации"

ИЗДАТЕЛЬСКИЙ ДОМ
МЕДИА
ПАБЛИШЕР
+7 (495) 957-77-43

В состав издательского дома «Медиа Паблишер» входят:

- дизайн-центр (полный цикл предпечатной подготовки книг и рекламной продукции);
- редакция периодических изданий (журнал «T-Comm – телекоммуникации и транспорт», журнал «Наукоемкие технологии в космических исследованиях Земли»);
- типография офсетной и цифровой печати с полным производственным циклом, ориентированная на оперативный выпуск высококачественной журнальной и листовой продукции.

WWW.MEDIA-PUBLISHER.RU

Уважаемые партнеры, коллеги, друзья!

С радостью представляем вашему вниманию майский выпуск специализированного журнала Softline Direct, полностью посвященный актуальным вопросам из сферы информационной безопасности.
За последнее время в области информационной безопасности произошли значительные изменения.
С одной стороны, мы наблюдаем бурное развитие современных информационных технологий — повсеместное проникновение веб-приложений и электронной коммерции, облачных сервисов, мобильных решений для удаленной работы.
С другой стороны, сложные методы проникновения в информационные системы, которые еще недавно могли использовать разве что представители спецслужб, стали доступны рядовым злоумышленникам, использующим их с целью финансового обогащения.
На данный момент мы можем констатировать, что имеющиеся методы обнаружения угроз, основанные на известных сигнатурах атак, перестали обеспечивать требуемый уровень защиты – нужны более интеллектуальные решения.
Средства защиты, установленные «из коробки», не работают, а идеология Plug & Secure окончательно ушла в прошлое — современные решения по обеспечению ИБ требуют постоянного внимания и настройки под IT-инфраструктуру конкретной организации и меняющиеся условия.
Кроме того, мы больше не можем доверять пользовательским устройствам где бы они не находились — внутри периметра организации или за его пределами.
Все это определяет новый виток противостояния, в котором нам необходимо выработать новые способы противодействия изменившимся угрозам.
Мы способны ответить на этот вызов — все средства, необходимые для этого, уже есть в нашем арсенале. Главное — не бояться осваивать новые области знаний, активнее обмениваться информацией внутри сообщества ИБ и доверять друг другу.
Надеюсь, новый выпуск нашего журнала вам в этом поможет!
Мы желаем вам приятного чтения и успехов в делах!

С уважением, руководитель департамента информационной безопасности
Вячеслав Железняков

Руки прочь от наших данных 18

В кризис вопросам снижениям издержек и повышения эффективности традиционно уделяется больше внимания. Одним из эффективных способов снижения расходов является противодействие утечкам данных.

Представляем вашему вниманию набор решений в области компьютерной безопасности компании AccessData, которые сочетает в себе компьютерную криминалистику, сетевую криминалистику, полномасштабный аудит данных, предоставляя единый интерфейс мониторинга

14

Информационная безопасность

На отечественном рынке технологии строгой аутентификации и единого доступа успешно реализует комплекс решений Indeed ID, предназначенный для аутентификации и управления доступом на предприятии.Он поддерживает широкий спектр различных технологий строгой аутентификации

12

СПЕЦИАЛЬНЫЙ ВЫПУСК

Каталог
IT-решений
и сервисов для
бизнеса
Softline
direct
МАЙ
2015-5(156)–RU

Учредитель: ЗАО
«СофтЛайн Трейд»

Издатель:
Игорь Боровиков

Главный
редактор:
Максим Туйкин

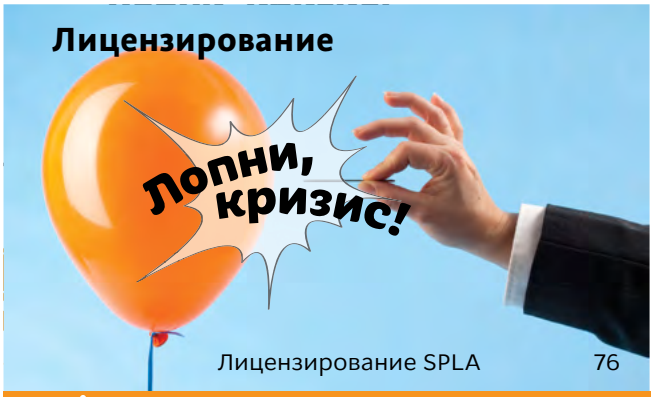
Выпускающий
редактор:
Лидия Добрачева

Редакторы:
Александра
Почечун,
Владимир
Цветков, Яна
Ламзина

Дизайн
и верстка: Юлия
Константинова,
Константин
Косачев,
Сергей Ососков

Над номером
работали:
Ольга Стрижко,
Юлия Лесничая,
Дарья Пивоварова,
Анна Любушкина,
Кристина
Меламед,
Екатерина
Болтаева,
Анастасия
Меркулова,
Анастасия
Подлепич, Ирина
Галактионова,
Анастасия
Ерастова, Татьяна
Татаринцева,
Ярослав
Михайлов,
Вячеслав
Железняков,
Анастасия
Лахтина, Дарья
Бекренева
и др.

Тираж: 60 000 экз.
Зарегистрировано
в Государственном
комитете РФ
по печати, рег. №
ПИ ФС77-23773



Global IT Solution and Service Provider

Портрет компании

Промышленность

Северсталь · РусГидро · КАМАЗ · УРАЛКАЛИЙ · БАЛТИКА · e.on · mondi business paper · Группа компаний ЭТАЛОН · helicon · АВК

А также
РУСАЛ • STADA CIS • Акрихин • Трансмашхолдинг • Совкомфлот • Sollers • GM-Avtovaz • СО ЕЭС • Трансмашхолдинг ОАО «Камчатскэнерго» • Вимм-Билль-Данн • МРСК Северного Кавказа

Розница, услуги

М.видео · ВИКТОРИЯ группа компаний · TUI · BDO · Снежная Королева · ile ИЛЬ ДЕ БОТЭ · Комус · РИГЛА · Inchcape · LEROY MERLIN

А также
Эльдорадо • Invitro • Рольф • Лаборатория Касперского • Хендэ Мотор СНГ • Славянка • ПИК • Роспечать • АББ • Комус • ГК «Форвард»

Банки и финансовые организации

СБЕРБАНК · ВТБ24 · Русский Стандарт БАНК · Райффайзен БАНК · ГАЗПРОМБАНК · Nb НОМОС БАНК · ЛокоБанк · АЛЬФА СТРАХОВАНИЕ · СОГЛАСИЕ · СОГАЗ СТРАХОВАЯ ГРУППА

А также
АТОН • ВТБ Страхование • Барклайс банк Россия • Газпром банк • Ренессанс Капитал • Бинбанк • Кредит Европа банк • ОПМ-банк • РВК • Автоваз Банк

20+
лет в IT

3 000+
поставщиков программного и аппаратного обеспечения

softline®

600+
технических специалистов

Телекоммуникации, СМИ, развлечения

НТВ · МТС · МегаФон · Ростелеком · TELE2 · 5 · Старт Телеком · BIGLION · BANKIR.RU · MTT.DOM

А также
Российская телевизионная и радиовещательная сеть • Всероссийская государственная телевизионная и радиовещательная компания • ТНТ • ПрофМедиа • Голос России • Yota

Госзаказчики

ROSOBORONEXPORT · РОСНАНО · Российская академия медицинских наук (РАМН) · МФТИ · Мострансавто · ИРВ

А также
Министерство связи и массовых коммуникаций РФ • Министерство образования и науки РФ • Управление делами Президента РФ • Сколково • Администрация города Иванова • Центральная базовая таможня • Администрация Ростова-на-Дону «Башкиргранждапроект» • ПИНРО • САФУ им. М.В. Ломоносова • Администрация Иркутска

1 300+
менеджеров по продажам

Нефтегазовая отрасль

Газпром · Транснефть · TATNEFT · РуссНефть · Зарубежнефть · ТомскНИПИнефть · Волгограднефтепроект · Гипровостокнефть

А также
Газпром Подземные хранилища газа • Газпром добыча шельф • Газпром Автоматизация • Нарьянмарнефтегаз • Мособлгаз • Уралтранснефтепродукт • «Аки-Отыр» • ОАО «Газпром газораспределение Белгород»

60 000+
корпоративных клиентов

Cloud Software Hardware Services

Почему заказчики выбирают Softline в качестве поставщика IT-решений и сервисов?

80 городов

1 Весь спектр решений и сервисов

Softline — лидирующий глобальный поставщик IT-решений и сервисов. Мы предлагаем комплексные технологические решения, лицензирование программного обеспечения, поставку аппаратного обеспечения и сопутствующие IT-услуги. Наш портфель решений содержит разнообразные облачные услуги: публичные, частные и гибридные облака на базе собственной облачной платформы Softline.

2 Сильный игрок с безупречной репутацией

Клиенты Softline — это 60 000 частных и государственных организаций всех масштабов — от крупных корпоративных заказчиков до среднего и малого бизнеса. Более 1300 менеджеров по продажам и 600 инженеров и технических специалистов обслуживают наших клиентов и помогают им выбрать оптимальные IT-решения. По итогам 2013 финансового года Softline достигла оборота около $1 млрд, а за последние 10 лет совокупный среднегодовой темп роста продаж (CAGR) составил 40%.

Статусы Softline

Microsoft Partner

- Gold Messaging
- Gold Business Intelligence
- Gold Small Business
- Gold Collaboration and Content
- Gold Management and Virtualization
- Gold Communications
- Gold OEM
- Gold Software Asset Management
- Gold Volume Licensing
- Gold Mobility
- Gold Server Platform
- Gold Devices and Deployment
- Gold Application Integration
- Gold Midmarket Solution Provider
- Gold Customer Relationship Management
- Gold Identity and Access
- Silver Application Development
- Silver Learning
- Silver Hosting
- Silver Project and Portfolio Management

KASPERSKY ENTERPRISE PARTNER

ORACLE Platinum Partner

AUTODESK. Gold Partner

HUAWEI

EMC² BUSINESS PARTNER

cisco Premier Partner

vmware PARTNER PREMIER SOLUTION PROVIDER

MathWorks

Код Безопасности

27 стран

3 Место действия — весь мир

Softline работает на рынках России, СНГ, Латинской Америки, Индии и Юго-Восточной Азии. Компания представлена в 80 городах 27 стран мира. За более чем 20 лет успешной деятельности на IT-рынке нам удалось накопить уникальный опыт работы на крупных, динамично развивающихся рынках.

4 Крепкий союз с производителями

Компания Softline является партнером более чем 3000 производителей программного и аппаратного обеспечения, имеет высочайшие партнерские статусы всех ключевых вендоров. Для них мы предоставляем уникальный канал маркетинга и продаж, охватывающий все страны нашего присутствия.

5 Заказчик — в центре внимания

Softline — это клиентоориентированная компания: мы всегда находимся на стороне клиента и предлагаем решения, наилучшим образом решающие его задачи, вне зависимости от бренда.

Эффект синергии

Только сочетание разных подходов к ИБ обеспечивает полную безопасность веб-ресурсов

Насколько часто рекомендуется проводить аудит безопасности сайтов?
Для банков периодичность проверок прописана в стандарте PCI DSS. Но, кроме того, надо учитывать жизненный цикл ресурса: насколько часто он обновляется и как часто выпускаются патчи.

Веб-сайт — это лицо компании, а веб-приложения и веб-порталы предоставляют важнейший функционал и конкурентные преимущества. Антон Афанасьев, руководитель направления прикладных решений департамента ИБ управления сервисов компании Softline, рассказывает об основных проблемах веб-безопасности и их решениях.

С чего все начиналось

10–15 лет назад большинство сайтов компаний в Интернете выполняли функцию «визитных карточек». Они были написаны на языке HTML и содержали статичную информацию для посетителей. Однако с появлением новых языков программирования ресурсы стали содержать меньше статического и больше динамического контента.

Пользователи стали вносить данные на веб-ресурсы, и в них начали появляться уязвимости, которые можно эксплуатировать. Все это стало стимулом развития инструментов обеспечения веб-безопасности.

Для каких компаний важнее всего защита веб-ресурсов?

Раньше всех попали в зону риска банки: они создавали системы ДБО (дистанционного банковского обслуживания), с помощью которых пользователи могли авторизоваться и выполнять платежи и денежные переводы. Такие возможности не могли не заинтересовать злоумышленников – они начали искать уязвимости в этих ресурсах, стремясь выполнять неавторизованные платежи от лица других людей. Поэтому первыми защитой веб-ресурсов стали заниматься банки, и сейчас они в большинстве своем уже имеют несколько уровней защиты. Затем к ним присоединились телекоммуникационные операторы и прочие организации, которым требуется защищать свои личные кабинеты.

Новая тенденция — защита электронных торговых площадок и бирж. Там тоже велики риски мошеннических операций. Возникает спрос на защиту систем дистанционного обучения, которые широко внедряются в российских вузах. В них пользователи могут получать контент, сдавать тесты, и подмена информации может привести к искажению результатов. Кроме того, у государственных организаций, особенно коммунальных служб и энергетических компаний, возникает потребность в обеспечении безопасности систем личных кабинетов. Они работают по принципу «единого окна», активно развиваются во многих городах и регионах. Они позволяют оплачивать услуги и штрафы, а там, где есть денежные переводы, возникает угроза взлома.

Какие бывают уязвимости у веб-приложений

Некоторые уязвимости могут привести к так называемому дефейсу сайта — на нем размещается информация, порочащая владельца.
Другой тип уязвимостей приводит к загрузке на ресурс вредоносного контента. Пользователи, которые посещают этот ресурс, заражаются вирусами. Injection-атаки ставят своей целью похитить информацию с веб-ресурса. Учетные записи, электронные адреса и телефоны могут применяться для целевых атак или для рассылки спама, вирусов и т.д.
Веб-порталы могут послужить для хакеров точкой входа в корпоративную сеть. На портале они создают исходную точку атаки, а с нее уже ведется атака на инфраструктуру.

Как же обеспечить безопасность сайтов?

Многие интеграторы предлагают WAF (Web Application Firewall) как основное средство решения проблем с веб-безопасностью. WAF — это продукт, который анализирует данные, передаваемые на ресурс, выявляет атаки на него и несанкционированные действия.
WAF действительно может функционировать в режиме «по умолчанию», предотвращая основные атаки. Веб-файервол сокращает время реакции на инцидент: он сигнализирует о любом простейшем сканировании портов или переборе известных уязвимостей и заблокирует его.
Со временем содержимое и функционал сайтов меняется, поэтому нужно следить за правильностью функционирования WAF и регулярно проверять безопасность веб-ресурсов.

Анализ уязвимостей и пентесты

Два основных вида услуг по обеспечению безопасности веб-сайтов — это тесты на проникновение (пентесты) и услуги по проверке на уязвимости. Немногие компании предоставляют две эти услуги без «перекоса» в сторону одной из них. Softline имеет опыт выполнения комплексных проектов, включающих и тесты на проникновение, и поиск уязвимостей с помощью нашей исследовательской лаборатории. Результаты проверки позволяют наиболее точным образом настроить WAF для защиты веб-ресурса.

Внедрение WAF — не панацея: любой инструмент защиты нужно обслуживать, поддерживать и настраивать.

Уязвимости нулевого дня: что делать?

Исследователи и хакеры постоянно находят новые вектора атак, уязвимости «нулевого дня». Их обнаруживают в ходе специальных конкурсов, и хакер, который вас атакует, может знать их. В такой ситуации средства веб-защиты позволяют выиграть время. Вы будете видеть, что кто-то вас целенаправленно атакует, сможете оцените периодичность и вектор атак, и служба безопасности и ИТ-отдел смогут заблаговременно принять меры.

Не все виды аудита одинаково полезны

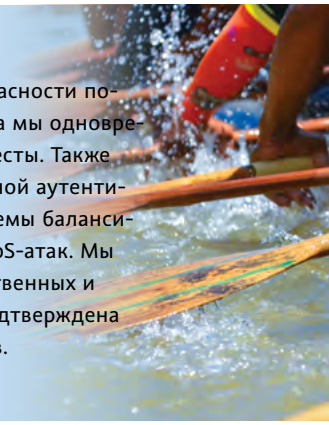
Некоторые компании предлагают автоматизированное сканирование вместо анализа уязвимости, но такая проверка может рассматриваться лишь как дополнение к ИБ-аудиту. Другие выполняют пентест по следующему сценарию: находят одну уязвимость и из нее расширяют свой вектор атаки, выдавая потом клиенту пугающий список возможных несанкционированных действий, основанный всего лишь на одной лазейке. Разумеется, такая проверка не является исчерпывающей, и специалисты Softline не расширяют вектор атаки, а продолжают поиск уязвимостей.

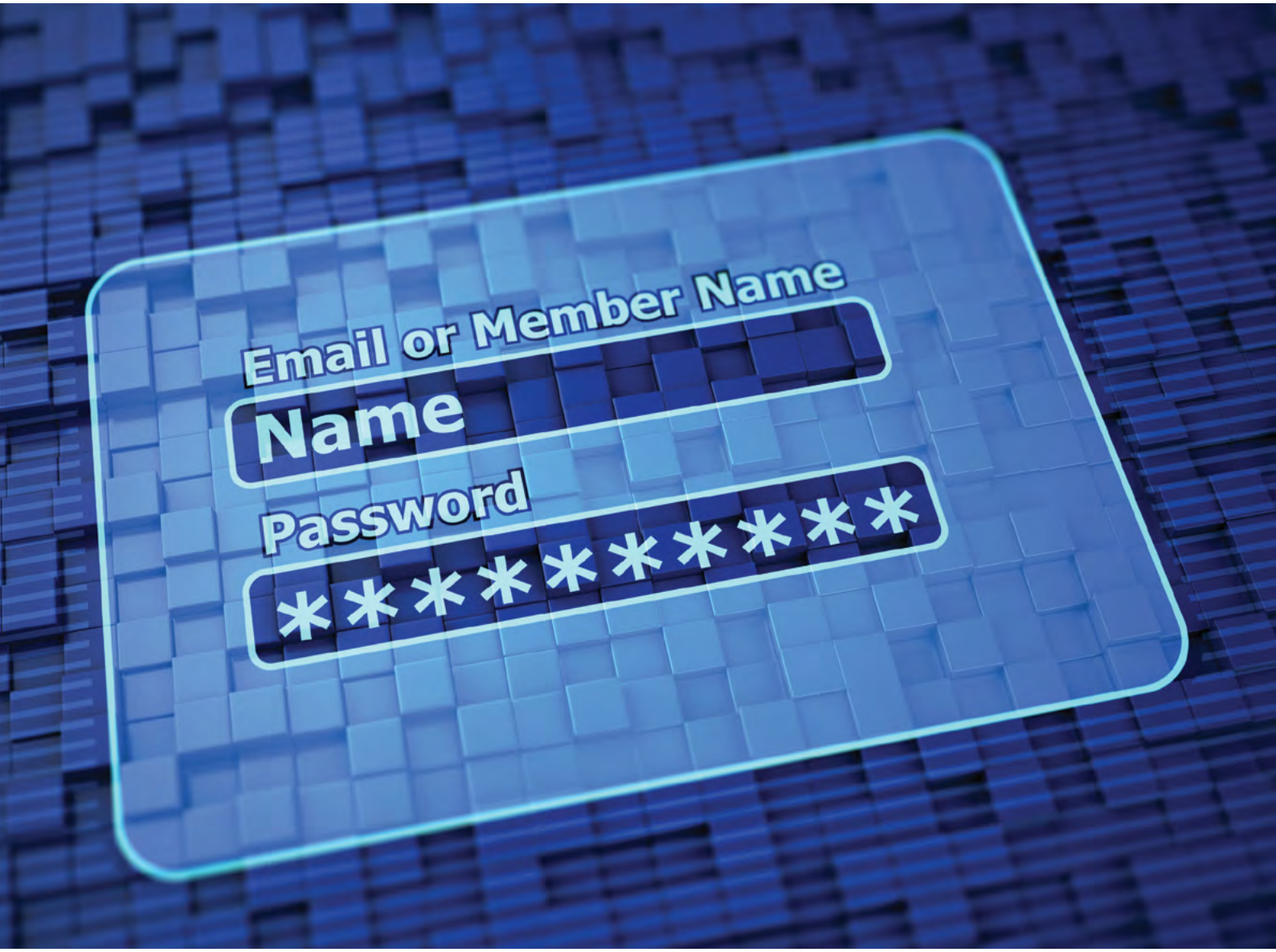
Дефейс приводит к серьезным репутационным рискам — например, на сайте областной Думы одного из субъектов РФ хакеры разместили информацию о том, что он выходит из состава России и становится независимой республикой.

Преимущества аудита ИБ от Softline

В Softline работает хорошая команда экспертов по тестам на проникновение и аналитиков, разбирающихся не только во защите инфраструктуры, но и веб-порталов и приложений. Наши специалисты регулярно участвуют в национальных и международных соревнованиях по ИБ.
Когда эксперты Softline находят одну уязвимость, они оповещают о ней клиента, и поясняют, какие действия она позволяет осуществить. Но после этого они не расширяют вектор атаки из этой исходной точки, а продолжают поиск новых уязвимостей.

Естественно, наиболее высокого уровня безопасности позволяют добиться комплексные проекты, когда мы одновременно внедряем WAF, проводим аудит и пентесты. Также Softline поставляет решения по многофакторной аутентификации, классические сетевые экраны и системы балансировки нагрузки, системы предотвращения DDoS-атак. Мы сотрудничаем с большим количеством отечественных и зарубежных вендоров, наша квалификация подтверждена партнерскими статусами и отзывами клиентов.





Аутентификация и управление доступом на предприятии

Парольная аутентификация подвергается серьезной и вполне обоснованной критике. Несостоятельность парольного доступа в контексте обеспечения корпоративной IT-безопасности сегодня очевидна.

Неудобные пароли

В современных компаниях для выполнения бизнес-задач сотрудники используют большое количество бизнес-приложений и информационных систем. При стандартном подходе к обеспечению безопасности это означает необходимость запоминать множество логинов и паролей, а также достаточно часто их менять согласно установленным политикам безопасности. Поэтому пользователи стараются использовать несложные пароли, дополнительно записывая их на бумажках, которые затем хранят в совершенно неподходящих для этого местах.

Кроме того, зачастую пользователи сами сообщают свои пароли коллегам в случае болезни или необходимости выполнения каких-то срочных действий. Поэтому даже если пользователь вводит пароль, это не означает, что он является владельцем предоставляемых учетных данных.

Неудобны пароли и для специалистов IT- и ИБ-служб. Забытые после отпусков пароли и заблокированные учетные записи требуют от них дополнительных затрат на восстановление этих данных.

«Неуправляемое» управление доступом

Другой проблемой, связанной с учетными данными, является управление доступом к данным и ресурсам компании. Прием новых и увольнение старых сотрудников, перестановки требуют от администраторов постоянной модификации данных о правах доступа, которые, в свою очередь, как показывает практика, часто неструктурированы, а потому управление ими затруднено и существует риск возникновения ошибок в таких изменениях. В результате в работе сотрудников, не получивших необходимый доступ, возникают вынужденные простои, а уволенные сотрудники могут по-прежнему получать доступ к корпоративным ресурсам и выполнять какие-то деструктивные действия.

Все это существенно снижает эффективность работы персонала. Но главное, что в такой ситуации возрастает риск несанкционированного доступа к ресурсам компании, а значит, существенно снижается общий уровень безопасности.

Для решения этих проблем используются технологии строгой аутентификации и единого доступа.

Строгая аутентификация

Одним из наиболее эффективных способов решения проблем использования парольного доступа является строгая (многофакторная) аутентификация, основанная на проверке дополнительных данных (факторов) для идентификации пользователя.

Факторами аутентфикации могут быть известная пользователю информация (пароль, PIN-код), имеющееся у пользователя устройство (смарт-карта, токен, генератор одноразовых паролей) или биометрические параметры пользователя (отпечаток пальца, рисунок вен на ладони, сетчатка глаза).

Аутентификация с применением каждого из этих факторов имеет свои преимущества и недостатки. Однако недостатки отдельных факторов легко устраняются путем применения комбинации нескольких параметров аутентификации. Очевидно, что чем больше факторов используется для аутентификации, тем она надежнее (наиболее распространенным является применение двух факторов).

Что касается выбора сочетания способов аутентификации к ресурсам целевой IT-инфраструктуры, это вопрос компромисса между удобством использования, полнотой интеграции, степенью безопасности и ценой итогового решения.

Кроме того, применение технологии строгой аутентификации обеспечивает автоматическое исполнение регламентов доступа к IT-системам компании.

Технология единого входа

Технология единого входа (Single Sign-On, SSO) обеспечивает возможность использовать один идентификатор для доступа ко всем (разрешенным) ресурсам и системам.

SSO-решения централизованно хранят все пароли пользователя и автоматически подставляют их в запросы аутентификации, когда это требуется.

То есть для того, чтобы выполнить вход в приложение, пользователю достаточно лишь предоставить данные для аутентификации (например, приложить палец к считывалю или выполнить какое-то иное действие в зависимости от используемой технологией аутентификации). Учетные данные (логин и пароль) будут подставлены SSO-системой автоматически без участия пользователя.

Таким образом, пользователи освобождаются не только от необходимости запоминания множества логинов и паролей, но также от необходимости их ручного ввода при аутентификации, что существенно упрощает доступ к приложениям и снижает нагрузку на IT- и ИБ-службы.

В концепции SSO также реализуется компонент управления правилами и политиками доступа ко множеству приложений и систем как для отдельных пользователей, так и для целых групп (отделов, подразделений и проч.), что делает прозрачным процесс управления учетными данными и паролями пользователей. При этом появляется важный «бонус» в виде возможности мгновенной блокировки доступа сразу во все системы в случае такой необходимости.

Комплекс решений Indeed ID

На отечественном рынке технологии строгой аутентификации и единого доступа успешно реализует комплекс решений Indeed ID, разработанный одноименной российской компанией и предназначенный для аутентификации и управления доступом на предприятии.

Данный комплекс поддерживает широкий спектр различных технологий строгой аутентификации (смарт-карты, токены и RFID-карты различных производителей, биометрия, одноразовые пароли), позволяя реализовать различные сценарии многофакторной аутентификации пользователей. Все поддерживаемые технологии можно комбинировать между собой. Например, можно аутентифицировать пользователей по отпечатку пальца и бесконтактной карте, смарт-карте и OTP и т.д. При этом, если на предприятии уже используются какие-то способы строгой аутентификации, они могут быть поддержаны данным комплексом благодаря особенностям архитектуры входящих в него решений, что особенно удобно, поскольку не требует дополнительных затрат на приобретение новых средств аутентификации и дает возможность гибко адаптировать систему аутентификации к потребностям и текущим условиям работы компании.

Подход Single Sign-On в масштабе предприятия реализует продукт Indeed Enterprise SSO, входящий в состав комплекса. Система централизованно хранит пароли пользователя от всех приложений, требующих аутентификации, и автоматически подставляет их, когда приложение этого требует. При истечении сроков действия паролей в приложениях система автоматически выполняет их смену.

Indeed Enterprise SSO подходит для любых типов приложений (Windows, Java, Web), независимо от их архитектуры: однозвенная, двухзвенная, трехзвенная, «толстый» клиент, «тонкий» клиент, терминальные приложения. При этом организовать доступ можно как в коробочные приложения, так и в приложения, разработанные на заказ.

Система также адаптирована к работе в терминальной среде (Remote Desktop, VDI, Citrix), что избавляет сотрудников от явного использования паролей в командировках и других ситуациях, когда работа с приложением выполняется в терминальной сессии.

В компаниях, использующих смарт-карты и токены, Indeed Enterprise SSO позволяет связать учетные данные пользователей с жизненным циклом ключевых носителей, интегрировав систему аутентификации с системами управления ключевыми носителями (Card Management System, CMS). Можно отметить, что в состав комплекса входит CMS-система этого же разработчика (Indeed Card Management), хотя при необходимости интеграция возможна и с другими системами данного класса, представленными на рынке.

В завершение следует отметить, что все действия администраторов и пользователей фиксируются в специальных журналах событий системы, что существенно упрощает процесс анализа и расследования инцидентов.

ПОСЛЕДНИЙ оборонительный РУБЕЖ

Мир сталкиваются с новыми угрозами — более изощренными, разнообразным и сложными, чем когда-либо прежде.

Порой просто невозможно быстро обнаружить и устранить инцидент безопасности в процессе его реализации до момента нанесения серьезного ущерба, что в конечном итоге имеет значительные последствия для всей организации. Большинству команд безопасности не хватает рабочих рук, компетенций и опыта, необходимых для быстрого и точного исследования огромного объема оповещений, создаваемых существующими в организации системами безопасности. Проактивное обнаружение новых угроз, проникающих через существующие системы защиты, все более и более актуально. Тем не менее, часть нарушений безопасности остается незамеченной до тех пор, пока не станет слишком поздно, и приходится устранять уже их последствия, которые, в свою очередь, могут привести к возникновению прямых и косвенных затрат и оказать влияние на всю бизнес-деятельность организации. Практики безопасности и управления инцидентами в этом случае неизбежно потребуют привлечения дополнительных внутренних и внешних сил.

Художники высокотехнологических угроз

Ушли в прошлое дни тех вирусов, которые писались без каких-либо целей, кроме самовоспроизведения. Вредоносы пытаются различными методами обмануть систему, при этом пустив специалистов по ИБ по ложному следу. В самом деле, многие нарушения совершаются только с использованием только фишинга, эксплуатации уязвимостей веб-приложений, а также встроенных ошибок, заложенных в функционал системы. В инцидентах безопасности, где применяется заражение вредоносом, это давно делается с далеко идущими целями. Современные команды безопасности понимают, что для защиты сотрудников, интеллектуальной собственности и других активов требуются высокоинтеллектуальные средства защиты. Они признают, их истинные противники — настоящие художники высокотехнологических угроз, использующие все достижения прогресса в своих шпионских целях, которые включают в себя распределенные атаки на сетевой периметр и внутреннюю сеть, выполнение масштабных разведывательных действий с нанесением ущерба активам, расширением привилегий, воздействиям в разных направлениях, созданием скрытых бэкдоров и кражей данных.

Что же произошло?

Старые методы и подходы по обеспечению безопасности и по обнаружению и реагированию на инциденты показали себя крайне

неэффективно. Аналитику приходится просматривать сетевой трафик, данные с конечных точек, информацию об угрозах и другие источники данных в отдельных продуктах. Каждое предупреждение систем безопасности, каждое найденное цифровое свидетельство требовало ручного анализа, чтобы затем сложить воедино всю получившуюся головоломку по инциденту — восстановить, что же произошло и принять соответствующие меры. Эти огромные усилия расходовали всю энергию ценных аналитиков в области безопасности и реагирования на инцидент. А между тем, стоимость потерь от инцидентов растет, число жертв постоянно увеличивается, появляются новые бреши в защите, пароли учетных записей воруются и кражи данных как происходили, так и происходят.

Дело в том, что в случае, когда злоумышленник уже проникает в систему, его действия в сети сложно отследить стандартными средствами, а методы, основанные на сигнатурном поиске уже абсолютно бесполезны. Единственный способ обнаружить, изучить и предотвратить подобные угрозы — это заранее внедрить решение, которое даст полный обзор ситуации со всех сторон, в частности — даст полную и прогнозируемую картину о том, что происходит на рабочих станциях и в сети.

AccessData

Представляем вашему вниманию набор решений в области компьютерной безопасности компании AccessData, который сочетает в себе компьютерную криминалистику, сетевую криминалистику, полномасштабный аудит данных, предоставляя единый интерфейс мониторинга.

Данная автоматизированная и интегрированная инфраструктура безопасности позволяет быстрее и эффективнее решать проблемы, связанные с угрозами информационной безопасности, утечкой данных и обязательствами по соблюдению нормативных требований. Используя ПО из пула решений AccessData, можно заблаговременно и быстро определять, анализировать и разрешать любые инциденты, включая уязвимости «нулевого дня», взлом, утечку данных и целенаправленные атаки. К примеру, можно просканировать тысячи компьютеров организации для выявления вредоносных исполняемых файлов, существующих в сети. Можно эффективно выполнять анализ первопричин путем сопоставления сетевых данных и данных из локальных ресурсов в рамках единого интер-

Наиболее значимые преимущества полностью интегрированной инфраструктуры безопасности

- Легкий постоянный мониторинг; выполняемые операции автоматизируются с помощью информационных материалов, формируемых в реальном времени.
- Сопоставление журналов событий.
- Эффективное обнаружение угроз безопасности.
- Выполнение поиска первопричин инцидента и восстановление удаленной информации в различных системах.
- Комплексные аналитические инструменты позволяют более эффективно выявлять целенаправленные устойчивые угрозы.
- Эффективный сбор данных для дальнейшего анализа инцидентов.
- Возможность создания профилей защиты сети.
- Автоматизированный полномасштабный аудит данных позволяет выявить утечки информации.
- Легкий поиск документов по FOIA-запросам в соответствии с требованиями зарубежного законодательства в сфере защиты информации о гражданах, что также может быть использовано и для поиска и предоставления информации в соответствии с отечественным законодательством о персональных данных.
- Эффективное и менее затратное выполнение регулярного аудита по стандартам PCI.
- Подключение к различным информационным банкам данных для целевого поиска без создания индекса.
- DOD-сертифицированное стирание данных, если этого требуют обстоятельства или политики.

Компания AccessData — мировой лидер в области решений по расследованию инцидентов ИБ (Computer Forensic) и поиска в неструктурированных данных (eDiscovery).

фейса. Во время анализа можно заново воспроизвести инцидент, чтобы четко понять, как развивалось вторжение; при необходимости подробно изучить поврежденные машины можно проанализировать поведение зловреда на уровне рабочей станции. Просканировать информационную систему организации для определения всех поврежденных узлов и, что более важно, для устранения угрозы. И наконец, используя аналитические данные, полученные с помощью ПО AccessData при анализе инцидента, можно создать профили угроз для предотвращения появления таких угроз в будущем.

Критически важные возможности

Весь пул решений компании AceessData интегрируется в едином интерфейсе, с помощью которого можно анализировать и соотносить локальные статические, динамически изменяющиеся данные и сетевой трафик. Более того, набор решений системы реагирования на инциденты может предложить надежную функцию дистанционного «пакетного восстановления» удаленной информации. Инфраструктура защиты предоставляет критически важные возможности, которые на сегодняшний день отсутствуют в традиционной инфраструктуре информационной безопасности.

КАКИЕ ОСНОВНЫЕ ВОЗМОЖНОСТИ ОТЛИЧАЮТ ЕДИНУЮ ИНФРАСТРУКТУРУ БЕЗОПАСНОСТИ, ПОСТРОЕННУЮ С ПОМОЩЬЮ РЕШЕНИЙ ACCESSDATA?

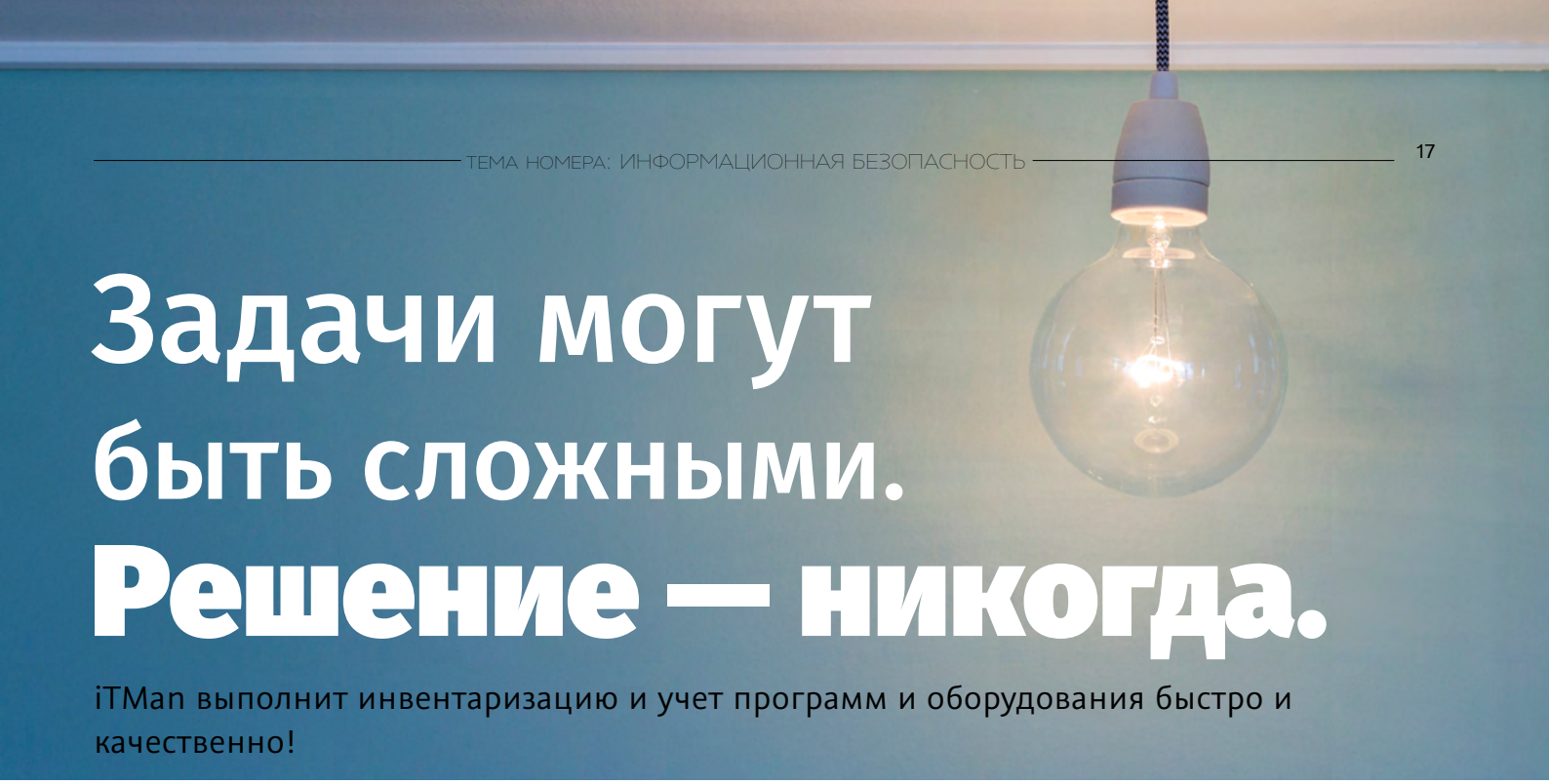
1. **Простота использования, основанная на процессах схема работы, оперативная связь по всей иерархической цепи.**
- Легкий в использовании веб-интерфейс, позволяющий осуществлять доступ к системе в реальном времени из любого места.
- Ролевой доступ к системе.
- Обеспечение безопасности в реальном времени.
- Интеграция с Active Directory для более быстрого развертывания.
- Быстрая реакция на инцидент, в том числе анализ всех активных процессов.
- Расширенный агентский поиск и анализ задействованной памяти на компьютерах под управлением 32- и 64-битной версий Windows.
- Автоматическое сканирование тысяч компьютеров аномалий.
- Сопоставление статических и переменных данных с сетевым трафиком.
- Комплексный анализ и сбор данных со всех совместно используемых сетевых ресурсов для криминалистического анализа.
- Первый в отрасли сбор одним кликом данных с жестких дисков, с ОЗУ, а также переменных данных.
- Автоматизированный пакетный сбор данных.

2. **Перехват сетевых данных в реальном времени.**
- Перехват данных в реальном времени на скорости вплоть до 1 Гбит/сек.
- Возможность отслеживать более 1500 протоколов и служб по умолчанию.
- Сетевые данные размещаются в центральной базе данных.
- Перехват и анализ данных в беспроводных сетях стандарта Ethernet 802.11b и 802.11g.
- Сопоставление и анализ журналов.

3. **Анализ модели и содержания с воспроизведением нужного инцидента.**
- Расширенные средства визуализации для более эффективного анализа первопричин.
- Интерактивное представление распространения вторжения.
- Разделение ложных и злоумышленных инцидентов.
- Составление карты распространения вирусов, червей и утечек конфиденциальных данных.
- Отслеживание точной последовательности событий с воспроизведением инцидента по запросу.

4. **Улучшенный, направленный и полномасштабный аудит.**
- Автоматизированный, эффективный способ обнаружения утечки данных и обеспечение соответствия стандартам PCI.
- Расширенные возможности использования панели инструментов и составления отчетов.
- Расширенные возможности регистрации всех обнаруженных вторжений для обеспечения безопасности и аудита.
- Определение места расположения секретных или персональных данных и их классификация.
- Проведение автоматизированных проверок с использованием практически любых критериев поиска.

5. **Возможность действовать немедленно, эффективно и надежно.**
- Возможность быстро отвечать на FOIA-запросы.
- Возможность сигнализации о файлах, не отвечающие нормативным требованиям, с сохранением информации об их расположении.
- Централизованное маркировка и удаление подозрительных файлов и замена их файлами-заглушками.
- Завершение процессов через контекстное меню правой кнопки мыши и пакетное восстановление для авторизованных пользователей.
- DOD-сертифицированное стирание.
- Взаимодействие компонентов системы через защищенное соединение в соответствии со стандартом FIPS 140-2 и использующее 128-битное SSL-шифрование.



Задачи могут быть сложными. Решение — никогда.

iTMan выполнит инвентаризацию и учет программ и оборудования быстро и качественно!

Что вам действительно нужно?

Классифицируйте и стандартизируйте свои IT-активы — так вы сможете оптимизировать структуру их использования, потому что всегда будете видеть «картину целиком». И значительно сократите IT-затраты.

Волнуетесь насчет репутационных или юридических рисков? Эти тревоги вполне обоснованы — но если у вас есть iTMan— решение для инвентаризации оборудования в сети — риски можно не только оценить, но и максимально минимизировать.

Решения учета и инвентаризации IT-активов давно перестали быть инструментом работы исключительно администраторов сети: данные, собираемые iTMan, интересны также директорам компаний, руководителям и сотрудникам финансовых подразделений.

Распорядитесь средствами с умом

Гарантированно сэкономьте на платежах за лицензии и поддержку от 5 до 30% в год. Кроме того, обеспечивая соответствие приобретаемых IT-активов реальным бизнеспотребностям, вы сбережете 7-15% IT-бюджета вашей компании.

iTMan — идеальное решение для организаций малого и среднего бизнеса.

Настраивайте под себя!

Какие данные нужно собрать и когда — решать исключительно вам. iTMan — многозадачная система, вы можете настроить задачи на сканирование всей сети или только необходимых вам ПК. Сканируйте по любому удобному вам расписанию.

Все под контролем

Хотите прогнозировать свои затраты на IT и точно знать, сколько времени и денег уйдет на реализацию того или иного управленческого решения? iTMan станет для ценнейшим источником информации для прогнозирования затрат на IT!

У ВАШИХ СОТРУДНИКОВ МНОГО СВОБОДНОГО ВРЕМЕНИ?!

Знаете ли вы, что по статистике 73% IT-сотрудников тратят рабочее время на механические действия, которые можно и нужно автоматизировать, а именно: на проверку соответствия лицензий требованиям законодательства и производителей, аудит лицензионных соглашений, объединение данных об установке и использовании программного обеспечения.

Почему качественная инвентаризация ПО и «железа» необходима компаниям, которых волнуют вопросы информационной безопасности? Практически ежедневно в сети среднестатистической организации появляются новые устройства. Мы знаем, ваша компания — вовсе не среднестатистическая, а уникальная, но... Ситуация все же не меняется. Скажем, сотрудник может принести сетевой коммутатор из дома, обходя ограничения маршрутизаторов по портам и меняя сеть. Как узнать о происходящих изменениях? Этот вопрос с легкостью поможет решить iTMan: среди всех его грандиозных возможностей — гарантированная идентификация подключенного к ПК свитчей и вообще любого оборудования.

Закачайте мобильную версию и протестируйте ITman прямо сейчас: app.itman24.ru

iTMan

Руки прочь от наших данных

В кризис вопросам снижения издержек и повышения эффективности традиционно уделяется больше внимания. Одним из эффективных способов снижения расходов является противодействие мошенничеству. В этой статье мы рассмотрим основные виды мошенничества в банках и компаниях-ритейлерах, и способы минимизации потерь от них.

Банки

Для защиты от злоумышленников банки предлагают своим клиентам использовать различные технические и программные средства (USB и OTP-токены, среды безопасного доступа — «песочницы», sms-информирование и т.д.). Очевидным минусом подобных средств является невозможность заставить клиента их использовать. Дополнительным фактором опасности служит доходность и, как следствие, развитость данной индустрии мошенничества. Еще одной проблемой является превосходство средств атаки над средствами защиты: свежий троян безнаказанно функционирует, как минимум, несколько дней, прежде чем попасть в сигнатуры антивирусов.

Существенным риском для банков является и мошенничество со стороны сотрудников. Как правило, мошенничеством занимаются люди, работающие в компании несколько лет и хорошо знающие бизнес-процессы банка, их уязвимые места. Самыми распространенными нарушениями сотрудников являются некорректное кредитование, хищение средств со счетов клиентов и «слив» информации о клиентах банка.

История с преступной группой Carbanak наглядно показала, что самая качественная, эшелонированная техническая защита организации вполне может быть взломана, пусть это и займет несколько месяцев.

В условиях, когда техническая защита не дает 100% гарантии защиты от мошенничества, на сцену выходят специализированные решения — системы противодействия мошенничеству и гарантированию доходов. Такие решения показали эффективность в деле минимизации потерь от внутреннего и внешнего мошенничества и стали общемировой практикой. Антифрод-системы защищают клиентов банка (физических и юридических лиц) и позволяют контролировать действия сотрудников. Основной принцип работы таких решений — поведенческий анализ действий клиента. Обрабатывая данные текущей сессии и профиль клиента, антифрод-система может блокировать подозрительные транзакции, запрашивать дополнительную авторизацию у клиента, оповещать уполномоченных сотрудников банка. Поскольку антифрод работает целиком на стороне банка, его внедрение и использование происходит незаметно для клиентов. Как следствие, повышается лояльность клиентов за счет повышения качества (защищенности) предоставляемых услуг.

Дистанционное банковское обслуживание

Самой актуальной угрозой для ДБО являются атаки на клиентские устройства с целью получения контроля над ними и проведения несанкционированных списаний денежных средств на подконтрольные мошенникам счета. Как известно, далеко не все клиенты выполняют даже минимальные рекомендации работы с ДБО (например, не используют антивирусы), что повышает уровень опасности данной угрозы. Рынок мошенничества велик, и на нем есть четко выраженное распределение специализаций: одни группы мошенников пишут трояны (и продают их), другие — занимаются заражением клиентских станций и выводом средств, третьи специализируются на «дропе» (т.е. выводе денег из мошеннической схемы).

Основное средство защиты — поведенческий анализ действий клиентов. Транзакции совершаемые мошенниками, как правило, отличаются от клиентских транзакций и имеют ряд характерных признаков. Антифрод-система сравнивает каждое действие клиента с профилем его поведения и ищет признаки мошенничества.

ХАРАКТЕРНЫЕ ПРИЗНАКИ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ:

- Вывод не менее 75% остатка на счете.
- «Разбивка» — переводы на несколько новых счетов.
- Переводы нескольких клиентов банка на новый счет.
- Несколько сессий разных клиентов с одной станции за короткий промежуток времени.
- Минимальный промежуток времени между операциями (при ручном вводе требуется больше времени).
- Сессии из разных регионов за короткий промежуток времени.
- Неурочное время и новая клиентская станция.

Пластиковые карты

Количество выпускаемых карт в России стабильно растет, и вместе с тем растет и риск мошенничества с пластиком. Несмотря на обилие технических и организационных мер по повышению защищенности банковских карт, ущерб от мошенничества с пластиком остается высоким.

Распространенные виды мошенничества:

- Мошенничество с кредитными картами (в том числе с участием сотрудников банка) – получение карт по фальшивым документам (или без них).
- Мошенничество с POS-терминалами — двойная прокатка карт, установка скимера работниками сферы обслуживания.
- PoS RAM scrapers — атака нацеленная на получение данных карт непосредственно из оперативной памяти терминала. Функционально, это некий аналог скимера, фактически — вирус для платежного терминала. Постепенное развитие mPoS-ов делает этот вид атак все более актуальным.
- Фишинг — получение конфиденциальной информации клиентов путем обмана. Например, создается сайт, внешне и адресом URL похожий на существующий интернет-банк. Злоумышленники выводят свой сайт в топ выдачи поисковиков, размещают рекламу на сайтах, рассылают письма содержащие ссылки на фальшивый сайт.
- Вишинг и смишинг — получив установочную информацию о клиенте, мошенники совершают

транзакцию перевода средств или покупку чего-либо. Далее следует звонок от «сотрудника банка» или смс, где просят указать поступивший sms-код якобы для «отмены платежа».

- Таргетированые атаки — злоумышленники собирают данные о клиентах с большим остатком на счете. По фальшивой доверенности от имени клиента переоформляют абонентский номер сотовой связи на другую сим-карту, что позволяет обойти защиту 3D Secure и не допустить своевременного информирования клиента о неправомерном доступе к его счету.

Методы обнаружения

В случае CNP (card not present) алгоритмы выявления подозрительных действий аналогичны алгоритмам, используемым при защите ДБО. При операциях с использованием физической карты появляются дополнительные факторы для анализа (расположение и принадлежность платежных устройств). Использование статистических данных позволяет оперативно выявлять скомпрометированные терминалы.

Внутреннее мошенничество

Все действия сотрудников оставляют «следы» в бизнес-системах банка. Антифрод-система собирает информацию о действиях сотрудников из разрозненных систем, и агрегирует их в единую модель данных. Посредством многомерного анализа собранных данных выявляются подозрительные действия сотрудников имеющие, либо признаки мошеннических схем, либо аномальные активности (отклонения от поведенческого профиля). Подобный подход позволяет выявлять неправомерные действия сотрудников во всех сферах банковской деятельности — от кредитования и присвоения активов клиентов, до непреднамеренных ошибок и «слива» информации о клиентах.

Оформление кредитов с предоставлением заведомо некорректных данных — один из самых старых видов мошенничества. Нечестные сотрудники оформляют кредит на своего сообщника, используя фальшивые документы или вообще обходясь без них. Кроме того, сотрудники могут оформлять кредит на имя существующего клиента банка без его(клиента) ведома.

Имея физический доступ к выпушенным, но не выданным картам, сотрудники могут изготовить их дубликат.

Возможно разглашение информации о клиентах — поиск и использование в личных целях данных о клиентах, например, предоставления злоумышленникам информации для проведения таргетированых атак. Этот вид мошенничества характеризуется высоким уровнем косвенного ущерба, поскольку появление в прессе информации о подобных нарушениях сотрудников банка ведет к репутационным потерям.

Хищение небольших сумм со счетов клиентов может быть осуществлено, если сотрудник периодически производит небольшие списания с карт, которые активно используются клиентами. При существенном количестве операций, осуществляемых клиентами, особенно, при отсутствии смс-информирования, невысокая сумма может попросту затеряться.

«Спящие» счета — те, которыми давно не пользуются, с существенным остатком на счете. Хищение с таких счетов характеризуется тем, что клиент очень долго может не замечать пропажу. Анализ действий сотрудников, проводимый антифрод-системой, легко выявляет по-

СТАНДАРТНЫЕ ВИДЫ ФИЛЬТРОВ

- Контроль рисковых операций (например, «спящие» счета, корректировки).
- Нехарактерные действия (например, поиск клиентов по остатку на счете).
- Обращение к информации по чужому VIP-клиенту.
- Операции по клиенту, от которого нет обращений в CRM.
- Нестандартные следы операции обслуживания (например, мало времени между шагами операции).
- Аномально высокое количество операций по сравнению с другими сотрудниками (например, повышение кредитных лимитов, разблокировка счетов).
- Неоднократное обращение к данным клиента (шпионаж).
- Высокая сумма выданных «плохих» кредитов.
- Обращение к счету клиента незадолго перед мошенничеством.
- Нарушение процедур обслуживания.
- Просмотр счетов сотрудников.

дозрительные активности, связанные со спящими счетами.

Меры противодействия

Проактивный мониторинг данных, проводимый антифрод-системой, является самым эффективным средством противодействия мошенничеству (по данным отчета ACFE за 2014 год, применение подобных инструментов снижает ущерб в два раза). Как правило, бизнес-системы логируют доступ к информации только в случае внесения изменений, т.е. просмотр информации не фиксируется. Антифрод-системы способны перехватывать сетевой трафик и логировать, в том числе, и просмотр данных. Полнота информации о действиях сотрудников позволяет выявлять неправомерные действия на раннем этапе. Например, легко отслеживаются попытки «пробивки» клиентов, поиск спящих счетов с существенным остатком и так далее.

Обрабатывая все действия сотрудников, антифрод-система с помощью интеллектуальных фильтров выявляет подозрительные.

Результаты внедрения антифрод-решения в банке:

- снижение ущерба от мошенничества;
- контроль сотрудников;
- выполнение требований регуляторов;
- оптимизация работы СБ.

Ритейл

Для ритейлеров всего мира актуальна проблема мошенничества (в России в среднем потери составляют 1,5% от годового оборота)[1]. Примерно треть потерь приходится на воровство покупателей, оставшаяся часть потерь приходится на мошеннические действия сотрудников компании, поставщиков, а также ошибки в IT-системах. Поскольку вся информация, начиная от кассовых операций до поставок товаров и выплаты премий, содержится в IT-системах компании — самым эффективным средством сокращения расходов от мошенничества общепризнано являются системы проактивного мониторинга данных (антифрод-системы).

Немного о мошенниках

Согласно исследованию PwC за 2014 год, «респонденты, которые столкнулись с внутренним мошенничеством, к самым важным факторам относят наличие возможности (76%), мотивацию и давление внешних обстоятельств (12%) и возможность самооправдания (9%). Таким образом можно говорить о том, что риск мошеннических действий связан в первую очередь с наличием возможности совершения мошенничества, причем в этом отношении ситуация в России соответствует глобальным тенденциям».

В ритейле большое количество территориально распределенных офисов и магазинов вынуждает предоставлять солидные полномочия сотрудникам на местах и затрудняет контроль за ними. Таким образом, широкие возможности для совершения мошенничества сотрудниками компаний-ритейлеров вызваны в первую очередь объективными требованиями бизнеса. В этой ситуации наиболее эффективным фактором удерживающим сотрудников от мошенничества является оперативное раскрытие прецедентов мошенничества. Это позволяет создать у сотрудников ощущение четкого контроля и неотвратимости наказания.

РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСТВА В РИТЕЙЛЕ

- Сторнирование чеков.
- Модификация сумм-количества товаров в чеке.
- Выставление экономически неоправданных скидок.
- Браковка товара: продавец в сговоре с сотрудником СЦ.
- Использование карты продавцом для накопления баллов за покупки.
- Предоставление продавцом существенных скидок по своей карте аффилированным лицам.
- Пополнение счета без внесения средств в кассу.
- Оформление фиктивных кредитов.
- Завышение потерь товара при хранении (усушка).
- Фиктивные возврат и продажа товара со скидкой.

1. По данным отчета «Глобальный барометр потерь от мошенничества в Ритейле 2014» компаний The Smart Cube и Checkpoint.

Зачем нужен антифрод?

Антифрод-решения предназначены для постоянного мониторинга данных в бизнес-системах с целью выявления признаков мошенничества. Для этого используются два основных метода:

1. **Поиск в данных признаков известных схем мошенничества;**

2. **Статистический анализ данных с целью выявления неизвестных схем мошенничества и ошибок в IT-системах.**

Антифрод-решение посредством оперативного анализа данных:

- оперативно выявляет случаи мошенничества сотрудников;
- оперативно выявляет случаи мошенничества с участием партнеров и клиентов;
- выявляет утечки доходов;
- автоматизирует работу сотрудников безопасности;
- предоставляет инструменты анализа и проведения расследований;
- оперативно оповещает об инцидентах.

Выгоды от внедрения антифрод решения для ритейл-бизнеса:

- минимизация ущерба от мошеннических действий и ошибок IT-систем;
- гарантирование доходов (revenue assurance);
- помощь в проведении расследований;
- автоматизация действий сотрудников СБ.

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АНТИФРОД-РЕШЕНИЙ.

По данным исследований позволяет[2] снизить прямые потери от мошенничества на 60% и сократить время жизни мошеннических схем в два раза. Кроме того, своевременное выявление мошенничества существенно сокращает непрямые потери.

2 По данным отчета «Report to the Nations on Occupational Fraud and Abuse 2014» ACFE (ассоциация сертифицированных специалистов по противодействию мошенничеству)

Data Base Firewall

Броня — по-другому не скажешь!

Большая часть информации компании содержится в ее базах данных. Как правило, именно данные из СУБД становятся целью атаки злоумышленников. Продукты класса DBF (DataBaseFirewall) являются комплексным инструментом защиты корпоративных СУБД, покрывающим все основные угрозы.

Распространенные проблемы защиты СУБД

Необходимо контролировать всех пользователей

Любой пользователь может быть скомпрометирован, любой пользователь может не устоять перед искушением – согласно исследованию PwC от 2014 года, основным фактором (76%) для совершения мошенничества сотрудниками российских компаний является наличие технической возможности.

Трудоемкость анализа большого объема данных

Даже простейшее бизнес-действие может оборачиваться группой действий в СУБД. Количество событий в СУБД в сутки от десятков тысяч до десятков миллионов и выше, что делает ручной анализ весьма низкоэффективным.

Логи бизнес-систем не содержат всей необходимой информации

Даже если на текущий момент информации в логах хватает, в следующем релизе продукта эта функциональность может быть существенно изменена. Логирование не является основной функцией бизнес-системы, и может быть в любой момент урезано, например, в пользу производительности. Да и надежность такого логирования оставляет желать лучшего. Особенно остро вопрос стоит при трехзвенной архитектуре: сотрудник осуществляет действия в веб-интерфейсе, веб-сервис отправляет запрос в СУБД от своего имени. В результате, СУБД «видит» обращения не пользователей, а только веб-сервиса.

Управление доступами средствами СУБД проблематично

Для управления доступами необходим привилегированный доступ в СУБД, специфическое ПО и много времени. СУБД не содержат средств оповещения, а данных для анализа может быть немало. Кроме того, СУБД могут содержать функциональные уязвимости, например, select for update в Oracle — эта команда позволяет пользователю, не имеющему прав на изменение данных, заблокировать таблицу.

Шпионаж и «тихое» мошенничество

Ряд мошеннических операций не требует внесения изменений в бизнес-системы, например, шпионаж. Бывает достаточно даже просто просмотреть информацию (кодовое слово, принадлежность счета). Бизнес-системы, как правило, либо не содержат функционала полного логирования, либо этот функционал отключен по причине высокой нагрузки. DLP и другие средства контроля за распространением информации не дадут полную защиту от шпионажа – необходимо фиксировать доступ к информации на чтение, причем на уровне самих бизнес-систем или СУБД.

Таргетированные атаки

В последние годы все чаще появляются новости о взломах систем крупных, хорошо защищенных компаний. Злоумышленники, действуя в составе хорошо организованной группы, планомерно получают привилегированный доступ к бизнес-системам. Отсутствие защиты на уровне СУБД позволяет мошенникам осуществить крупное хищение, окупающее длительные попытки проникновения. Если же настроенные ограничения в бизнес-логике не дают с ходу провести хищение — отсутствие оповещения о подозрительных действиях позволит мошенникам подбирать нужную комбинацию действий оставаясь незамеченными.

Сложность расследования

Современные мошеннические схемы могут отличаться крайней сложностью, особенно при большом количестве вовлеченных лиц. Бизнес-системы не содержат инструментария для проведения расследований и способны только выгружать лог-файлы различной степени удобства. Без специальных инструментов, проведение расследования может приводить к выполнению руками сотрудника безопасности массы однообразных, рутинных действий.

Доказательства для правоохранительных органов

При выявленном факте мошенничества встает вопрос, как его доказать. Для заведения уголовного или административного дела, возмещения ущерба и даже просто увольнения сотрудника необходимы доказательства, которые будут приняты судом. Бизнес-системы не содержат специальных средств аудита, гарантирующих защиту данных от постороннего вмешательства. Это позволяет мошенникам оспаривать данные из бизнес-систем под предлогом того, что они

ЗАДАЧИ, РЕШАЕМЫЕ DBF:

- защита СУБД от хакерских атак;
- защита от инсайда;
- контроль и управление доступами;
- управление уязвимостями;
- контроль привилегированных пользователей;
- автоматизация действий сотрудников СБ.

ВЫГОДА ОТ ВНЕДРЕНИЯ

- Снижение ущерба от мошенничества, блокировка неправомерных операций.
- Контроль сотрудников.
- Управление уязвимостями: сканирование, виртуальный патчинг.
- Выполнение требований регуляторов.
- Оптимизация работы, автоматизация рутинных и трудоемких действий.

могли быть незаметно изменены теми же администраторами систем. К сожалению, в нашей стране отсутствуют единые стандарты касательно мер обработки информации для использования ее в качестве судебного доказательства. В результате, единственным доступным способом превращения информации в доказательство является использование специальных мер (разграничение доступа, внутренний аудит, защита от изменений), достаточных с точки зрения здравого смысла.

Сложность управления уязвимостями

Большое количество разнообразных СУБД (даже в рамках одной бизнес-системы) приводит к неэффективности ручного управления уязвимостями. Как правило, используются сканнеры уязвимостей, в разной степени пригодные для анализа СУБД. Не стоит забывать, что сканеры лишь оповещают о найденных уязвимостях или нарушениях политик ИБ, но не позволяют сотруднику ИБ самому принять экстренные меры. В результате, безопасность напрямую зависит от доступности IT-администратора.

Кстати, что делать в случае, если в тестовую БД, еще вчера содержащую только обезличенные тестовые данные, попадает критичная информация? Обнаружат ли ее сканеры?

Проблема своевременного обновления

Общеизвестный факт, что лакуна между обнаружением уязвимости и выходом патча может быть весьма длительной (срок выхода полноценного исправления достигает нескольких месяцев). Конечно, зачастую вендоры предлагают workaround-ы разной степени эффективности. Но как проверить корректность применения? Как проверить достаточность этого временного решения? Это может потребовать специфичных технических навыков и трат времени.

Регуляторы требуют полного и непрерывного контроля

Регуляторы требуют вести учет событий безопасности, контролировать доступы, управлять уязвимостями, проводить аудит на постоянной основе и многое другое. Ручное выполнение этих требований в развитой инфраструктуре крайне трудоемко.

Сложность возмещения ущерба

Согласно исследованию ACFEE за 2014 год, при обнаружении фактов мошенничества лишь в 14% случаев удалось полностью возместить ущерб от незаконных действий, а в 58% не удалось возместить даже частично. Кроме того, в суде можно оспорить прямые потери, а косвенные потери сложно поддаются монетарной оценке.

Невозможность блокировать операции

Лишь малую часть операций можно проверять вручную и предотвращать некорректные действия, фактически все случаи мошенничества расследуются постфактум. Соответственно, злоумышленник может совершить даже явно недопустимое действие, и будет обнаружен только спустя некоторое время. Нередки ситуации, когда сотрудник в последний день работы в компании совершает массу нарушений и пропадает с деньгами.

Нагрузка на бизнес-системы

Включение полного логирования средствами бизнес-систем или СУБД всегда ощутимо увеличивает нагрузку. Создание аналитических отчетов также может быть весьма ресурсоемким. Между тем, критичные данные, как правило, находятся именно в критичных бизнес-системах...

Решение: проактивная защита СУБД

- **Логирование любых действий в СУБД,** в том числе, чтения информации и технических действий администраторов, без влияния на бизнес-системы.
- **Раскрытие шифрованного трафика** — злоумышленник больше не спрячется за SSH!
- **Контроль привилегированных пользователей:** администраторы целевых систем и другие сотрудники не могут вмешиваться в работу DBF. Доверяйте, но проверяйте ваших администраторов — ведь учетные записи даже у самых лояльных сотрудников могут оказаться скомпрометированными!
- **Блокировка недопустимых действий** — возможность предотвращения заведомо некорректных действий.
- **Сканирование уязвимостей:** в отличии от стандартных сканеров, системы DBF могут находить критичную информацию (например, в случае нелегальной реплики).
- **Виртуальный патчинг** — технология оперативного (0-5 дней) закрытия уязвимостей средствами DBF (без внесения изменений в бизнес-системы).
- **Создание инцидентов и оповещение уполномоченных сотрудников** увеличивает скорость реакции на происшествия.

Наше — лучше

Отечественная контентная фильтрация на примере Usergate

Организация контролируемого доступа в Интернет является важным звеном в цепочке мероприятий по обеспечению мерами информационной безопасности вашего бизнеса. Современный прокси-сервер должен обладать множественным функционалом. Особенно важно это стало в условиях повышенного интереса к импортозамещению западных решений в условиях кризиса и режима санкций западных стран. В этих условиях повысился интерес к отечественным решениям этого класса. В частности, к продукту Usergate от компании Entensys из Новосибирска.

Методы HTTP-фильтрации:

- по категориям сайтов (собственный каталог);
- морфологический анализ и регулярные выражения;
- фильтрация загружаемых файлов по их типу;
- функция «Безопасный поиск»;
- фильтрация контекстной рекламы;
- черные и белые списки;
- антивирусная проверка загружаемого контента;
- блокировка приложений социальных сетей;
- блокировка фишинговых сайтов.

Оперативная коммуникация с партнерами и контрагентами уже невозможна без широкополосного Интернета. При всех своих достоинствах Интернет также несет опасность проникновения в корпоративную сеть вредоносного кода, допускается потенциальная утечка конфиденциальной информации и персональных данных. Нецелевое использование Интернета наносит не меньший вред бизнесу, нежели намеренное уничтожение или кража данных. Сотрудники проводят время на развлекательных порталах, в социальных сетях, эти сайты уже давно предоставляют собой некие агрегаторы информации различных направлений (развлекательный контент, видео, публичные чаты, распространение файлов и т.п.), а также являются удобным средством коммуникации. Дабы снизить потенциальные потери от нецелевого использования таких ресурсов необходимы решения, которые смогут разграничивать доступ к так называемым порталам Web 2.0, например — допускать коммуникации в чате социальной сети и запрещать просмотр\комментирование видео.

UserGate Web Filter

Это специализированное программное обеспечение, позволяющее контролировать использование Интернета на всех устройствах в локальной сети независимо от их типа и операционной системы. Внедрение продукта обеспечивает безопасность доступа во всемирную паутину и способствует сведению к минимуму нецелевого веб-серфинга.

Продукт предоставляет 3 типа фильтрации трафика:

- фильтрация DNS-запросов пользователей;
- фильтрация HTTP-трафика;
- фильтрация HTTPS-трафика.

Кроме этого, UserGate WebFilter предлагает в качестве дополнительной возможности фильтрацию HTTPS-трафика.

Фильтрация

DNS-фильтрация позволяет фильтровать интернет-ресурсы с помощью категорий сайтов и черных и белых списков хостов. При запрете доступа к определенному сайту с помощью DNS-фильтрации пользователь может быть перенаправлен на сторонний веб-сайт, на котором ему будет указано, что он пытается

получить доступ к запрещенному ресурсу.

HTTP-фильтрация обладает большим набором механизмов фильтрации, а также способна ограничивать доступ как к сайтам целиком, так и к их частям.

Фильтрация позволяет не только блокировать веб-страницы, но и предупреждать пользователя о ее неприемлемом содержании, оставляя пользователю возможность решать, следует ли продолжать просмотр или воздержаться от посещения данного ресурса.

Особенности решения

UserGate Web Filter способен работать в распределенной отказоустойчивой сети, когда нагрузка может распределяться между узлами кластера, что позволяет масштабировать систему до больших размеров. Подробнее о схемах распределения нагрузки и вариантах встраивания в любую сеть можно узнать в специальном разделе в конце данного руководства. Также UserGate Web Filter может выступать ICAP-сервером для любого оборудования, которое поддерживает фильтрацию по протоколу ICAP.

Существует несколько вариантов исполнения продукта:

- софтверное исполнение для самостоятельной установки;
- физический appliance;
- подготовленный программный appliance.

Продукт сертифицирован ФСТЭК РФ, а также есть возможность приобретения антивирусного движка Avira.

Сценарии применения продукта

Бизнес (EPG, SMB)

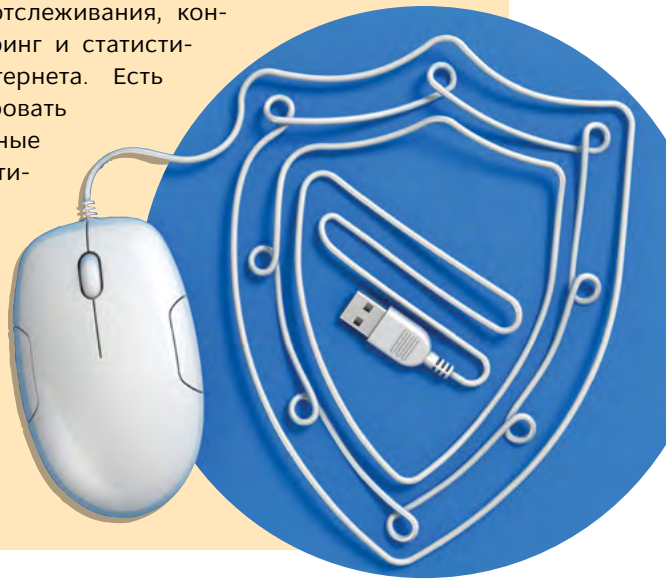
UserGate Web Filter обеспечивает безопасность посещения сотрудниками интернет-ресурсов, ограждает их от загрузки опасного и вредоносного содержимого, позволяет блокировать посещение ресурсов, не связанных с работой — социальных сетей, сайтов знакомств, поиска работы, онлайн-игр, развлекательных и других. Также UserGate Web Filter может блокировать любые ресурсы, запрещенные законодательством, содержащие произведения, включенные в список Министерства Юстиции РФ, в Реестр Роскомнадзора и любые другие списки.

Сфера образования

Интернет широко используется практически во всех образовательных учреждениях, и использование программного обеспечения для фильтрации стало необходимо не только для соответствия многочисленным законодательным требованиям, но и в целях обеспечения защиты сети от всевозможного вредоносного ПО и несовершеннолетних детей от вредной и опасной информации.

Технологии компании полностью удовлетворяют данным потребностям. В решениях представлены такие функции, как фильтрация по категориям, морфологический анализ содержимого страниц, безопасный поиск, фильтрация баннеров и скриптов отслеживания, контроль закачек, мониторинг и статистика использования интернета. Есть возможность блокировать опасные сайты, связанные с порнографией, наркотиками, суицидом, экстремизмом, а также обеспечить исполнение любых политик доступа.

Решения используют школы, интернаты, колледжи и библиотеки России и СНГ.



Системные требования

До 100 пользователей	**IntelAtom D2500 1.86GHz, 4Gb RAM, HDD 500Gb**
100-500 пользователей	**Intel Pentium Dual-Core G620 2.60GHz, 8Gb RAM, HDD 500 Gb**
500-1000 пользователей	**Intel Core i5 - Core i7 3550 3.30GHz, 16Gb, HDD 1Tb**
Более 1000 пользователей	**По запросу**

ActiveDRS

Виртуальный резервный дата-центр в облаке ActiveCloud

Чего не хватает вашей IT-инфраструктуре, если все классические меры для обеспечения информационной безопасности приняты — операционные системы и приложения регулярно обновляются, политики безопасности проходят регулярный аудит, внедрен современный центр обработки данных?

ActiveCloud DRS предоставляет защиту (как с использованием служб-агентов, так и без них) для платформ Microsoft Windows, Linux, Oracle, VMWare vSphere и Microsoft Hyper-V. Double-Take защищает основные и резервные серверы независимо от того, являются они виртуальными, физическими или облачными, локальными или удаленными. Решение уникально своей независимостью от платформы — исходная система может с равным успехом размещаться на физическом оборудовании, в виртуальных средах vSphere, Hyper-V, KVM или других.

К сожалению, ни один бизнес не застрахован от катастрофических событий, или событий, которые приравниваются к катастрофическим, причем самого разного рода. Потеря данных, важных для бизнеса, может произойти в результате форс-мажора — стихийного бедствия, пожара, военных действий, террористического акта. Остановка бизнеса может быть вызвана и более мирными событиями — аварией в системе коммуникаций, сбоем в энергоснабжении, бытовым затоплением.

Постоянным источником угроз для IT-систем остается человеческий фактор. К сожалению, приходится брать в расчет не только возможные последствия неаккуратности и некомпетентности, но и угрозы, связанные со злым умыслом.

Есть ли у вас план действий на случай аварии?

К сожалению, у многих организаций практика планирования восстановления IT-инфраструктуры и приложений отсутствует из-за отсутствия резервной инфраструктуры.

Очевидное решение для резервирования основного ЦОДа или серверной комнаты заключается в создании дублирующего резервного ЦОДа. Это решение имеет очевидные и серьезные минусы:

- очень высокая стоимость владения сопоставимая с основной инфраструктурой;
- капиталовложения в простаивающее здание/помещение и оборудование;
- дополнительные затраты на поддержание резервных образов систем и приложений в актуальном состоянии).

При этом тестирование плана восстановления после аварии в резервном физическом ЦОДе равноценно самой аварии и не может часто повторяться.

Дешевле и быстрее — перенести все данные и приложения в облако и сохранить их там, арендовав две независимые облачные площадки. Но в ряде случаев это решение слишком резко меняет привычную для предприятий модель угроз и рисков, связанных, например, с информационной безопасностью.

Многие предприятия оказываются готовы перенести свои данные в облако лишь частично — но этот компромиссный вариант не решает проблему в случае аварии в основном ЦОДе. Что же делать?

Построение собственного резервного физического ЦОДа	Держать все в облаке	Частично держать у себя, частично — в облаке	Все держать у себя, иметь резервный ЦОД в облаке
✓ Очень дорого ✓ Очень долго	✓ Дешевле ✓ Быстрее ✓ Изменение модели угроз и рисков	✓ Дешевле ✓ Быстрее ✓ Не решает проблему в случае гибели ЦОД	✓ Дешевле ✓ Быстрее ✓ Не меняет модель угроз и рисков

Варианты решения для обеспечения непрерывности бизнеса

Оптимальное решение для тех, кто по каким-либо причинам не готов полностью переносить основную инфраструктуру в облака — создание виртуального (облачного) резервного ЦОДа.

Логика приводит нас к действительно оптимальному решению — не нужно отказываться от уже используемых локальных приложений и аппаратных мощностей, включая физический основной ЦОД, если он есть. Но физический резервный ЦОД строить нет смысла — значительно выгоднее и быстрее разместить его в облаке.

Как работает ActiveCloud DRS?

Решение ActiveCloud DRS обеспечивает полную защиту основной инфраструктуры и данных путем репликации в виртуальный резервный ЦОД в облаке ActiveCloud в режиме реального времени. В случае отключения любого сервера восстановление данных выполняется мгновенно.

Постоянно фиксируя все изменения на уровне байтов и асинхронно реплицируя их в реальном времени на любом устройстве хранения, любом гипервизоре, любом физическом устройстве, в локальном или мировом масштабе, ActiveCloud DRS обеспечивает постоянный доступ к текущей копии ваших данных. В случае аварии основного ЦОДа технология решение обеспечит незамедлительное развертывание одного или нескольких резервных серверов, готовых принять на себя нагрузку центрального офиса и филиалов.

Решение выполняет миграцию рабочих нагрузок между физическими, виртуальными и облачными платформами с минимальными перебоями в работе пользователей, т.е. может функционировать и в

рабочее время. Решение не требует приобретения дополнительного оборудования и аренды выделенных каналов связи.

Важной функцией решения ActiveCloud DRS с технологией Double-Take является возможность внедрения Windows Server Failover Clustering без общего хранилища, что устраняет «слабое звено» и обеспечивает возможность свободно располагать кластерные узлы в любом месте.

Внедрение решения ActiveCloud DRS позволит обойтись без строительства центров обработки данных и внедрения оборудования, которое будет загружено максимум на 20%. Поддержка решения ActiveCloud DRS осуществляется силами специалистов предприятия или компанией ActiveCloud.

Пирамида защиты ActiveCloud DRS

Облачный резервный ЦОД ActiveCloud DRS обеспечивает полное резервирование IT-инфраструктуры и приложений предприятия — из одного ЦОД в резервный или в облако. Технология работает в реальном масштабе времени на ограниченных сетевых каналах с информационными системами любой степени распределенности.

Чтобы разработать стратегию защиты с использованием резервного облачного ЦОДа, необходимо выделить среди корпоративных приложений и данных те, которые являются критически важными, и менее критичные.

Как критические важные, так и менее критичные серверы и приложения организации должны быть защищены от логического повреждения данных при помощи ActiveCloud DRS.

Для критичных серверов необходима индивидуальная защита каждой виртуальной машины с агентами и расширенный канал связи, что обеспечит восстановление в случае сбоя в реальном масштабе времени — т.е. менее, чем за секунду, и период простоя не более получаса.

Для защиты менее критичных приложений нет необходимости оптимизировать канал связи и использовать агентов Double-Take. Восстановление в этом случае также занимает не более секунды, но выполняется по требованию.

Как внедрить ActiveCloud DRS?

Для внедрения ActiveCloud DRS специалисты ActiveCloud изучат IT-инфраструктуру организации и предложат решение, адекватное поставленным задачам. Предложенное решение будет обосновано подсчетом полной стоимости владения на базе ActiveCloud DRS и альтернативными вариантами.

Следующим шагом будет пилотный проект, в рамках которого специалисты ActiveCloud настроят репликацию тестового сервера заказчика (физического или виртуального) в облако. Далее заказчик выключит тестовый сервер, и инженеры ActiveCloud в течение 15 минут восстановят его в облаке. Период планирования и внедрения решения ActiveCloud DRS, включая обязательное тестирование планов восстановления, занимает от нескольких дней до нескольких недель. Затраты на резервную IT-инфраструктуру на базе ActiveCloud DRS на порядки ниже, чем требуется для строительства физического резервного ЦОДа и полного создания физической резервной IT-инфраструктуры.

Дальнейшая оптимизация затрат на облачную инфраструктуру достигается путем приобретения облачной IT-инфраструктуры и виртуальных серверов, а также необходимого программного обеспечения, по программе аренды и необходимой консалтинговой помощью. Полученную экономию можно направить на оптимизацию бизнес-процессов и развитие бизнес-приложений при помощи IT.

Облачные технологии в кризис:
ВОДОПАД ВОЗМОЖНОСТЕЙ
Расслабьтесь...
Деньги — не главное!

Более чем двукратное повышение курса рубля остановило закупки нового оборудования для многих компаний.
Однако стоимость облачных вычислительных мощностей в Softline не подорожала!
Этот факт, а также отсутствие необходимости платить за проект сразу, сделало облачные сервисы самым быстрорастущим направлением Softline в первом квартале 2015.

Итак, вполне реально сократить IT-бюджет за счет переноса части CAPEX в OPEX!

Капитальные затраты: «платим все сейчас»	**Операционные затраты: «платим каждый месяц»**
Покупка оборудования	Вычислительные мощности из облака или аренда оборудования из дата-центров Softline
Покупка ПО	Аренда ПО
Резервный ЦОД	Резервирование в облако

Какие типы бизнес-приложений в первую очередь переносятся в облака?

Все базовые сервисы: почту, 1С, файловое хранилище. Это позволяет предприятию обеспечить свою работу вне зависимости от состояния собственной серверной комнаты и почти полностью снять с себя вопросы покупки и обслуживания серверного оборудования.

Отказ от значительных инвестиций позволяет многим компаниям не только продержаться в условиях драматического сокращения IT-бюджета, но и значительно снизить риски неправильного прогнозирования.
Очень сложно сказать, как будет развиваться бизнес хотя бы через полгода, поэтому есть очень большой риск, что купленная инфраструктура будет недозагружена или наоборот — ее мощностей не будет хватать.
Softline предоставляет бесплатный тестовый период и помощь в миграции. Датацентры Softline находятся в Москве (кластер из двух ЦОДов), Санкт-Петербурге, Новосибирске и Владивостоке.

Леонид Аникин,
руководитель направления облачной инфраструктуры Департамента облачных технологий

Проект миграции почтового сервиса Правительства Сахалинской области

О проекте

Заказчик:
Правительство Сахалинской области через ГБУ «Сахалинский областной центр информатизации» (СОЦИ)

Отрасль:
государственная

Размер:
более 1500 пользователей

Проект:
консалтинг

Результаты:
подготовлен план миграции почтовой системы заказчика на более современную версию платформы, техническое обоснование проекта, описание его этапов и особенностей функционирования решения.

О заказчике

Заказчиком со стороны Правительства Сахалинской области выступало ГБУ «Сахалинский областной центр информатизации» (СОЦИ) — государственное учреждение, развивающее систему межведомственного электронного взаимодействия (СМЭВ), а также обеспечением работоспособности IT-сервисов.

Ситуация

Ранее в Правительстве Сахалинской области использовалась почтовая система на базе Exchange 2007, обеспечивающая работу более 1500 пользователей. Для подключения сотрудников органов исполнительной власти региона к современным средствам корпоративных коммуникаций заказчиком было принято решение о миграции с Microsoft Exchange Server 2007 на версию 2013.

Решение

Специалисты Softline предложили реализовать проект в рамках программы поддержки вендором корпоративных клиентов (Software Assurance Deployment Planning Services). Использование таких ее преимуществ, как оперативный доступ к новым продуктам, выгодные условия рассрочки платежей, разработка плана развертывания систем и приложений позволит заказчику получить максимальный возврат инвестиций и сэкономить бюджетные средства.

Основными задачами проекта были: предоставление в рамках обновленной версии возможности обмена почтовыми сообщениями на базе Microsoft Outlook, доступа к корпоративным почтовым ящикам через веб-интерфейс. Также необходимо было проконсультировать заказчика по вопросам предоставления внешним сотрудникам удаленного доступа к корпоративной почте с использованием существующей системы сетевой безопасности на основе решения Microsoft Forefront TMG.

Результаты

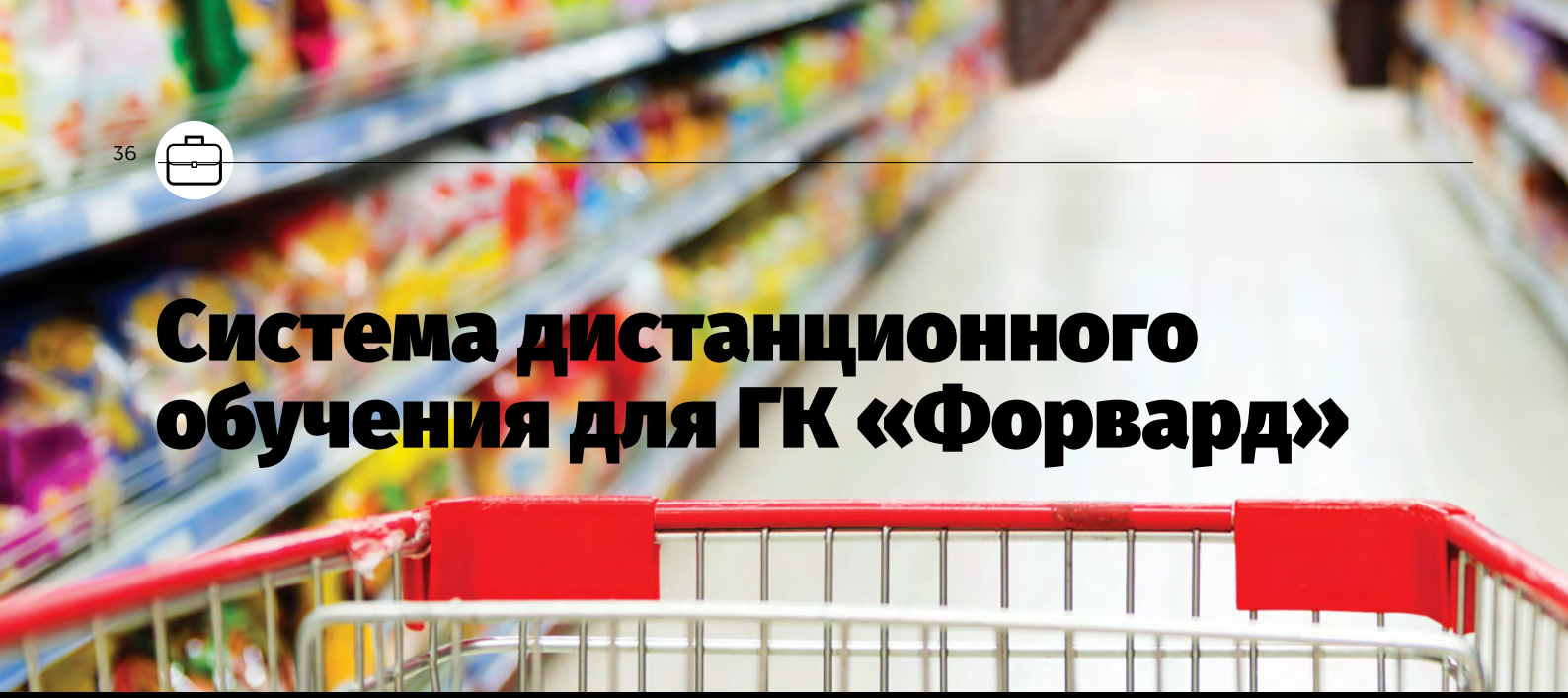
В ходе проекта специалистами Softline было разработано техническое задание на осуществление миграции, которое включало программу-методику испытаний. Помимо этого, была предоставлена архитектурная и эксплуатационная документация для MS Exchange Server 2013.

Мы получили подробные сведения о функционале предложенного решения, поэтапный план миграции и состав работ. Поскольку сервис электронной почты является одним из ключевых для взаимодействия Правительства и органов исполнительной власти Сахалинской области, одним из условий, отраженных в документации, было выполнение миграции во внерабочее время. Специалисты Softline оказывали поддержку на каждом этапе работ, что стало одним из факторов успешной реализации проекта миграции.

Егор Недбай, начальник аппаратно-технологического отдела ГБУ «Сахалинский областной центр информатизации»

Нами был подготовлен подробный план по развертыванию системы Microsoft Exchange Server 2013 и прописан порядок поэтапной миграции почтовых ящиков после завершения настройки системы. Заказчику было предоставлено решение, обеспечивающее непрерывный доступ пользователей к почтовым ящикам, календарям, планировщику задач, сервисам совместной работы, — как через браузер, так и локально, с мобильного устройства или ПК. Кроме того, механизм встроенного мониторинга рабочих процессов запускает самовосстановление сервиса после сбоев в системе.

Павел Моругов, менеджер по продаже решений Softline в Хабаровске



Система дистанционного обучения для ГК «Форвард»

О ПРОЕКТЕ

Отрасль:
продажа и производство продуктов питания

Заказчик:
Группа компаний «Форвард» развивает три основных направления деятельности: розница, опт и производство продуктов питания. Головной офис компании находится в Уфе. Розничное звено группы представлено магазинами «Йомарт» и «Полушка» (в сети более 200 социально-ориентированных магазинов, расположенных на территории Башкортостана, Оренбургской области и Татарстана).

Ситуация:
компания нуждалась в организации единого пространства для обучения и обмена материалами, предоставляющего возможность получения аналитической информации об уровне подготовки специалистов

Решение:
создание универсальной системы дистанционного обучения персонала на платформе Microsoft SharePoint 2013

Ситуация

В территориально-распределенных филиалах с большим числом сотрудником наблюдались определенные сложности с выделением подготовленных для обучения помещений. Кроме того, образовательные планы компании ограничивались штатным числом преподавателей. Эти факторы стали предпосылками создания универсальной системы дистанционного обучения персонала.

Решение

В качестве партнера проекта была выбрана компания Softline, специалисты которой имеют обширный опыт разработки и внедрения подобных систем для организаций различных отраслей экономики.

В рамках проекта было реализовано решение, позволяющее участвовать в образовательном процессе нескольким группам пользователей – преподавателям, ученикам, руководителям. При этом каждая группа имела соответствующие права доступа. Сотрудники, выступающие в роли преподавателей, могут создавать в системе библиотеки и базы знаний, курсы и учебные модули, наполнять их материалами, промежуточными и финальными тестами. Каждый курс ориентирован на конкретную группу учеников. В процессе обучения слушатели не только получают постоянный доступ к знаниям, но и имеют возможность ознакомиться с персональной статистикой по пройденным курсам, а также иметь под рукой календарь предстоящих. Руководители могут обучаться сами, а также просматривать сводные образовательные отчеты по своим подчиненным. Гибкая система уведомлений стимулирует всех участников процесса планировать время обучения и укладываться в отведенные сроки.

Система рассчитана на 3000 пользователей и обладает интуитивно понятным интерфейсом. Кроме этого, она поддерживает возможность дальнейшей модернизации и уже в ближайшем будущем, согласно планам компании «Форвард», может стать частью корпоративного портала.

Решение позволило нам полностью обеспечить преподавателей средствами подготовки и проведения курсов удаленного обучения, а также возможностью контроля за усвоением материала. Сотрудники получили возможность обучаться в удобном для них формате, а руководство — эффективный инструмент сбора и анализа данных по аттестации персонала.

Ирина Валентинова,
руководитель службы управленческого учета ГК «Форвард»

«Новаком» получила награду от Directum

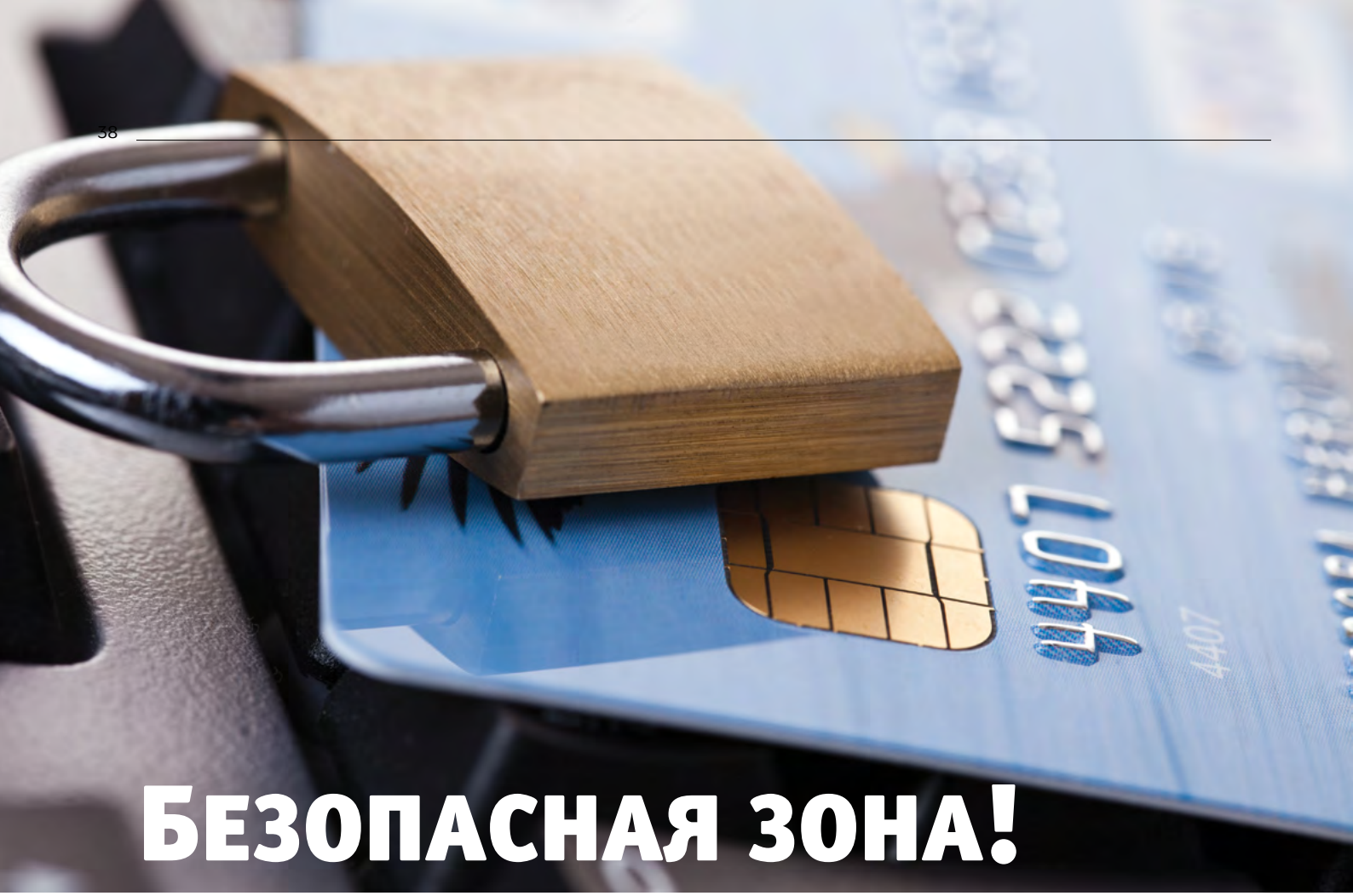
Компания «Новаком», входящая в ГК Softline, объявляет о получении награды Directum «За самое большое количество проектов». В 2014 году было реализовано более 20 новых совместных проектов — это впечатляет.

В рамках прошедшего в Сочи ежегодного партнерского форума Directum компания «Новаком» была признана лидером по количеству реализованных проектов в России и СНГ на платформе Directum.

Компания Directum — ведущий разработчик решений для электронного документооборота. ECM-система вендора позволяет строить инфраструктуру электронного взаимодействия, закрывающую различные задачи бизнеса на разных уровнях: от делопроизводителей — до топ-менеджмента.

Сотрудничество «Новаком» и Directum началось в 2008 году. За это время было реализовано более 100 крупных проектов на территории России и стран СНГ. В 2014 году портфель пополнился еще 20 новыми совместными кейсами, — и это без учета проектов по расширению, дополнению и реализации новых потребностей тех клиентов, у которых решение было внедрено ранее. В числе наиболее значимых заказчиков можно отметить: Министерство по налогам и сборам Республики Беларусь (МНС РБ), «Главное хозяйственное управление» Управделами Президента РБ, «МТБанк».

DIRECTUM
электронный документооборот



Безопасная зона!

Дата-центры Softline подтвердили соответствие требованиям по обеспечению безопасности данных о держателях платежных карт.

Payment Card Industry Data Security Standard (PCI DSS) — стандарт безопасности индустрии платежных карт. Он разработан советом по безопасности, учрежденным представителями крупных международных платежных систем: Visa, MasterCard, American Express и др. Наличие у ЦОДа сертификата PCI DSS гарантирует защищенность от потенциального мошенничества или кражи информации при расчете с использованием карт. Требования стандарта соблюдаются в кредитно-финансовых учреждениях, торговых точках, процессинговых центрах, являются обязательными для систем электронной коммерции и организаций с большим объемом транзакций.

Согласно заключению сертифицированного аудитора, Softline может размещать в облаке IT-сервисы организаций, которым необходим повышенный уровень конфиденциальности данных.

Леонид Аникин, руководитель облачной инфраструктуры компании Softline.

Softline и DataLine: крупнейший в России и СНГ контракт по программе vCAN

Компания Softline и сервис-провайдер DataLine заключили трехлетний договор на аренду лицензий VMware по программе vCloud Air Network (vCAN). Данный проект стал самым крупным за всю историю работы этой программы на территории России и СНГ!

Соглашение Cloud ELA — важное событие для развития рынка аренды ПО. Это демонстрирует, что данный сегмент укрепляется, что в IT-аутсорсинг и облачные сервисы вкладываются все большие деньги. С другой стороны, качество предоставления cloud-услуг за последние два года существенно повысилось. Соответственно, крупные заказчики из разных отраслей постепенно преодолевают недоверие к «облакам». Сочетание качества, удобства и экономии оказывается неоспоримым аргументом при выборе «чужой» IT-инфраструктуры вместо построения, развития и сопровождения собственной.

Сергей Василевич,
менеджер по развитию
бизнеса Softline

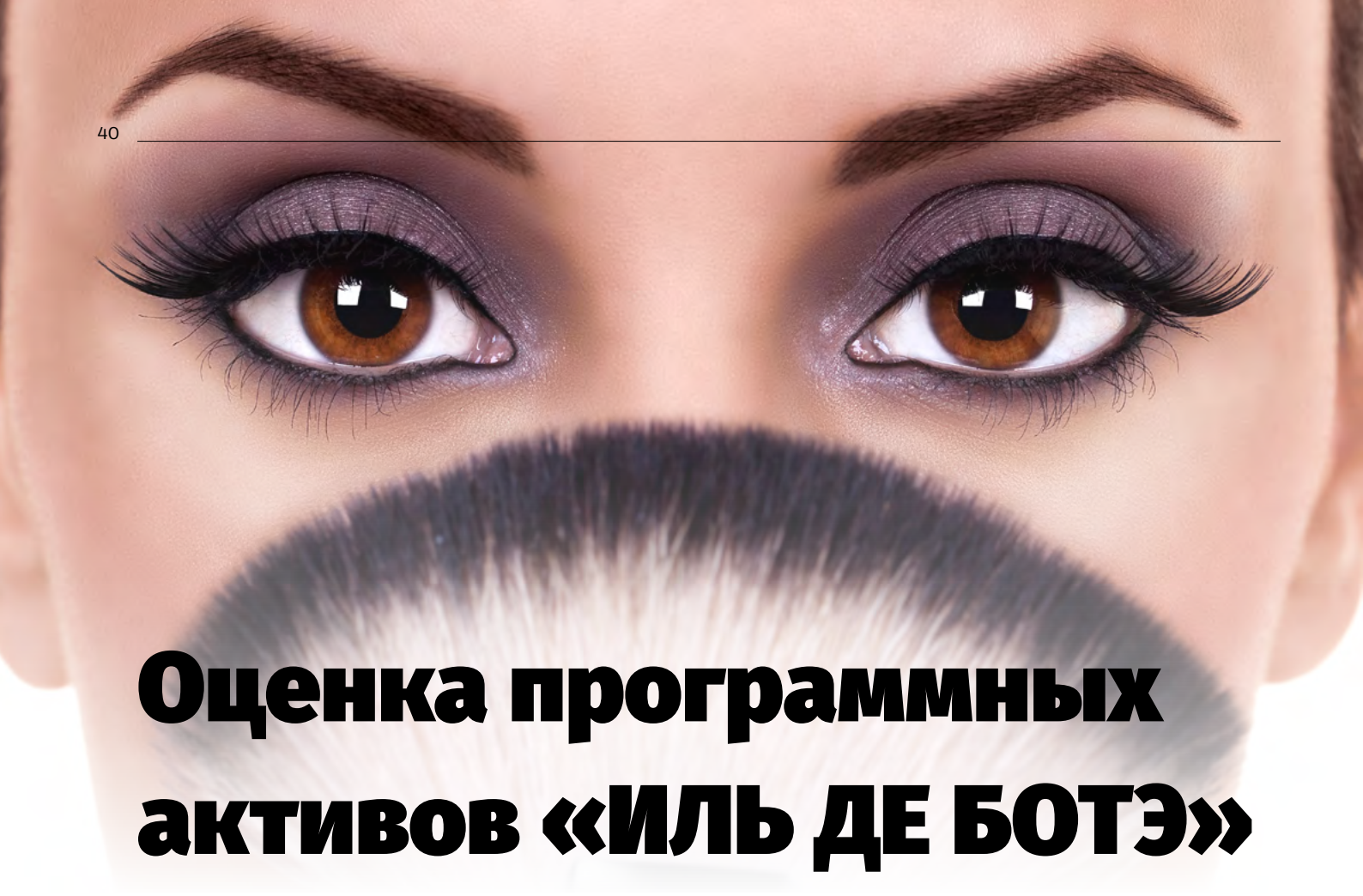
Программа vCloud Air Network

Разработанная специально для сервис-провайдеров, она дает возможность оказывать услуги по предоставлению виртуальной инфраструктуры конечным пользователям на базе технологий VMware — программного обеспечения, предоставляемого в аренду. В числе таких сервисов — стандартные облачные модели: SaaS, IaaS, DaaS, PaaS. Ключевыми преимуществами программы являются подключение без первоначальных вложений, обширный набор предоставляемых услуг, маркетинговая поддержка вендора и оплата по принципу Pay as you go, Pay as you grow, то есть по факту использования ПО в течение месяца.

Softline была одной из первых российских компаний, получивших статус VSPP Aggregator в соответствии с программой vCloud Air Network (ранее — VMware Service Provider Program). На протяжении нескольких лет направление аренды лицензий VMware успешно развивается. Сегодня Softline активно сотрудничает более чем с 35 партнерами по данной программе.

Плоды сотрудничества

DataLine — единственный в России сервис-провайдер уровня Premier по программе аренды ПО VMware — является специализированным поставщиком услуг IT-аутсорсинга на базе собственной сети дата-центров Tier 3 в Москве. Сотрудничество компаний Softline и DataLine по программе аренды VMware началось в 2011 году. В DataLine развернуты несколько платформ для предоставления виртуальной инфраструктуры, в том числе и по технологиям VMware. За время партнерства спрос на аренду лицензий со стороны заказчиков значительно вырос, и в 2014 году DataLine вышла на больший уровень потребления услуг и получила специальные условия от вендора — Cloud Enterprise License Agreement (ELA). Это позволяет компании в течение трех лет предоставлять заказчикам услуги на базе ПО VMware по более выгодной цене. В настоящее время это первый трехгодовой контракт подобного масштаба на территории России и СНГ.



Оценка программных активов «ИЛЬ ДЕ БОТЭ»

Компания «ИЛЬ ДЕ БОТЭ», входящая в группу компаний LVMH, провела инвентаризацию программных продуктов Microsoft с целью проанализировать свои активы и разработать стратегию лицензирования на ближайшие 3-5 лет.

«ИЛЬ ДЕ БОТЭ» — одна из крупнейших в России розничных сетей парфюмерно-косметических товаров. Более 140 магазинов работают во всех крупных городах страны: от Калининграда до Владивостока. Территориально распределенная IT-инфраструктура компании, состоящая из 500 ПК, 200 планшетов, 13 физических и 39 виртуальных серверов, нуждалась в «тонкой настройке» всех ее составляющих. IT-департаменту был необходим постоянный доступ к информации о текущем состоянии и стоимости обслуживания программных активов Microsoft, для чего и был реализован проект Software Asset Management (SAM).

Кроме того, компания планирует обновить свой компьютерный парк, и инвентаризация программного обеспечения помогла не только подтвердить лицензионное соответствие ПО, оценить его объем и актуальность, но и наметить оптимальные пути для модернизации всей IT-инфраструктуры компании.

Тонкая настройка

Внешне розничная торговля парфюмерией и косметикой напоминает сплошной праздник: просторные светлые залы, благоухание изысканных ароматов, утонченные покупатели. Неплохо и с точки зрения организации бизнеса: нет нужды занимать большие площади под складские помещения, ведь компания торгует товаром, спрос на который не закончится никогда. Однако на практике бизнес по продаже духов и пудры столь же труден, как и любой другой. И специализированная розничная сеть — весьма сложный «организм», нуждающийся в грамотном менеджменте и тонкой настройке всех его составляющих.

Чистая работа

В ходе проекта анализировалась лицензионная чистота десктопных систем, работающих под управлением Microsoft Windows, серверных систем, баз данных Microsoft SQL, средств разработки Microsoft Visio и Microsoft Project Manager. Инвентаризация программных активов, проведенная IT-департаментом совместно с компанией-партнером Softline, позволила точно установить объем используемого в «ИЛЬ ДЕ БОТЭ» ПО — лицензионная чистота составила более 95%.

«Мы весьма щепетильно относимся к использованию программных продуктов и были удовлетворены тем, что инвентаризация еще раз подтвердила лицензионную чисто-

ту нашего ПО. Но ценность проекта для компании была не только в этом. Специалисты Softline помогли нам подобрать оптимальные модели лицензирования, указали на ряд устаревших систем (Microsoft Windows XP и Microsoft Office 2003), которые до сих пор использовались на ряде компьютеров, — говорит Заместитель начальника отдела сопровождения бизнес процессов Александр Макар. — Это особенно важно для нас еще и потому, что на 2015-2016 гг. запланировано значительное обновление парка персональных компьютеров, которые будут приобретаться вместе с предустановленным программным обеспечением».

Еще один результат проекта, по мнению Александра Макара, в том, что компания «ИЛЬ ДЕ БОТЭ» получила инструмент для самостоятельного анализа своих программных активов. Заместитель начальника отдела сопровождения бизнес процессов замечает, что периодическую инвентаризацию используемого ПО необходимо проводить постоянно: она помогает и обеспечивать лицензионную чистоту ПО, и сверять соответствие IT-инфраструктуры дорожной карте ее развития.

Microsoft SAM Services

«Наш проект в компании «ИЛЬ ДЕ БОТЭ» проводился в рамках программы Microsoft SAM Services, — рассказывает IT-консультант департамента управления лицензиями компании Softline Антон Белошицкий. — Эта программа инициирована корпорацией Microsoft и направлена на популяризацию среди клиентов корпорации управленческого подхода при покупке и использовании программных активов. Мы, как крупнейший партнер Microsoft в России, заняты реализацией этой программы, а ее финансирование осуществляется самой корпорацией».

Для проведения инвентаризации использовались автоматизированные средства учета и анализа программного обеспечения от разных производителей: средства Антивируса Касперского, программа iTMan, разработанная Softline, и Microsoft MAP. Полученные данные прошли выборочную проверку на предмет корректности полученных сведений. Еще одна составная часть проекта — сбор правоустанавливающих документов, который проводился в различных структурных подразделениях «ИЛЬ ДЕ БОТЭ»: бухгалтерии, IT-департаменте. Кроме того, была проведена проверка OEM-лицензий на предустановленное ПО, приобретенное в комплекте с оборудованием. После сверки лицензий и завершения проверки лицензионной чистоты ПО был подготовлен итоговый отчет. Весь проект был реализован в течение двух месяцев.

Проще, чем кажется!

«Признаться, мы не ожидали, что проект удастся осуществить настолько просто и быстро. Нас смущал довольно большой объем работ, связанных со сбором необходимых финансовых и юридических документов, а также сам процесс проверки ПО на лицензионную чистоту. Такие задачи не свойственны нашим техническим специалистам, — рассказывает Александр Макар. — Однако, на практике оказалось, что эта часть проекта не столь обременительна: большую роль сыграло участие в проекте специалистов Softline, которые прекрасно организовали работу по первичному сбору и анализу необходимой информации. Не могу не отметить, что они одинаково глубоко знают и особенности лицензирования, и авторское право, и тонкости управления программными активами предприятия».

Проекты по оценке активов программного обеспечения часто помогают заказчику решить попутно целый ряд смежных задач. Не стал исключением и проект в «ИЛЬ ДЕ БОТЭ». Крупного ритейлера ожидает весьма значительное обновление компьютерного парка. Благодаря инвентаризации используемого ПО мы смогли подготовить рекомендации относительно очередности выполнения обновлений. Кроме того, в ходе анализа были выявлены проблемные места в IT-инфраструктуре заказчика, вызванные прежде всего использованием устаревшего программного обеспечения.

Антон Белошицкий,
IT-консультант департамента управления лицензиями компании Softline

Техподдержка для «Мэйертон Инжиниринг»

Softline реализовала проект по технической поддержке IT-инфраструктуры компании «Мэйертон Инжиниринг». Заказчик получил единую точку входа для оперативного решения технических вопросов, была обеспечена устойчивость IT-систем и удобство работы пользователей.

Цель — никаких простоев!

Перед руководством компании стояла цель обеспечить бесперебойное функционирование IT-инфраструктуры, минимизировав тем самым вынужденные простои рабочих станций пользователей.

Оптимальная стоимость, и только то, что нужно!

В рамках проекта специалисты Softline предложили заказчику стандартный пакет услуг, полностью удовлетворяющий текущие потребности по мониторингу IT-систем. «Мэйертон Инжиниринг» была предоставлена выделенная линия для разрешения технических запросов посредством службы ServiceDesk, электронной почты, а также по телефону. Было настроено и установлено сетевое оборудование; обеспечено управление офисным ПО; предоставлены услуги технического менеджера. Сервисом были обеспечены технические, почтовые и прокси-серверы, а также рабочие станции пользователей (ноутбуки и ПК), периферийное оборудование, системы безопасности.

Результаты

В результате у компании отпала необходимость в найме собственных технических специалистов, что позволило существенно сэкономить средства. При этом полностью была обеспечена отказоустойчивость инфраструктуры и получены все необходимые услуги для корректной работы IT-сервисов.

«Мэйертон Инжиниринг» занимается производством и поставкой огнеупорных материалов для металлургии. Компания имеет представительства в 50 странах, являясь стратегическим партнером для крупнейших промышленных предприятий.

Услуги технической поддержки, предоставленные специалистами Softline, повысили качество работы ключевых IT-сервисов компании, что позволило минимизировать риски простоя рабочих станций пользователей и обеспечить непрерывность IT-процессов.

Михаил Мальков, директор «Мэйертон Инжиниринг»

Корпоративный портал «МегаФона» на Урале поддерживает Softline

О проекте

Отрасль:
телеком

Заказчик:
«МегаФон» на Урале

Количество сотрудников call-центра:
более 200

Решение:
выделенная линия для разрешения технических запросов

Результат:
круглосуточная техническая поддержка и усовершенствование системы поиска на «Корпоративном портале знаний» Уральского филиала компании «МегаФон». Специалисты оператора значительно ускорили обработку заявок абонентов

«МегаФон» на Урале предоставляет услуги связи и скоростного мобильного Интернета в 10 регионах: Свердловской, Челябинской, Тюменской, Кировской, Курганской областях, Пермском крае, Республике Коми и Удмуртской Республике, ХМАО и ЯНАО. Абонентами оператора являются более 5 800 000 уральцев.

Благодаря услугам техподдержки Softline нам удалось улучшить работу «Корпоративного портала знаний» — одного из основных информационных источников в работе специалистов call-центра и фирменных салонов. По итогам ежегодного исследования уровня удовлетворенности пользователей работой информационных систем, служба поиска на портале получила оценку 100 баллов из 100 возможных. Это свидетельствует об успешной реализации проекта и его значимости для нас.

Александр Тропец, руководитель по продажам и обслуживанию компании «МегаФон» на Урале

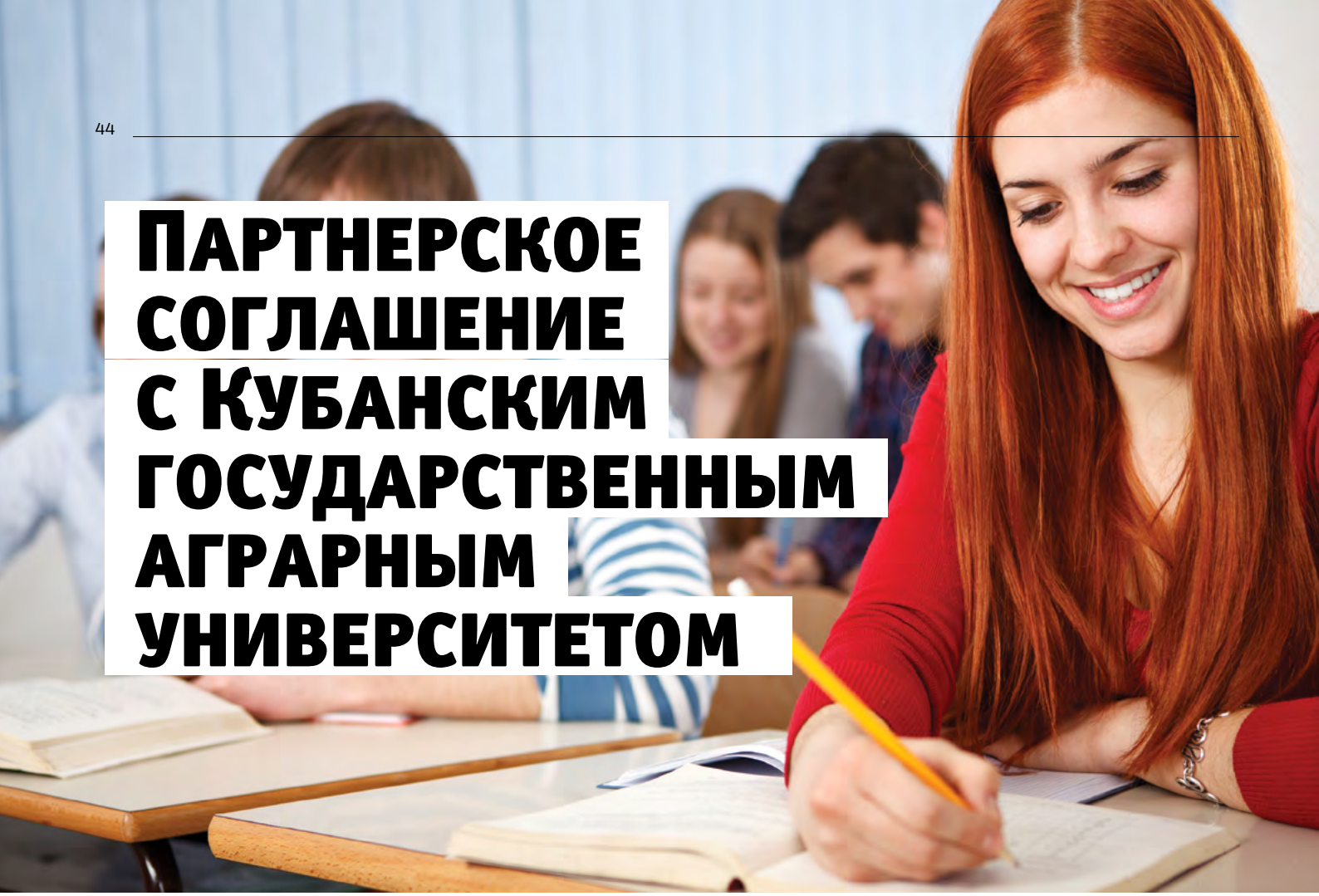
Ситуация

Сервисную поддержку клиентов «МегаФона» осуществляет call-центр, сотрудники которого являются пользователями «Корпоративного портала знаний», функционирующего на базе SharePoint 2013. Для обеспечения бесперебойной работы call-центра, оптимизации поиска нужной информации и ускорения реагирования на запросы абонентов заказчик принял решение о передаче на аутсорсинг задач по технической поддержке работы портала.

В рамках проекта специалисты Softline предоставили заказчику выделенную линию для разрешения технических запросов. Пользователи могут обратиться за помощью посредством службы Service Desk, электронной почты, телефонной связи. Помимо этого, Softline взяла на себя диагностику сбоев и отказов в системе и их устранение, а также установку обновлений портала.

Результаты

Все услуги оказываются в режиме 24/7, что обусловлено круглосуточным режимом работы call-центра. Специалисты Softline усовершенствовали функционал поисковой системы за счет добавления возможности ошибочного или вариативного написания слов, автоматического распознавания транслитерации. В результате повысилась скорость обработки запросов пользователей, что позволило осуществлять консультативную помощь более эффективно. Помимо работников call-центра, удобство использования «Корпоративного портала знаний» повысилось для менеджеров по продажам и консультантов, которые также имеют доступ к корпоративной информации. Таким образом, они смогли более оперативно находить необходимые сведения, тем самым улучшая качество работы с покупателями.



Партнерское соглашение с Кубанским государственным аграрным университетом

Учебный центр компании Softline и Кубанский государственный аграрный университет стали партнерами. Сотрудничество предоставляет возможность проводить IT-курсы на базе высшего учебного заведения как для специалистов вуза, так и для заказчиков всего региона.

История и перспективы

Компания Softline в течение длительного времени является партнером КубГАУ в сфере лицензирования программного обеспечения и поставок оборудования.

КубГАУ — одно из ведущих учреждений высшего аграрного образования в России. В составе вуза — 20 учебных и учебно-лабораторных корпусов, а также библиотека, центр бизнес-образования, компьютерный центр, оснащенный всем необходимым оборудованием.

Первый авторизованный курс Microsoft («Администрирование Windows Server 2012 R2») прошел в компьютерном центре университета в конце прошлого года. Обучение проводил эксперт, имеющий статус Microsoft Certified Trainer. Слушатели получили сведения о поддержке инфраструктуры, управлении данными пользователей и группами в Active Directory, обеспечении защиты сетевого доступа и безопасности данных. По итогам обучения сертификаты получили IT-специалисты КубГАУ, администрации Краснодара, а также компаний «Юг-Инвестбанк», «АЯКС-риэлт» и «Каргилл Юг».

В перспективе планируется регулярное проведение авторизованных курсов Microsoft (администрирование Windows Server, баз данных SQL Server; возможности Exchange, Lync). Готовятся к набору группы слушателей на обучающие программы по решениям Cisco.

Обучение позволило в сжатые сроки получить знания по администрированию Microsoft Windows Server 2012, которые можно применять непосредственно в работе. Хотелось бы отметить высокий уровень профессионализма преподавателя и организации курса.

Сергей Дацюк,
главный специалист управления информационно-коммуникационных технологий и связи администрации Краснодара

Новое облачное бизнес-решение — EMC VSPEX

Softline получила статус EMC VSPEX accredited partner. Партнерство дает возможность предлагать заказчикам облачное решение EMC на базе платформы VSPEX и услуги по его технической поддержке. Помимо этого, компания активно развивает собственную демозону!

Статус VSPEX accredited partner присваивается партнерам EMC, имеющим большой опыт реализации проектов по решениям вендора. Подключившись к партнерской программе, Softline повысила компетенции по комплексному сопровождению облачного решения EMC VSPEX. Новый формат сотрудничества с EMC расширит возможности компании по поставке, внедрению и технической поддержке облачных инструментов вендора.

Использование платформы VSPEX упрощает процесс перехода бизнеса к облачной среде: развертывание не требует интеллектуальной проработки, сокращены этапы внедрения по сравнению с традиционными инфраструктурами. Такое решение повышает эффективность работы IT-сервисов предприятий среднего и малого бизнеса.

EMC VSPEX — это инфраструктура для быстрого перехода к облачным вычислениям, на базе которой строятся простые, эффективные и гибкие архитектурные решения, собранные из оптимальных компонентов. В ее основе лежит платформа хранения данных EMC VNX, которая может быть сконфигурирована и настроена под конечные задачи заказчика и в результате предоставляет им масштабируемый, надежный и экономичный формат хранения данных.

Кто владеет информацией, тот владеет миром!

Известная цитата Натана Ротшильда актуальна и сегодня, разница только в том, что информации, требующей анализа, в сотни раз больше, а времени на детальное изучение все меньше.

Чем полезен «Стахановец»?

Управляющий персонал оценит:

- анализ эффективности использования рабочего времени сотрудниками;
- контроль эффективности работы филиала и удаленных сотрудников;
- анализ системы мотивации и KPI;
- контроль стоимости печати на принтерах.

Служба информационной безопасности сможет:

- использовать «Стахановец» в качестве DLP-системы;
- мониторить подозрительные действия сотрудников;
- предотвращать утечки информации;
- получать объективную информацию в случае расследования инцидентов безопасности.

Работа или только ее видимость?

Уверены ли вы, что:

- сотрудники работают эффективно на 100%, а не создают только видимость деятельности?
- ценная коммерческая информация используется по назначению, а не утекает к конкурентам?
- сотрудники используют ресурсы компании строго на ее благо, а не на развитие собственного бизнеса?
- на печать отправляются документы, необходимые для работы, а не для личных нужд?

Зачастую, доподлинно знать ответы на все эти вопросы руководителю просто невозможно, нельзя же незаметно стоять за спиной у каждого, а между тем по статистике около 70% сотрудников готовы продать информацию конкурентам, 30% случаев утечки происходят на напечатанных документах, 60% времени в Интернете сотрудники тратят на общение и развлечения, 28% времени уходит на неважные для основной работы вещи. Возникает резонный вопрос: должен ли работодатель платить 100% заработной платы за примерно 50% отработанного времени вместо положенных 8 часов в день? Как узнать, кто из сотрудников работает честно, а кто занимается чем угодно, но только не работой?

«Стахановец» — программный комплекс, способствующий руководителю выявить риски, которые могут возникнуть ввиду действий недобросовестных сотрудников, а также определить неэффективных работников и «узкие» места в их работе. Стахановец автоматически регистрирует все действия сотрудников за компьютерами, затем анализирует собранную информацию и сводит в удобный для руководителя отчет.

В каких случаях необходимо внедрение системы контроля?

- Вы считаете, что ваша компания в текущем составе может зарабатывать больше.
- Прибыль стала резко снижаться, а причины вам непонятны.
- Сотрудники ссылаются на высокую загруженность и просят расширить штат.
- Клиенты жалуются на качество обслуживания.
- Требуется сократить штат, а определить, кого именно уволить, сложно.
- Важная коммерческая информация доступна сотрудникам и нужно не допустить утечек.

Таким образом, система контроля работы сотрудников Стахановец позволит вам заранее выявить возможные риски по каждому сотруднику до того, как тот успел совершить вредоносное действие; определить, кто недорабатывает, а кто действительно достоин поощрения; понять, кого сократить, а кого повысить в должности; к кому присмотреться с точки зрения безопасности, а кому вполне можно доверять.

Стахановец
Система контроля сотрудников

50 ЛИЦЕНЗИЙ БЕСПЛАТНО НА 14 ДНЕЙ

Отправьте на demo@stakhanovets.ru письмо с темой «Акция каталог»

В письме укажите:

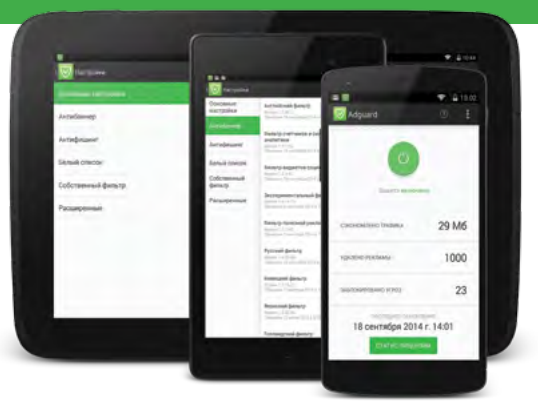
- ваше имя
- название компании
- контактный телефон
- необходимое количество лицензий (до 50)
- дату, когда вы готовы приступить к установке

Ключи к ПК «Стахановец» будут вам направлены в течение следующего рабочего дня после получения запроса. Лицензии начинают действовать в день отправки.

При возникновении вопросов пишите:
marketing@stakhanovets.ru, звоните +7 (495) 272 03 40

www.stakhanovets.ru

В помойку весь рекламный мусор!



Путешествовать по просторам Интернета, не отвлекаясь на вездесущую и навязчивую рекламу, — реально!

Вы совершенно не обязаны наблюдать весь рекламный мусор, который пытаются вывалить на пользователей некоторые рекламодатели. И если в случае рекламы по телевизору остается только смириться, то в сети у вас есть выбор! Все, что вам нужно, — это надежная программа, отвечающая за блокировку ненужных баннеров, видеороликов и других элементов.

Веб-фильтр Adguard

Это уникальная программа, которая сочетает в себе все необходимые функции для комфортного использования Интернетом. Основная задача этого веб-фильтра — качественная блокировка абсолютно всех видов рекламы. Теперь, чтобы посмотреть ролик на Youtube или любимый сериал, вам не придется ждать несколько минут, пока пройдет реклама. Всплывающие окна будут заблокированы, все надоедливые баннеры с отвратительным содержимым исчезнут. Так как все лишние элементы на сайтах удалятся (а их довольно много!) — страницы будут загружаться быстрее. Да, Adguard значительно сэкономит трафик и ускорит Интернет на вашем устройстве.

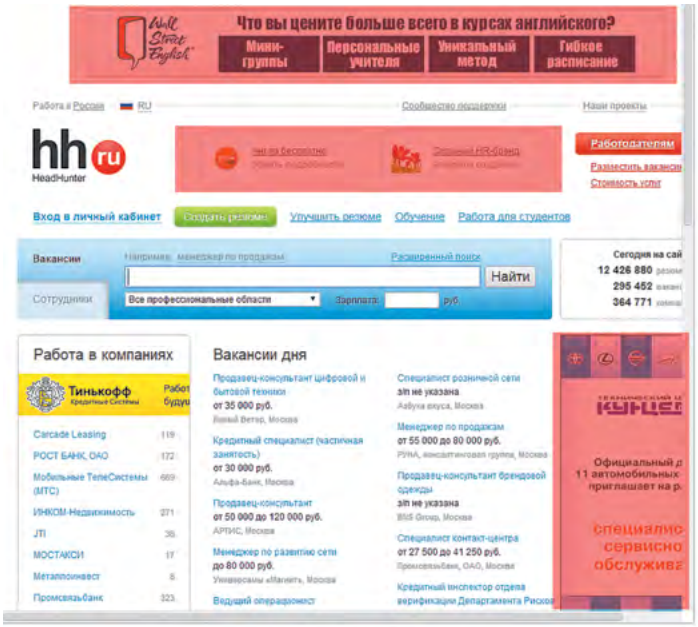
Многофункциональность

Помимо полного удаления рекламы онлайн и в программах на вашем компьютере (Skype, uTorrent) Adguard обладает и другими полезными функциями. Так, отдельный модуль «Антифишинг» защитит пользователей от вредоносных сайтов, фишинга и других возможных онлайн-угроз. Модуль счетчиков и систем аналитики запретит кому-либо следить за вами в сети. А вот модуль «Родительский контроль» необходим всем, у кого дети сидят в Интернете. Блокировка доступа к сайтам для взрослых, фильтрация нецензурных материалов, защита паролем — Adguard защитит маленьких пользователей от информации, которую им знать еще рано.

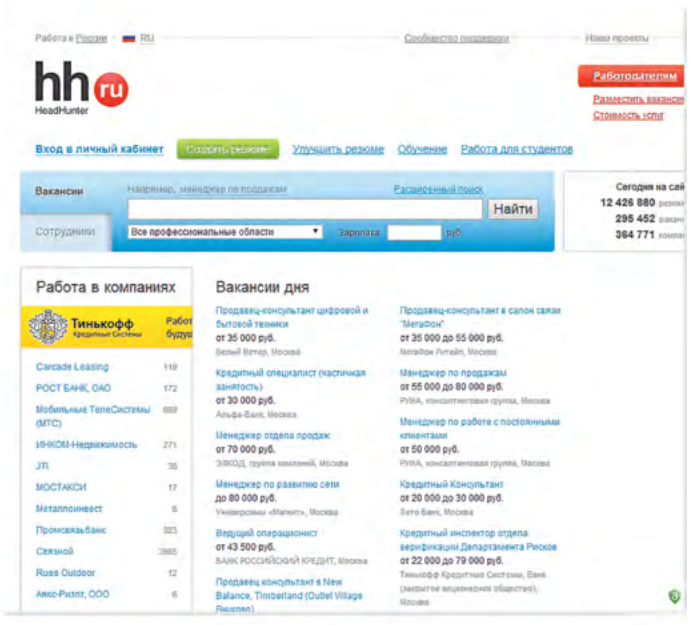
Подробнее о функциях

Итак, Adguard — это блокировка рекламы, защита от онлайн-угроз, защита детей от нецензурных материалов и защита личных данных. Все эти функции представлены соответствующими модулями.

«Антибаннер» полностью удаляет все рекламные элементы с веб-страниц. Блокирует видеорекламу, всплывающие окна, убирает объявления, баннеры и другие материалы



без Adguard



с Adguard

рекламного характера. При этом фильтрация происходит еще до загрузки сайта в браузере, а это значит — никакой рекламы и сокращение времени загрузки сайтов.

«Антифишинг» защищает вас от сайтов, содержащих вредоносный код, а также от сайтов интернет-мошенников. Программа действительно снижает вероятность заражения компьютера вирусами. Adguard использует черные списки, насчитывающие миллионы опасных сайтов. Модуль «Антифишинга» обрабатывает URL-адреса в режиме реального времени — сверяет их с доменами сайтов в своей базе данных. А благодаря оптимизации данного процесса такая проверка занимает доли секунды.

Родительский контроль позволяет защитить детей от вызывающих и нецензурных материалов и сайтов для взрослых, что в целом обеспечивает безопасность детей онлайн. Родители могут быть абсолютно спокойны.

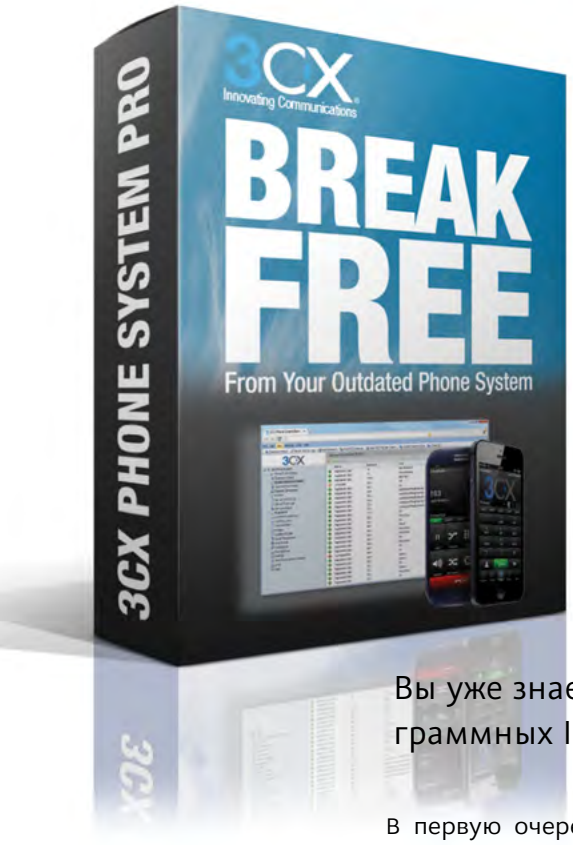
«Антитрекинг» — это защита от посторонних наблюдателей истории вашего серфинга. С Adguard рекламные сети и счетчики не смогут отследить ваши поисковые запросы и посещенные вами сайты и использовать эти данные в корыстных целях.

Для любого устройства

Adguard — эта целая линейка программного обеспечения, а значит, каждый сможет найти веб-фильтр подходящего формата: программа Adguard для Windows для ваших компьютеров и ноутбуков, мобильное приложение Adguard для устройств на базе Android, Adguard для Mac — первый в мире полноценный блокировщик рекламы для OS X.

НЕ ТРАТИМ НЕРВЫ ЗРЯ!

1. Вас не будут отвлекать все эти пестрые, мигающие и просто неприятные баннеры.
2. Больше не нужно ждать, пока наконец пройдет видеореклама.
3. Вы заметите насколько быстрее станет работать Интернет: страницы, не отягощенные ничем лишним, загружаются гораздо быстрее.
4. Вы сможете спокойно позволять детям сидеть в Интернете, так как с Adguard вы будете уверены, что они не увидят ничего лишнего.
5. Adguard — отличное дополнение к антивирусу; предупредит вас об опасности при переходе на подозрительные сайты.
6. Adguard запретит трекинг ваших действий онлайн, таким образом ваши личные данные будут под надежной защитой.
7. Adguard — простая в использовании программа, которая содержит все функции, необходимые каждому интернет-пользователю. Работает незаметно, в фоновом режиме, вы увидите только результат — чистый и безопасный Интернет.



IP АТС для Windows

От возможностей к эффективности

Вы уже знаете о преимуществах, которые дает использование программных IP АТС?

В первую очередь, это хорошая масштабируемость или возможность без серьезных вложений увеличивать номерную емкость и функциональность. Кроме того, нет необходимости в закупке специального оборудования и прокладке телефонной проводки. Для переговоров можно использовать как программные, так и аппаратные решения. Стоимость междугородних и международных звонков можно снизить за счет использования операторов IP-телефонии. Наконец, предоставляется возможность иметь прямой городской номер в нескольких городах.

Все это традиционные аргументы. 3CX подходит к вопросу IP АТС немного с другой стороны. Экономия, конечно, является важным параметром, и она, безусловно, присутствует (можно просто сравнить цены с конкурентами), но для наших заказчиков не менее важна эффективность работы, и в первую очередь это касается связи.

Возможности 3CX

Рассмотрим компоненты самой IP АТС:

- сервер IP АТС 3CX Phone System for Windows, который предлагается в 2 версиях: Standard и Professional;
- программные клиенты 3CXPhone for Windows, iOS, Android и Mac. Все клиенты имеют похожий интерфейс и принципы работы, что полностью соответствует концепции Unified Communications

Эффективность для системного администратора

Программный сервер IP АТС можно установить на любую Windows-платформу, начиная с Windows 7 Professional (т.е. серверная ОС при небольшой нагрузке необязательна), сам процесс занимает около 20 минут, при этом с помощью Мастера можно сразу завести абонентов и подключить VoIP-провайдера по готовым шаблонам.

Для того, чтобы настроить рабочее место клиента для IP-телефона из поддерживаемого списка (Yealink, Fanvil, Snom), достаточно подключить аппарат к локальной сети. 3CX найдет этот телефон и отобразит в панели управления, после чего вам остается просто присвоить ему номер. Для программных клиентов (независимо от платформы) достаточно отправить сотруднику Welcome Email с настройками по электронной почте, и он, кликнув на вложение, настроит свой программный клиент 3CXPhone.

Для удаленных пользователей доступна уникальная технология 3CX Tunnel, которая позволяет подключать программный телефон используя всего один порт, что снижает вероятность односторонней слышимости.

Эффективность для абонентов. Исходящий звонок

Возьмем для примера клиент для Windows, сопряженный с настольным аппаратом. Сразу стоит отметить, что 3CXPhone for Windows может работать в 2 режимах: и как самостоятельный софтфон, и как консоль для настольного телефона (CTI-приложение). Номер можно набрать несколькими способами:

- набрать вручную на настольном аппарате;
- набрать в панели 3CXPhone с клавиатуры или при помощи Copy-Paste;
- кликнуть на контакте Outlook;
- набрать номер из CRM (поддерживается 1С, Microsoft Dynamics, Salesforce и SugarCRM);
- выделить номер мышью в любом приложении и набрать номер при помощи комбинации горячих клавиш (при этом все лишние символы кроме цифр будут удалены);
- звонок будет осуществляться согласно настроенным правам и правилам, т.е. у 3CX есть возможность направить вызов по наиболее дешевому маршруту и, если это нужно, запретить отдельным группам пользователей, например, международные звонки.

Входящий звонок

На стороне IP АТС 3CX вы можете создать приветствие, многоуровневый IVR, организовать очереди или группы агентов для приема звонков. В тот момент, когда звонок будет принят сотрудником компании, система может отобразить карточку контакта из Outlook, 1С, Microsoft Dynamics, Salesforce и SugarCRM.

Видео

Начиная с v12.5 для любой коммерческой версии доступна видеоконференция через браузер Google Chrome на базе технологии WebRTC.

Лицензирование

Лицензируется 3CX крайне просто и прозрачно — по одновременным вызовам. Чтобы понять свои потребности, возьмите 1/3 от количества абонентов — это и будет максимальная нагрузка вашей АТС с точки зрения одновременных звонков в пиковые часы.

Мировой лидер по производству титана выбирает STATISTICA Quality Control от StatSoft

Представляем вашему вниманию интервью с начальником аналитического бюро отдела сертификации ОАО «Корпорация ВСМПО-АВИСМА» Ольгой Ледер.

В интервью Ольга поделилась опытом внедрения инструментов статистического контроля качества продукции на металлургическом предприятии с техническим директором компании StatSoft Russia — Максимом Милковым, который уже 8 лет занимается проблемами промышленной аналитики, руководит и участвует в проектах по внедрению систем статистического управления качеством на предприятиях.

М.Л.: Основные потребители продукции вашего предприятия — это крупнейшие авиа- и двигателестроительные компании. Среди них Boeing, AIRBUS INDUSTRIE, Rolls-Royce plc, Pratt&Whitney. Также вы поставляете изделия для оборонной промышленности Российской Федерации и стран СНГ. Очевидно, что требования к качеству продукции в данных отраслях не просто повышенные, а скорее исключительно высокие.

М.Л.: Расскажите, пожалуйста, вкратце историю организации системы менеджмента качества (СМК) на предприятии, как она развивалась в последние годы. Какие процессы на предприятии охвачены СМК?

О.А.: В 1992 году для обеспечения разработки, введения и поддержания системы менеджмента качества на ОАО «ВСМПО» (Верхнесалдинское металлургическое производственное объединение) была создана служба качества и назначен представитель руководства — директор по качеству и сертификации.

Генеральным директором предприятия утверждена Политика в области качества, введено Руководство по качеству, а также процессы системы менеджмента качества и основополагающие стандарты предприятия, отвечающие требованиям международного стандарта AS/EN 9100 (включая требования ИСО 9001:2000) и стандартов ведущих аэрокосмических фирм мира.

В августе 1993 года созданная на объединении система качества была сертифицирована германской

фирмой «TUV-CERT». Предприятием был получен первый сертификат.

Сегодня ОАО «Корпорация ВСМПО-АВИСМА» сертифицирована практически всеми мировыми производителями авиационно-космической техники: Boeing, Airbus, General Electric, Snecma, Rolls-Royce, Pratt & Whitney и многими другими.

Также объединение сертифицировано на AS9100 «Стандарт системы менеджмента качества – требования для оборонных, авиационных и космических организаций» и ГОСТ Р 9001 «Системы менеджмента качества. Требования».

«Корпорация ВСМПО-АВИСМА» имеет более 300 международных сертификатов на систему менеджмента качества, на методы производства и контроля, на отдельные виды продукции из титана и других материалов.

В настоящее время система менеджмента качества организации распространяется на производство следующих видов продукции: слитки, слябы, листы, плиты, штрипсы, биллеты, поковки кованые и штампованные, прутки катаные, кованые, трубы цельнокатаные и сварные, профили прессованные, панели, кольца цельнокатаные.

Основными заказчиками ОАО «Корпорация ВСМПО-АВИСМА» были и остаются высокотехнологичные отрасли: авиационная промышленность, ракетостроение, судостроение. Поэтому предприятие за весь период своей деятельности обеспечивает достаточно высокий уровень качества своей продукции.

М.Л.: Аналитическое бюро является неотъемлемым компонентом в структуре СМК. Расскажите, пожалуйста, о задачах, которые решает ваше бюро.

О.А.: Количество существующих методов производства на ВСМПО весьма велико — более тысячи. При этом производственные циклы изготовления изделий могут состоять более чем из двухсот операций. Повышенные требования к качеству продукции делают актуальными работы по улучшению стабильности и качества процессов. Основная задача бюро — внедрение на ВСМПО методологии непрерывного совершенствования процессов с применением статистических методов, требующей разработки и автоматизации процедур статистического управления производством.

М.Л.: Любому аналитику для эффективной работы нужен современный инструмент, ведь время миллиметровки и логарифмических линеек давно ушло. Если не секрет, поделитесь, чем пользуются сотрудники вашего предприятия.

О.А.: Системный статистический анализ невозможен без компьютерных технологий. В организации базовым статистическим программным продуктом является лицензионный пакет *STATISTICA* компании StatSoft.

М.Л.: Обрабатывать данные можно и в Excel, почему вы выбрали специализированное решение?

О.А.: Во-первых, *STATISTICA* является мощной аналитической системой для профессионального анализа, что позволяет решать широкий круг задач любой сложности.

Во-вторых, *STATISTICA* обеспечивает надежную реализацию статистических методов анализа. Кроме того, программа полностью переведена на русский язык, включая интерфейс, документацию и справочное руководство. Есть дополнительная литература по применению данного пакета и большой выбор графических инструментов.

Excel мы тоже используем под определенные задачи в силу его доступности широкому пользователю. Но смогли грамотно подойти к использованию Excel, уже имея навыки работы в *STATISTICA*.

М.Л.: Коробочный продукт для его полноценной эксплуатации зачастую требует адаптации под конкретное производство. Насколько удалось интегрировать пакет *STATISTICA* с базами данных предприятия. Используете ли вы стандартные модули программы или были реализованы специализированные интерфейсы под нужды аналитиков?

О.А.: Для управления технологическими процессами в организации на базе программного продукта *STATISTICA* специалистами аналитического бюро разработана автоматизированная система статистического контроля технологических процессов (АС СКТП), адаптированная под продукцию предприятия. Сбор данных, необходимых для выполнения статистического анализа в АС СКТП, организован непосредственно из базы данных АИС ЛКП (автоматизированная информационная система «Лабораторный контроль продукции»).

АС СКТП позволяет:

- выполнять статистический контроль ключевых характеристик всей продукции ВСМПО (механические и химические свойства);
- обеспечивать специалистов оперативной аналитической информацией о стабиль-

Ольга Ледер начала свою деятельность по внедрению статистического управления процессами на ВСМПО в 2005 году во вновь созданном по решению генерального директора отделе повышения эффективности производства. С 2009 года продолжила работу по данному направлению в службе качества.

Статистические методы оценки влияния факторов на процесс

Однофакторные методы		Многофакторные методы	
Графические методы	Аналитические методы	Регрессионный анализ	Планирование эксперимента
Ящичная диаграмма	T-критерий Стьюдента		
	U-критерий Манна-Уитни		
Диаграмма рассеивания	Дисперсионный анализ		
	Критерий Краскела-Уоллиса		
Круговая диаграмма	Корреляция Спирмена		
	Корреляция Пирсона		
	Корреляция Кендела		

Рисунок 1.

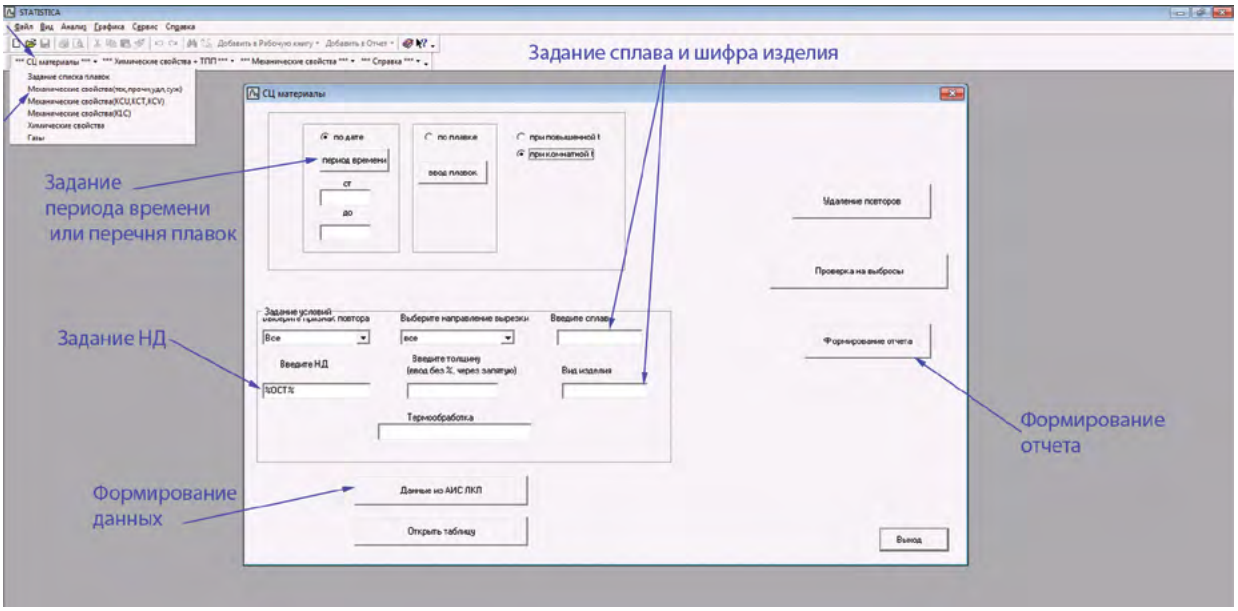


Рисунок 2. Пример диалогового окна для формирования отчета по оценке механических свойств при сертификации авиационных материалов

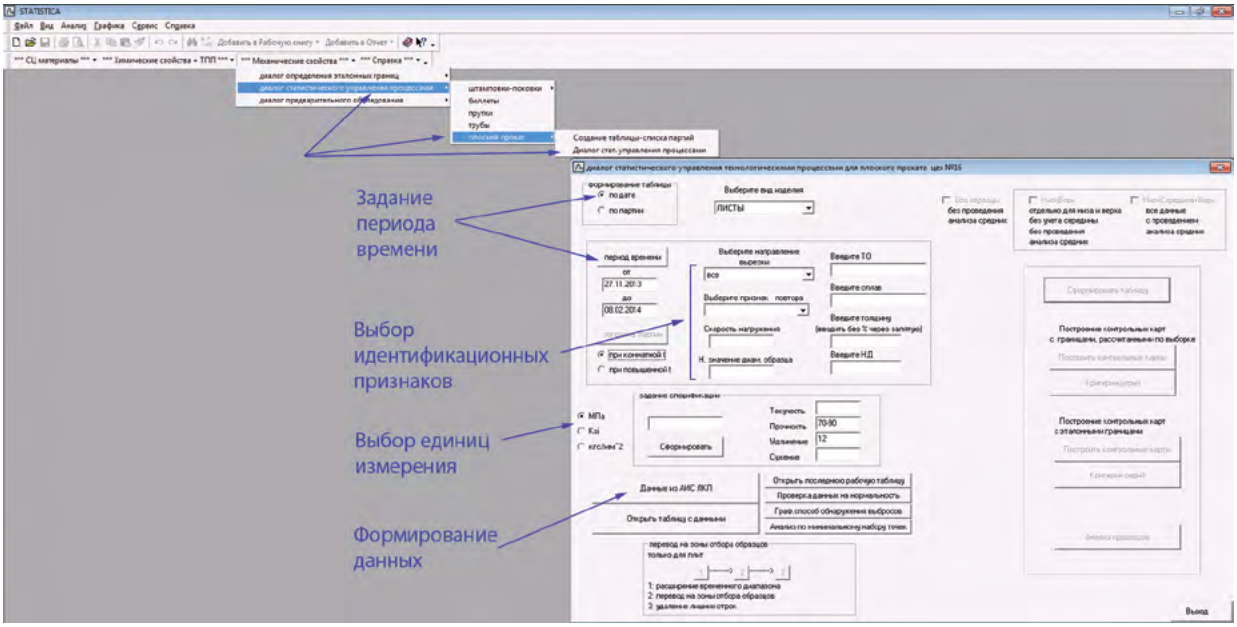


Рисунок 3. Пример диалогового окна для контроля качества механических свойств продукции плоского проката

ности и качестве технологических процессов на предприятии;
- прогнозировать выход процессов из стабильного управляемого состояния;
- выполнять оценки потенциального брака;
- осуществлять оперативный статистический контроль;
- проводить оценку качества серийных авиационных материалов/полуфабрикатов при сертификации их производства.

Интегрированные пакеты *STATISTICA* установлены в научно–техническом центре (НТЦ) в службах прокатного, плавильного, сортопрокатного, прессового, трубопрофильного, литейного производства. Проведено обучение специалистов НТЦ — владельцев технологических процессов — работе с автоматизированной системой статистического контроля.

Для решения новых, или нестандартных задач специалистами бюро активно используется стандартные модули пакета. Так с помощью *STATISTICA* нами освоены и применяются методика MSA, выборочный контроль, однофакторные и многофакторные методы оценки влияния факторов на процесс (рис. 1).

М.Л.: Компьютерные технологии постоянно прогрессируют, открывая новые возможности для специалистов. Расскажите о ваших планах развития. Какие задумки, на ваш взгляд, наиболее реально воплотить в жизнь в ближайшее время? Какие инструменты вы рассматриваете для их реализации?

О.А.: Разработанная нами автоматизированная система на базе пакета *STATISTICA* позволяет осуществлять статистический контроль

ОАО «Корпорация ВСМПО-АВИСМА» — российская металлургическая компания, мировой лидер по производству титана. На данный момент корпорация поставляет на экспорт 70% своей титановой продукции.

ключевых характеристик продукции и делает реальным системный анализ качества в масштабе производства.

Но время не стоит на месте. Подтверждение этому и ваши новые разработки, и новые потребности нас, как пользователей. Нас заинтересовала программа *STATISTICA* Enterprise/QC, надстройка MAS — проактивное предупреждение, которая дает возможность осуществления мониторинга процессов в режиме реального времени. Мы понимаем, что это серьезный проект, требующий в первую очередь больших временных ресурсов, из-за особенностей наших технологических процессов. Эта работа у нас в перспективных планах.

А в ближайших — задача внедрения модуля «Планирования эксперимента» в научно-техническом центре ВСМПО.

Для нас, практиков, изучение статистических методов с использованием статистического программного обеспечения является приоритетным. Надежный математический аппарат, отработанные алгоритмы методов значительно упрощают задачу грамотного внедрения статистических методов управления процессами на предприятии.

Intel Parallel Studio XE 2015

Ускорение написания кода с набором инструментов для комплексной разработки программ

Создавайте эффективный код

Достигните высокой производительности кода, функционирующего на процессорах и сопроцессорах настоящего и будущего поколения.

Что нового

- Значительное увеличение производительности посредством улучшения функции векторизации
- Широкая поддержка стандартов: OpenMP 4.0, C ++ 11, Fortran 2003, и 2008, MPI 3.0
- Ускорение процесса разработки приложений с использованием новых функций анализатора

Достигните максимальной производительности и надежности приложений с Intel® Parallel Studio XE. Этот набор инструментов C ++ и Fortran упрощает разработку, отладку и настройку кода, а также позволяет использовать функцию параллельной обработки для повышения производительности. Повысьте производительность на совместимых процессорах и сопроцессорах Intel® с меньшими усилиями.

Редакции

Intel® Parallel Studio XE поставляется в трех редакциях, в зависимости от ваших потребностей.

Разрабатывайте приложения быстро и эффективно, используя набор инструментов, предназначенный для упрощения создания эффективного и надежного параллельного кода.

Любые вопросы адресуйте руководителю группы продуктовой экспертизы Анне Курьяновой: Anna.Kurianova@softlinegroup.com

	Intel® Parallel Studio XE Composer Edition[1]	Intel® Parallel Studio XE1 Professional Edition[1]	Intel® Parallel Studio XE Cluster Edition
Intel® C++ Compiler	✔	✔	✔
Intel® Fortran Compiler	✔	✔	✔
Intel® Threading Building Blocks (только C++)	✔	✔	✔
Intel® Integrated Performance Primitives (только C++)	✔	✔	✔
Intel® Math Kernel Library	✔	✔	✔
Intel® Cilk™ Plus (только C++) Intel® OpenMP	✔	✔	✔
Rogue Wave IMSL Library2 (только Fortran)	В комплекте	Дополнение	Дополнение
Intel® Advisor XE		✔	✔
Intel® Inspector XE		✔	✔
Intel® VTune™ Amplifier XE3		✔	✔
Intel® MPI Library3		✔	✔
Intel® Trace Analyzer and Collector		✔	✔
Операционная система (Среда разработки)	Windows (Visual Studio) Linux (GNU) OS X4 (XCode)	Windows (Visual Studio) Linux (GNU)	Windows (Visual Studio) Linux (GNU)

1. Доступно на одном языке программирования (C++ или Fortran), либо на обоих языках сразу.
2. Доступно, как дополнение к любому приложению Windows Fortran, либо изначально включен в версию Composer Edition.
3. Поставляется как в комплекте, так и отдельно.
4. Доступно на одном языке для OS X.

Intel® VTune™ Amplifier XE 2015

Настройка производительности приложений в многоядерной архитектуре.

Новые возможности

- Анализ производительности и масштабируемости потоков в OpenMP 4.0.
- Анализ данных Windows или Linux на вашем Mac-устройстве.
- Настройка OpenCL и GPU для снижения нагрузки на Windows с точным определением параметров CPU и GPU.

Если вы производите настройку или оптимизацию производительности впервые, то Intel® VTune™ Amplifier XE поможет собрать все необходимые данные для настройки любой сложности. Вам будет доступен полный набор данных о производительности точек доступа, потоках, OpenCL, критических участках кода, DirectX, пропускной способности и о многом другом. Но просто полезных данных не достаточно. Нужны инструменты для анализа и толкования данных. Мощные инструменты анализа позволят сортировать, фильтровать и визуализировать результаты на временной шкале. Вы сможете определить дисбаланс времени и нагрузки, найти замедленные участки в Open MP и выяснить причины замедления.

Функции

1. **Быстрый поиск кода, нагружающего процессор.**
   Анализ горячих точек позволяет получить список функций, сильно нагружающих процессор. Именно в тут настройка будет наиболее эффективной. Нажмите [+] для вывода на экран списка вызовов. Дважды щелкните по элементу, чтобы увидеть источник нагрузки.
2. **Просмотр результатов в исходном коде.**
   Дважды кликните на списке функций, чтобы увидеть горячую точку функции, оказывающую наибольшую нагрузку
3. **Настройка потоков посредством анализа критических участков кода.**
   Осуществите быстрый поиск причин низкой производительности параллельных программ с долгими периодами задержки, не влияющих на загрузку ядер процессора во время ожидания. Поддержка новой версии OpenMP 4.0.
4. **Визуализация поведения потоков.**
   Определяйте активность и простой работы потоков, а также момент перехода из одного состояния в другое. Настройте баланс нагрузки. Осуществите поиск блокирующих участков кода.
5. **Быстрый поиск возможностей настройки с функцией подсветки.**
   Ячейка выделяется розовым цветом, если имеется потенциальная возможность настройки. Наведите на нее, чтобы увидеть предложения по настройке. Это особенно полезно для оптимизации кэширования, пропускной способности и т.д.

Узнайте больше и загрузите пробную 30-дневную версию:
http://intel.ly/vtune-amplifier-xe

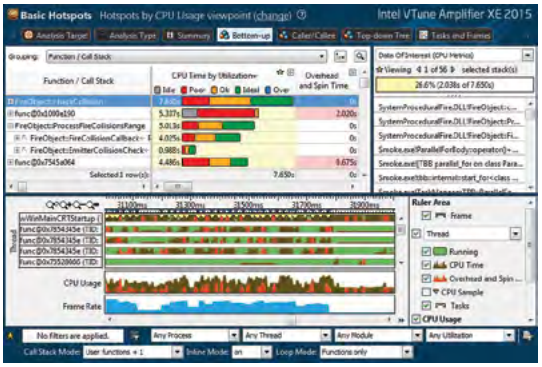
Общий ознакомительный центр:
https://software.intel.com/ru-ru/articles/try-buy-tools

Получите нужные данные

- Точки доступа (статистическое дерево вызовов), количество вызовов.
- Профилировка потоков с анализом критических участков кода.
- Анализ потерей кэша и пропускной способности.
- Отслеживание работы ядер OpenCL и сниждение нагрузки GPU на Windows.

Простота в использовании

- Не требует нестандартных компиляторов: C, C ++, C #, Fortran, Java, ASM.
- Возможность интеграции с Visual Studio или Eclipse, либо автономного использования на ОС Windows или Linux.
- Графический интерфейс и командная строка.
- Локальный и удаленный сбор данных.
- Новое: анализ данных Windows и Linux из OS X.



«Intel® VTune ™ Amplifier XE помогает нам быстро анализировать и выявлять проблемные участки сложного кода. Используя этот, а также и другие инструменты разработки программного обеспечения Intel®, мы смогли улучшить производительность PIPESIM в 10 раз по сравнению с предыдущей версией программного обеспечения».

Родни Лессард, старший научный сотрудник, компания Schlumberger

IBM Security QRadar SIEM

Улучшает защиту от угроз информационной безопасности и помогает соблюдать требования законодательства благодаря наличию интегрированной системы для создания отчетов, использующихся при расследовании инцидентов.

Современные сети стали больше размером и сложнее, чем когда-либо раньше, и их защита от вредоносных действий — это задача, которую нужно решать постоянно. Организации должны защищать свою интеллектуальную собственность, конфиденциальные данные своих клиентов и не допускать сбоев в работе бизнеса.

Оперативная информация о безопасности

Компаниям необходимо необходимо прилагать больше усилий по мониторингу журналов и данных о сетевых потоках, а также использовать современные инструменты для обнаружения подозрительных действий и выполнения операций по их устранению. Решение по управлению событиями и информацией, связанной с безопасностью, (SIEM) IBM® Security QRadar может использоваться как базовое решение в центрах обеспечения безопасности малых и крупных компаний для сбора, стандартизации и корреляции доступных сетевых данных с применением полученного за многие годы отраслевого опыта. В результате этих действий организации получают в свое распоряжение оперативную информацию о безопасности.

Центральным компонентом данного продукта является база данных с высокой степенью масштабируемости, предназначенная для сбора в реальном времени событий журналов и данных о сетевых потоках, что позволяет выявить следы деятельности потенциальных злоумышленников. QRadar SIEM – это корпоративное решение, которое консолидирует данные о событиях в источниках журналов, получаемые от тысяч устройств, распределенных по всей сети, сохраняет все действия в необработанном виде и затем незамедлительно

выполняет корреляцию, чтобы отличить реальные угрозы от ложных срабатываний.

Интуитивно понятный пользовательский интерфейс, используемый всеми компонентами семейства QRadar, помогает IT-специалистам быстро идентифицировать сетевые атаки и отреагировать на них в зависимости от степени их критичности. Благодаря этому сотни сигналов тревоги и шаблонных сигналов о выявлении аномальных действий можно существенно сократить до удобного для управления небольшого количества сообщений о предполагаемом нарушении безопасности, требующего дальнейшего расследования.

Данные об угрозах и их приоритете в реальном времени

Контекстуальный и практичный обзорный взгляд на всю IT-инфраструктуру, обеспечиваемый решением QRadar SIEM, помогает обнаружить и устранить угрозы, которые часто пропускают другие решения для обеспечения безопасности. Такие угрозы могут включать нецелевое использование приложений, действия, связанные с инсайдерским мошенничеством, современные медленно и незаметно реализуемые угрозы, которые легко упустить из виду на фоне «шума», создаваемого миллионами событий.

Эффективное управление борьбой с угрозами

Чтобы полностью понять характер потенциальных угроз ИБ, специалисты по обеспечению безопасности должны знать ответы на следующие ключевые вопросы: Кто атакует? Что атакуется? Каково влияние на бизнес? Где необходимо проводить расследование? Решение QRadar SIEM отслеживает значимые инциденты и угрозы и собирает статистику, необходимую для проведения расследований. При этом специалистам по обеспечению информации предоставляются такие подробные и полезные для расследования сведения, как цели атаки, точное время, ценность актива, состояние уязвимости, данные о пользователях, нарушающих безопасность, профили атакующей стороны, список активных угроз и статистические данные о нарушениях в прошлом.

Прозрачность приложений и обнаружение аномалий

Решение QRadar SIEM поддерживает широкий спектр функциональных возможностей для обнаружения аномалий и выявления изменений поведения, влияющих на приложения, хосты, серверы и участки сети. Например, решение QRadar SIEM может обнаруживать использование приложения или облачного сервиса в нерабочее время или необычно интенсивное использование таких активов, а также шаблоны сетевых действий, которые не соответствуют статистическим, рассчитанным по скользящим средним показателям профилям или сезонным особенностям использования. Решение QRadar SIEM способно обучаться таким суточным и недельным профилям использования, что помогает IT-персоналу быстро идентифицировать значимые отклонения.

QRadar SIEM собирает информацию, включающую:

- события безопасности: события, получаемые от брандмауэров (межсетевых экранов), виртуальных частных сетей (VPN), систем обнаружения взлома, систем противодействия взлому и т.д.;
- сетевые события: события, получаемые от коммутаторов, маршрутизаторов, серверов, хостов и т.д.;
- контекст сетевых действий: контекст приложений OSI-уровня 7 из трафика сетевых данных и данных приложений;
- контекст пользователя или актива: контекстуальные данные, получаемые от продуктов по управлению доступом и учетными записями пользователей и от сканеров уязвимостей;
- сведения об операционных системах: наименование изготовителя и номер версии сетевых активов;
- журналы приложений: системы планирования корпоративных ресурсов (ERP), рабочие потоки, прикладные базы данных, управленческие платформы и т. д.

Программно-определяемая СХД (SDS) невероятная экономия!

Вы получите решение, способное конкурировать в функциональном плане с СХД Hi-End уровня, в ценовых категориях от $100 000, за меньшие деньги. SSV предназначено для крупных заказчиков: показатель экономической эффективности становится очевиднее при больших объемах данных. Арифметика простая: чем больше — тем экономически эффективнее!

Для заказчиков, планирующих создание отказоустойчивой (катастрофоустойчивой) СХД, SSV станет волшебным средством, позволяющим решить задачу максимально быстро и с минимальными рисками. По сути, необходимо будет ответить всего на два вопроса: какой объем дискового пространства необходим и какой производительности. При этом показатель производительности можно смело увеличить в 2–3 раза, что позволит не промахнуться в выборе нужной дисковой подсистемы.

Облака, облачные вычисления, виртуализация — термины, описывающие подход к созданию гибкой и масштабируемой по запросу инфраструктуры. Технологии виртуализации серверов, десктопов и приложений в той либо иной мере применяет компания любого размера вне зависимости от своей миссии и бизнес-стратегии.

Концепция централизованного управления и доставки рабочего окружения конечному пользователю неоднократно доказывала свою экономическую эффективность и практическую целесообразность. Стоит отметить, что помимо экономической выгоды от снижения операционных затрат, внедрение облака также сопровождается и весомыми капитальными вложениями, в частности — в систему хранения данных.

Создание системы хранения данных — процесс не только затратный, но и технологически сложный. Ведь объемы данных, генерируемые в результаты рабочей деятельности организации, увеличиваются не пропорционально ее росту, а существенно его опережая, тем более в крупных компаниях. IT-департаменту необходимо заранее предусматривать варианты масштабирования данной системы, ее модернизации и т.д. Могут возникнуть ошибки: ведь то, что мы заложили в текущем году, уже через несколько лет не только морально, но и технологически устареет.

Возможно ли создать СХД, не ограничивая свой выбор в рамках решений отдельного вендора, сократить затраты на обслуживание СХД, увеличить доходность инвестированного в проект капитала (ROI), добавить новый функционал? Существует ли альтернатива классическому подходу в создании системы хранения данных и как будет выглядеть СХД в будущем?

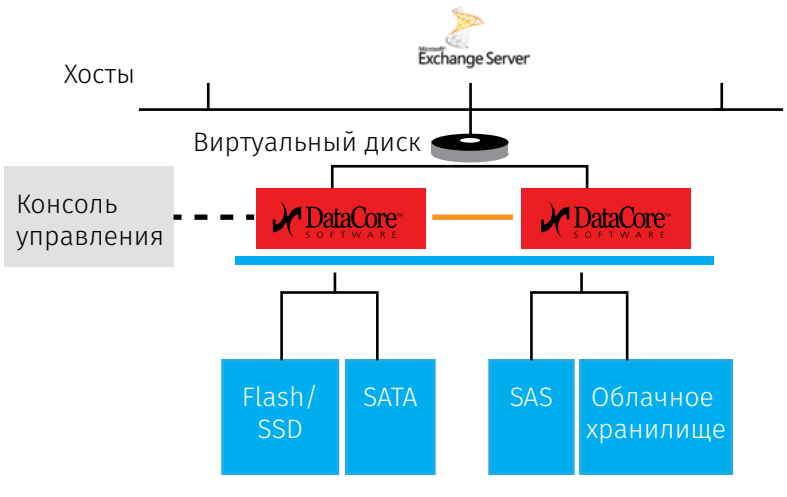


Рис. 1

Виртуализация ресурсов хранения

Известным подходом в создании СХД, активно использующимся в мире, является практика виртуализации ресурсов хранения. В ее основе лежит создание унифицированного контроллера СХД, способного объединять в единые логические пространства дисковые массивы любого вендора, поддерживающего любые протоколы передачи данных. Эти «виртуальные» СХД называют программно-определяемыми, представителями класса Software-Defined-Storage (SDS).

Мировым лидером в этом классе является компания Datacore (далее – DC) с решением SANsymphony-V.

В сущности, SANsymphony-V (SSV) – это программное-обеспечение, которое устанавливается на ОС Windows Server 2012R2 (2008R) и выполняет функции контроллера СХД. В качестве аппаратной платформы используется сервер x86-архитектуры. Таким образом, только вам решать, какими техническими характеристиками (здесь имеется ввиду CPU, объем RAM, количество и типы сетевых интерфейсов) он будет обладать. Сервера Datacore (далее ноды) устанавливаются между хостами приложений (UNIX, HP-UX, Sun Solaris, IBM AIX, RedHat Linux, Suse Linux, VMware ESX/vSphere, Citrix XenServer, Windows Server 2012, 2012 R2, 2008, 2008 R2 2003, 2000, Hyper-V, Windows 8, 7, XP) и любой дисковой подсистемой. Общая схема представлена на рис. 1.

Использование данного подхода позволяет не ограничиваться в выборе единого поставщика СХД, а комбинировать – приобретать то, что нужно, а не то, что можно.

Таким образом, в случае нехватки бюджета на конкретную модель СХД можно создать ее самому с использованием Datacore.

Функционал

Внедрение SSV может быть обусловлено рядом инициатив, начиная с точечного внедрения, к примеру, с целью повышения производительности существующей СХД под хранение баз данных и использования 30 дневных лицензий для переноса данных между площадками, до масштабного внедрения SDS на весь пул дисковых подсистем.

С функциональной точки зрения мы имеем следующее:

- высокопроизводительный кэш. DataCore использует весь свободный объем ОЗУ (до 1 ТБ на нод) серверов под высокопроизводительный мега-кэш и позволяет получить прирост производительности существующих дисковых подсистем от 3 до 10 раз;
- синхронная репликация данных для обеспечения отказоустойчивости (Fault Tolerance);
- механизмы оптимизации использования дискового пространства (Disk Pooling, ThinProvisioning и т.д.);
- создание динамической иерархической системы хранения данных (AST – Automatic Storage Tiering). DataCore позволяет создать до 15 уровней с динамическим назначением профилей как для ресурсов хранения, так и для данных, с автоматическим перераспределением блоков между уровнями;
- RAID Striping – возможность строить программные RAID0 и RAID1, даже если подключенный DAS этого не может;
- Load Balancing – автоматическая балансировка размещения данных на дисковых ресурсах;
- Performance Analysis – визуальные и статистические инструменты предоставления данных о всевозможных параметрах производительности с указанием «узких» мест;
- Synchronous Mirroring & Auto Failover – синхронная репликация и механизмы автоматического восстановления после сбоев. Функция самолечения дисковых пулов: если физический диск в пуле выходит из строя (или администратор отмечает диск как диск для замены), DataCore автоматически восстанавливает пул на доступных ресурсах;
- Virtual Disk Migration – простая и эффективная миграция данных с физических ресурсов в виртуальные и обратно без остановки приложений;
- Continuous Data Protection (CDP) & Recovery – «живой» журнал изменений на указанном диске с возможностью восстановления из любого состояния или временной точки;
- Online Snapshots;
- Remote Replication;
- Advanced Site Recovery (ASR);
- Random Write Accelerator.

Функционал дедупликации, как можно заметить, не упоминается, но на самом деле повторяющиеся блоки данных, попадающих в кэш, единожды записываются, поэтому алгоритмы дедупликации все-таки присутствуют. Datacore в качестве приоритета ставит производительность и рациональное использование ресурсов. Остановимся на этом поподробнее.

Увеличение производительности

Каждая нода Datacore может использовать до 1 ТБ ОЗУ в качестве кэш-памяти, что значительно быстрее при использовании SSD-дисков под кэш. Блоки данных кэшируются как на запись, так и на чтение. При этом используется механизм упреждающего чтения, т.е. блоки наиболее горячих данных автоматически подгружаются в кэш в зависимости от временных интервалов их использования.

Как правило, рост производительности составляет 300%–400%. При проведении тестирования на SATA-дисках картина выглядела следующим образом: (см. рис. 2)

На аппаратном уровне использовались сервера Dell R510 2.66 GHz

Тип нагрузки	Физические диски	Виртуальные (DataCore)	Производительность
SQL Server	119 IOPS	531 IOPS	346% ⇧
Exchange	124 IOPS	576 IOPS	365% ⇧
File Server	115 IOPS	734 IOPS	538% ⇧
Streaming Media	193 МБ/с	280 МБ/с	45% ⇧

Тип нагрузки: 8 Кб IO 100% random, 67% read

Рис. 2

Quad Core Xeon CPU 16GB RAM, 2x 1TB SATA HDD (в каждом сервере).

Рациональное использование ресурсов хранения

Концепция SDS подразумевает создание иерархичной системы хранения данных с автоматическим перемещением блоков между необходимыми по производительности в данный момент времени дисками. Экономическую целесообразность данного подхода можно объяснить на примере приобретения флэш-массива под хранение базы данных. Учитывая тот факт, что вся БД не может быть «горячей» (по статистике, лишь на 30% своего объема) в единый момент времени, то логично предположить, что большая ее часть занимает флэш-массив нерационально. Правильнее было бы «отпилить» от всего флэш-массива эти 30% и объединить их с дисками меньшей производительности, тем самым высвобождая оставшиеся 70% под другие задачи. Похожая ситуация может возникнуть при масштабировании СХД за счет дозакупки новой полки с SSD-дисками, когда в наличии уже есть не до конца используемая СХД с дисками SAS. Рационально было бы объединить их в единую логику, создать двухуровневую СХД, тем самым задействовав уже имеющиеся ресурсы.

В отличие от классической СХД, имеющей, как правило, 3 уровня (SSD, SAS, SATA), SSV предоставляет возможность создавать до 15 уровней (рис. 3), основанных на стоимости, производительности и емкости дисков. Перемещение блоков между уровнями происходит в режиме real-time, задержек в принятии решения о перемещении блоков между уровнями в виде сбора суточной информации и ее анализа не происходит. При этом добавление или удаление физического диска из пула не приводит к каким-либо простоям. В принципе, внедрение SSV сопровождается созданием отказоустойчивого решения (минимум 2 нод). Соображения простые: данные должны быть доступны всегда, без ограничения производительности (при наличии только одного нода кэш не работает на запись ввиду риска потери данных в случае сбоя в электропитании). Таким образом, классическая схема отказоустойчивого решения с реализацией асинхронной репликации на удаленный сайт выглядит следующий образом – см. рис.4.

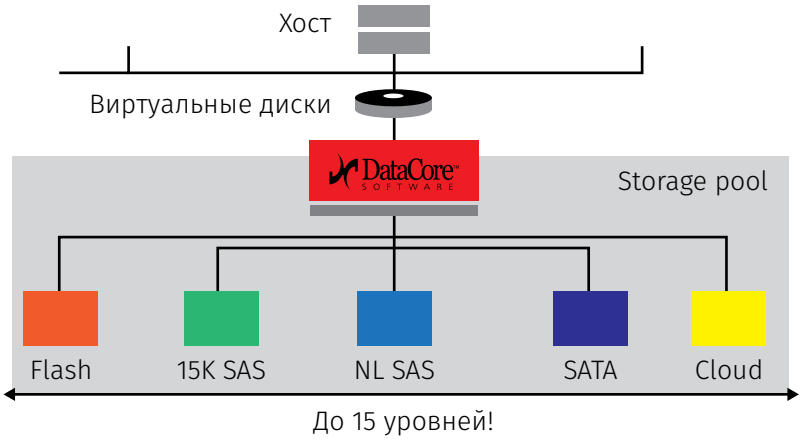


Рис. 3

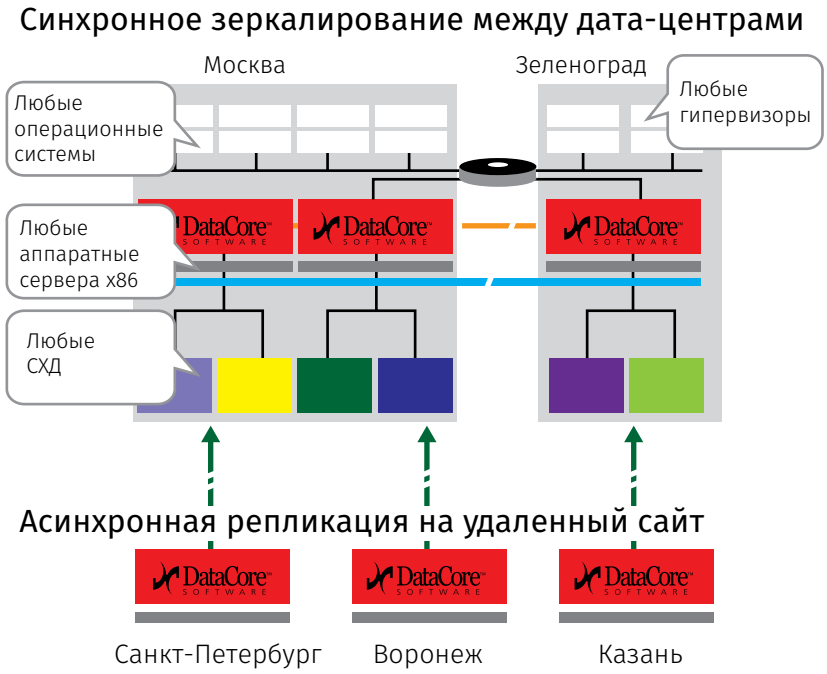


Рис. 4

Подводя итог, можно сказать, что SSV позволит, как минимум, рассмотреть альтернативное решение задач, которые стоят перед IT-департаментом. Оценить экономическую эффективность SDS можно в каждом конкретно взятом случае.

Практика показывает, что заказчики, внедрившие Datacore, не остались равнодушными к данному решению: начав с малого, сегодня они доверяют этому продукту управление все большими массивами данных в инфраструктуре своей компании.

За более подробной информацией по решению Datacore вы можете обращаться к Ивану Орлову, ведущему менеджеру по развитию бизнеса Департамента инфраструктурных решений Управления сервисов Softline:

+7-965-176-10-16

i.orl@softlinegroup.com

SCAD SOFT
www.scadsoft.com

ИНТЕГРИРОВАННАЯ СИСТЕМА
АНАЛИЗА КОНСТРУКЦИЙ
«SCAD Office»

СОСТАВ СИСТЕМЫ

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

КРИСТАЛЛ — расчет и проверка элементов стальных конструкций по СНиП II-23-81*, СП 53-102-2004, СП 16.13330.2011, ДБН В.2.6-163:2010, Evrocode-3

АРБАТ — подбор арматуры и экспертиза элементов железобетонных конструкций по СНиП 52-01-2003, СП 52-101-2003, СНиП 2.01.07-85, СП 63.13330.2012

КАМИН — экспертиза элементов каменных и армокаменных конструкций по СНиП II-22-81, СНиП 2.01.07-85, СП 15.13330.2012

МОНОЛИТ — проектирование монолитных ребристых железобетонных перекрытий.

КОМЕТА — расчет и конструирование узлов стальных конструкций.

КРОСС — расчет коэффициентов постели фундаментных плит на упругом основании.

ВЕСТ — Расчет нагрузок и воздействий по СНиП 2.01.07-85*(изменения №2), СП 20.13330-2011, СНиП 2.01.07-85 (нормы Украины), ДБН В.1.2-2:2006 (изменения №1, нормы Украины), СНиП 2.01.07-85 (нормы Р.Б.)

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

КОНСУЛ — формирование сечений, исходя из теории сплошных стержней.

ТОНУС — формирование сечений, исходя из теории тонкостенных стержней.

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

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

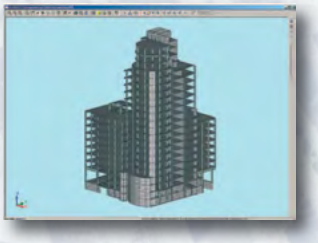
ДЕКОР — расчет и проверка элементов деревянных конструкций по СНиП II-25-80, СП 64.13330.2011

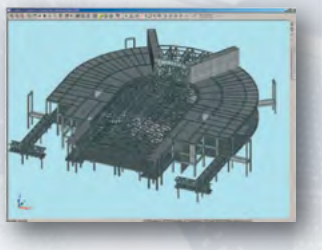
ОТКОС — определение коэффициента запаса устойчивости откосов и склонов.

КОКОН — электронный справочник для определения коэффициентов концентрации напряжений.

КУСТ — электронный расчетно-теоретический справочник инженера-проектировщика.

Сертификат соответствия РОСС RU.СП15.Н00668





ООО "АВТОМАТИЗАЦИЯ ПРОЕКТНЫХ РАБОТ"

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

Maple в массы

Компания Maplesoft – известный канадский производитель математического программного обеспечения по традиции представила в марте этого года новую версию своего флагманского продукта – систему компьютерной алгебры Maple 2015.

В связи с этим инженерами компании Softline, которая является эксклюзивным представителем Maplesoft на территории России и СНГ, был подготовлен краткий обзор не только основных нововведений свежего релиза, но и полного спектра продуктов компании, возможностей их использования в образовании и промышленности, а также основных направлений развития.

Что нового в Maple 2015?

Maple – это математическое программное обеспечение, которое сочетает в себе один из наиболее мощных математических «движков» и удобный интерфейс, что позволяет легко проводить различные исследования, визуализировать и обрабатывать результаты. Используйте пакет Maple, и вам не придется выбирать между мощными алгоритмами и простотой использования! Именно это и делает систему Maple идеальным средством для образования и исследований.

Работа с данными

Maple 2015 представляет новый интерфейс для работы как с встроенными, так и внешними данными. Интерфейс предлагает простой доступ к курируемым данным от компании Quandl, одного из мировых лидеров по сбору и хранению информации. С помощью Quandle пользователи Maple имеют доступ более чем к 12 млн массивов данных, которые они могут использовать в своих разработках бесплатно. Пользователям доступны данные из большого количества областей, включая макроэкономику, курсы валют, показатели рынка труда и многое другое. Поиск данных осуществляется через стандартные инструменты поиска, что позволяет использовать данные, не задумываясь об их хранении и доступности. А благодаря новым инструментам визуализации все данные можно представлять в наглядном виде.

Визуализация данных

В Maple 2015 представлена новая команда dataplot, которая используется для визуализации числовых двумерных и трехмерных данных, а также создания анимации. Команда поддерживает большое число различных настроек и по умолчанию работает со всеми основными типами данных.

Вас заинтересовал данный продукт и вы хотите пройти обучающие курсы? Свяжитесь с Алексеем Балашовым, руководителем отдела математического ПО компании Softline.

+7 (495) 232 00 23, доб. 0279

AlexeyBa@softline.ru

Maple Cloud

Благодаря развитию технологий, система Maple Cloud теперь доступна из любого веб-браузера, что дает возможность пользователям размещать и распространять в сети, созданные ими приложения. Используя мобильные устройства можно осуществлять поиск, изучать и взаимодействовать с документами системы Maple, не устанавливая ее. Созданные пользователями приложения могут использоваться всеми, кому предоставлен доступ, причем без ущерба для интерактивности. Пользователи могут выкладывать документы в облако нажатием всего лишь одной кнопки в системе Maple. На сегодняшний день там находятся сотни интерактивных приложений MathApps, посвященных различным областям знаний.

Приложения MathApps

MathApps представляют собой интерактивные обучающие приложения. В Maple 2015 доступно более 400 MathApps, 60 из которых были представлены в последнем релизе. Приложения покрывают такие области знаний как физика, статистика, химия и финансы. MathApps доступны как из системы Maple, так и с помощью бесплатного Maple плеера или Maple Cloud.

Новая визуализация

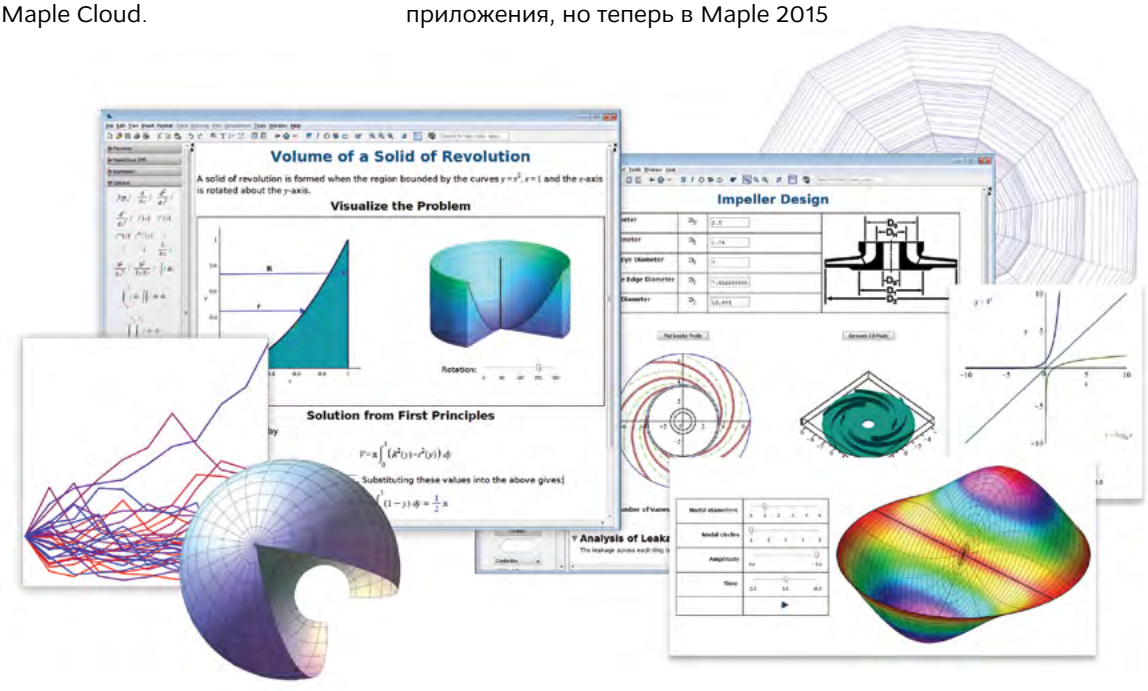
В Maple 2015 добавлено много новых настроек визуализации. Новый функционал включает в себя итерационные карты, группы, библиотеку многогранников и многое другое. Появились возможности закрашивания областей между несколькими графиками, использовать автоматические диапазоны построения. Также были обновлены цветовые схемы, представлен новый функционал для построения деревьев и многое другое.

Создание приложения в один клик

Команда Explore является простым инструментом для создания интерактивных приложений, так как позволяет работать через контекстное меню. В Maple 2015 были расширены возможности настройки команды Explore: добавлена простая инициализация кода приложений, усовершенствованы настройки внешнего вида двумерных графиков включая поддержку математической нотации и т.д.

Автоматическое создание документов

На протяжении многих лет пользователи могли легко создавать технические документы и интерактивные приложения, но теперь в Maple 2015



А ТАКЖЕ...

В новой версии системы был расширен функционал в области финансов, в частности добавлены 10 греков, используемых в области управления рисками. Отдельно стоит упомянуть о новом инструменте визуализации и интерактивных картах, которые служат для отображения бифуркационных диаграмм, фракталов и аттракторов. Процесс генерации интерактивных карт автоматически распараллеливается.

они могут делать это автоматически. Появилась возможность генерировать документы, внешний вид и содержание которых зависят от предыдущих вычислений. Новый функционал включает возможность автоматической генерации документов, содержащих текст, математические выражения, таблицы, графики, разделение на секции и прочее. Также можно автоматически создавать интерактивные приложения и модифицировать их, внося изменения в код, а не работая индивидуально с различными компонентами.

Интерактивные компоненты

Пользователям Maple доступны разнообразные интерактивные компоненты, такие как: кнопки, слайдеры, эмуляторы рычагов, которые они могут использовать при создании интерактивных приложений. В Maple 2015 представлены новые элементы, в частности для записи и воспроизведения звука, а также дополнительные настройки внешнего вида.

Новое в математике и физике

В Maple 2015 добавлена символьная поддержка новых классов интегралов, включая интегрирование гиперболических функций. Новый функционал был добавлен также в раздел теории групп и пределов, появилась возможность численного решения дифференциальных уравнений с запаздыванием, добавлен новый пакет для работы с ординалами.

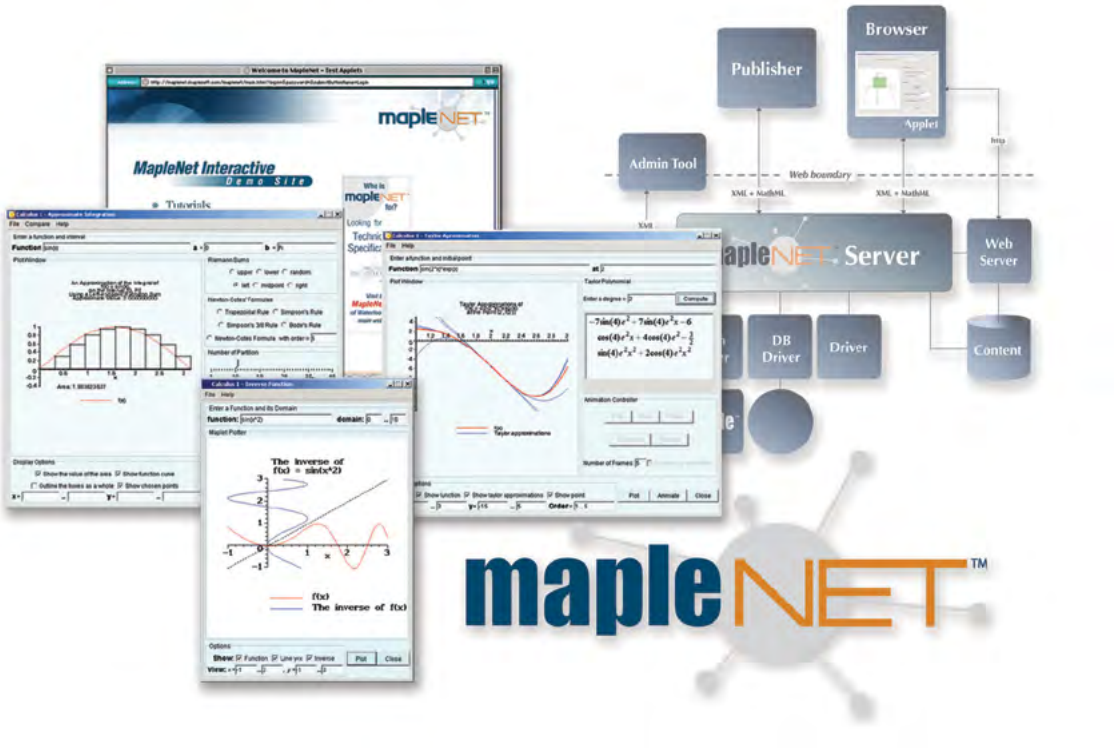
Помимо этого, Maple на протяжении многих лет является стандартом научных вычислений в области физики. В Maple 2015 реализовано более 400 улучшений в соответствующем разделе, касающихся, в частности общей теории относительности, операторов коммутации/антикоммутации и т.д.

Библиотека многогранников

В Maple 2015 появилась новая библиотека для работы с многогранниками, заданными, как через алгебраические выражения, так и через матрицы вершин и ребер. Библиотека включает функционал для исследования геометрических и топологических свойств многогранников, линейных преобразований над ними.

Статистика

В новой версии системы реализованы новые инструменты для проведения статистического анализа и визуализации. Был значительно



усовершенствован алгоритм lowess, добавлена поддержка визуализации временных данных с помощью пузырьковых диаграмм, появилось контекстное меню для работы с матричными данными и палитра для работы со случайными числами, с использованием различных распределений.

Работа с единицами измерения

В Maple 2015 стало невероятно просто работать с единицами измерения, их можно вводить с помощью комбинации клавиш. Представлен новый интерактивный помощник, позволяющий конвертировать единицы измерения и системы координат.

Генерация кода и работа с внешними файлами

В новой версии появилась возможность генерировать код на языках R и JavaScript. Обновленные команды импорта и экспорта предоставляют пользователю единый инструмент для работы с различными внешними файлами. Есть возможность импорта файлов в формате JSON. Также обновился интерфейс для параллельных вычислений, теперь вместо команд, похожих на MPI-сообщения, появились более понятные команды для работы с параллельными процессами.

Спектр решений компании Maplesoft

Система Maple позволяет пользователям решать любые математические задачи. Система содержит более 5000 функций, покрывающие почти все разделы математики, включая математический анализ, линейную алгебру, дифференциальные уравнения, статистику, геометрию и многое другое. В ней есть символьные, численные и гибридные алгоритмы, ее алгоритмическое ядро содержит методы недоступные другим платформам. Помимо этого, система обладает функционалом для создания 2D- и 3D- визуализации и анимации, и также предлагает пользователям эффективные алгоритмы для высокопроизводительных вычислений. Вне зависимости

На сегодняшний день система Maple используется более чем в 8000 университетов, исследовательских лабораториях и компаниях более чем в 90 странах по всему миру. Выбирая Maple, пользователь автоматически получает в свое распоряжение тысячи готовых примеров и интерактивных приложений от пользователей по всему миру, не говоря о поддержке, предоставляемой компанией - вебинары, обучающие видео, форумы, техническая поддержка.

от того, делаете ли вы простой расчет или разрабатываете сложный алгоритм, иллюстрируете концепцию или создаете интерактивный технический документ, система Maple поможет легко справиться с работой. Она предлагает пользователю функционал Clickable Math, который решает математические задачи, исключительно с помощью мышки. Maple основана на собственном языке программирования, ориентированном на математику и предлагает специальные образовательные инструменты для преподавания основных математических курсов.

Области использования

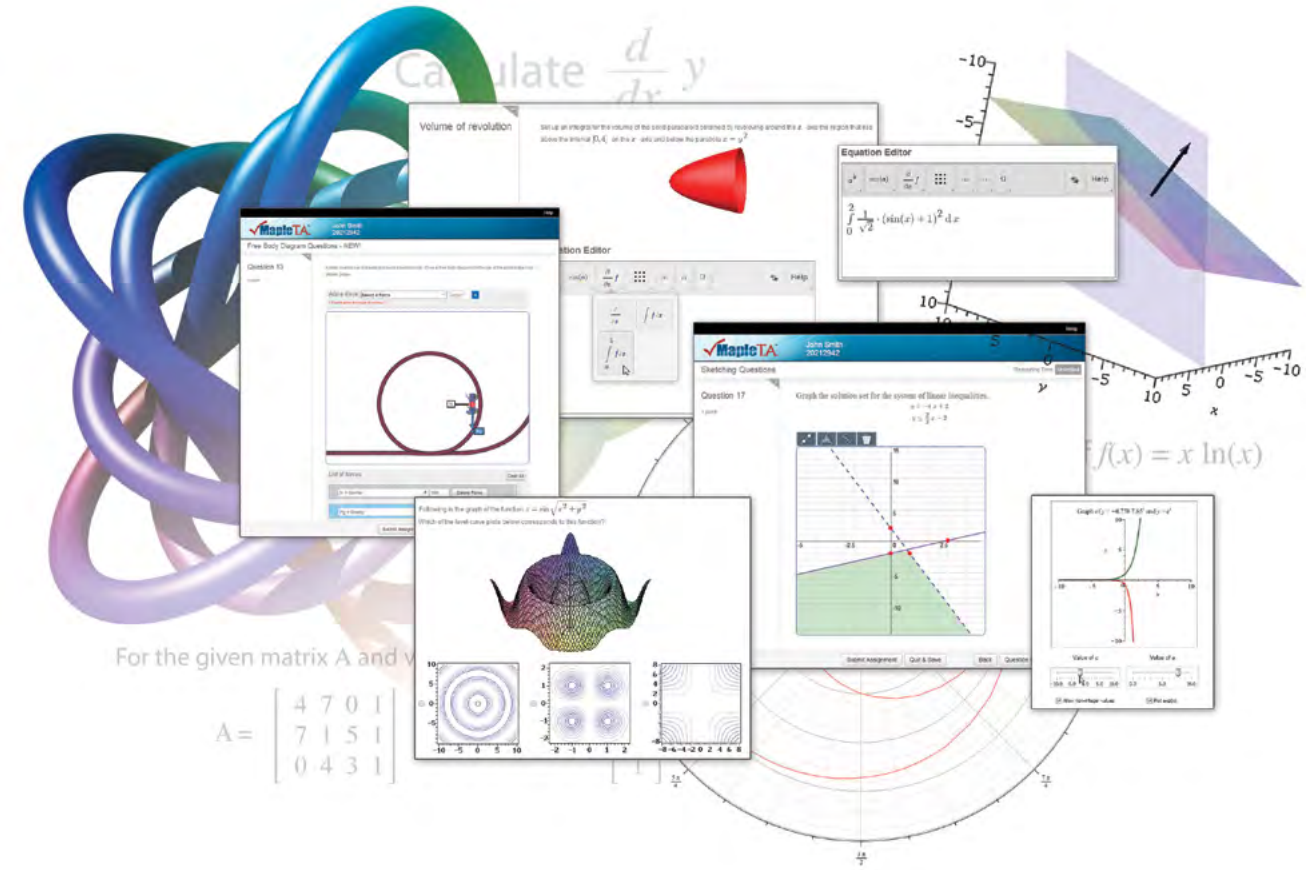
Математический анализ, визуализация, дифференциальные уравнения, системы уравнений, финансовое моделирование, генерация кода, параллельные вычисления, статистика, физика, инструменты аппроксимации, разработка приложений, работа с векторами и матрицами, оптимизация, обработка сигнала, единицы измерения, взаимодействие с САПР, работа с данными и многое другое.

Надстройки к системе Maple

Помимо флагманского продукта, системы компьютерной алгебры Maple, компания предлагает пользователю ряд дополнительных пакетов. В первую очередь это пакет Maple Global Optimization, который содержит мощные современные методы глобальной оптимизации для решения различного вида задач, как символьно, так и численно.

Следующий продукт – Maple Grid Computing, который позволяет разворачивать параллельные программы на крупномасштабных вычислительных кластерах и суперкомпьютерах.

Последний – Maple IDE, представляющий собой полнофункциональную среду разработки программ на внутреннем языке системы Maple.



SIROCCO
интернет-холдинг

ОТРАСЛЕВЫЕ И НИШЕВЫЕ
ИНТЕРНЕТ-ПРОЕКТЫ

НАШИ ПРОЕКТЫ

РУССТРОЙ НОВОСТРОЙКИ РОССИИ
www.russtroy.ru

fincredit
кредитный интернет-портал

russelhoz.ru
РУССЕЛЬХОЗ
интернет-портал

ВОЕННЫЕ НОВОСТИ
ARMYNEWS.RU

ruretail.ru
RU RETAIL
интернет-портал
о розничной торговле

FIGHTERS.RU
ЭНЦИКЛОПЕДИЯ БОЕВЫХ ИСКУССТВ

IT TUBE
информационные
технологии

POWER
MEDIA

Russian
Energetics
энергетический
интернет-портал

GAZNEWS
нефтегазовый портал

AVIATIONS.RU
авиационный портал

интернет-портал
БУХУЧЕТ.РУ
bukhuchet.ru

интернет-портал о софте
SOFTWEEK

ruswedding.com
RUSWEDDING
национальный свадебный портал

URBANLAND.RU
все о земельном рынке

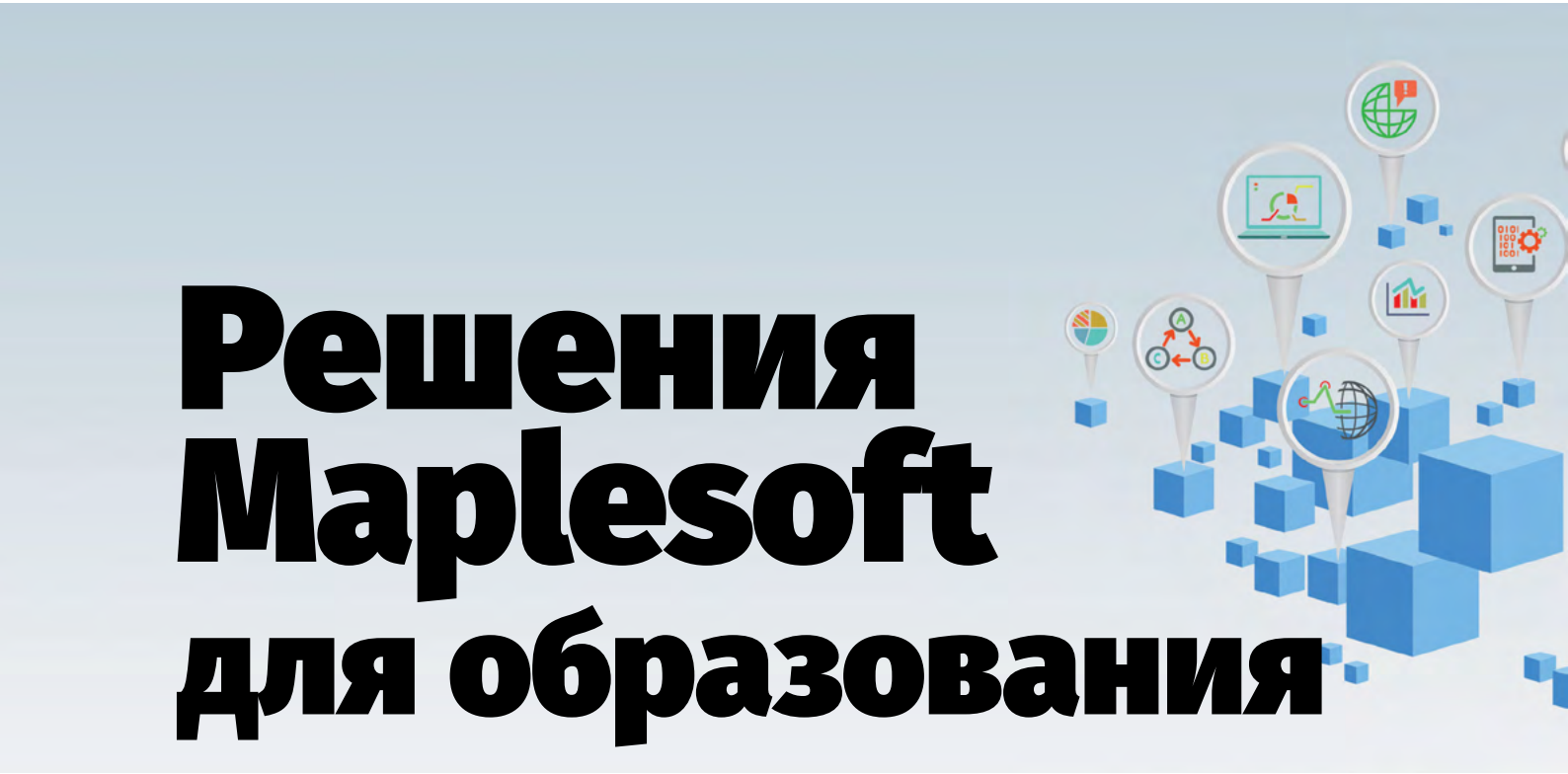
www.starparty.ru
STAR
PARTY
ИНТЕРНЕТ-ПОРТАЛ О ЗВЕЗДАХ

www.rusdorstroy.ru
РУСДОРСТРОЙ
интернет-портал о дорожном строительстве

RUSLOGISTIC.RU
логистический интернет-портал

LUXURY
FOOD

www.sirocco.ru info@sirocco.ru
+7 (495) 565-33-65, 8 (800) 77-55-284
Москва, ул. Ботаническая, 29, корп.2



Решения Maplesoft для образования

Maple T.A. – система онлайн-тестирования

Maple T.A. – это мощная система онлайн-тестирования и оценки знаний, созданная специально для STEM-курсов (Science, Technology, Engineering, Math), то есть курсов, так или иначе содержащих математику. Система дает преподавателям уникальные возможности для разработки заданий с гибкой системой автоматической проверки результатов, которая позволяет оценить истинный уровень знаний студентов. Система совместима практически с любой виртуальной системой управления курсами, поэтому может быть легко интегрирована в существующую инфраструктуру образовательного учреждения. Она также поддерживает мобильные платформы, позволяя студентам выполнять задания и просматривать результаты с планшетов.

Помимо этого, система предлагает опции по аренде серверов. Таким образом, вам не придется думать о том, где и как развернуть систему, а просто пользоваться ей через веб-браузер.

Поддержка математики

STEM-курсы обладают специфическими требованиями, которые необходимо учитывать при формировании автоматических систем оценок. Система Maple T.A. была создана именно с учетом этих требований. Она поддерживает стандартную математическую нотацию, инструменты для построения сложных 2D- и 3D-графиков, вопросы со свободной формой ответа, «умную» систему оценки, адаптивные и интерактивные вопросы и многое другое.

Совместимость с электронными системами управления курсами

Для расширения возможностей стандартных систем управления курсами или автоматизации систем собственной разработки Maple T.A. может быть легко интегрирована во все существующие онлайн- системы, включая Blackboard, Moodle и Brightspace. Это позволяет работать

с единой системой и легко получать доступ ко всем результатам студентов, вне зависимости от того в какой системе они были получены.

Поддержка мобильных платформ

В наши дни студенты привыкли, что все обучающие материалы доступны с мобильных устройств, в том числе задания и тесты. Вне зависимости от того разрабатываете ли вы систему дистанционного образования для мобильных устройств или просто разрешаете студентам выполнить задание за пределами университета, Maple T.A. предоставит все необходимые инструменты, совместимые с мобильными устройствами на базе iOS и Android.

Система MapleNet

Система MapleNet позволяет встраивать документы, интерактивные приложения и результаты расчетов, созданные в Maple, в веб-сайт. Ваши коллеги и студенты смогут взаимодействовать с Вашими разработками, выполнять расчеты и визуализировать результаты. Все это доступно через обычный браузер! Maple 2015 предлагает интуитивный интерфейс для создания веб-приложений с мощной алгоритмической поддержкой.

Пакет MapleSim

С MapleSim преподаватели получают в свое распоряжение профессиональный инструмент моделирования, соединяющий в себе теорию и практику. MapleSim широко используется в различных областях промышленности. Он основан на мощном символьном математическом «движке» Maple и позволяет увлечь студентов решением сложных практических задач, а также подготовить их к проблемам, с которыми они могут столкнуться в профессиональной деятельности.

Что делает MapleSim уникальным?

Моделирование мультифизических систем в одной среде.
Промышленности требуются системы, позволяющие проводить моделирование на системном уровне. Для этого требуется вводить в систему инженерного образования различные мультидисциплинарные концепции. Пакет MapleSim сочетает в себе компоненты из различных областей знаний, включая механику и электромагнетизм. Таким образом, студенты различных инженерных направлений могут создавать и исследовать реалистичные системы и изучать взаимодействие между компонентами с различной физической природой.

Связь концепций
С помощью MapleSim пользователи легко получают доступ к уравнениям, над которыми могут осуществлять различные виды анализа и преобразования, такие как оптимизация параметров, анализ чувствительности, линеаризация. С другой стороны, уравнения можно использовать для создания компонентов, что позволяет студентам получить представление о связи уравнений с поведением модели.

Работа с моделью, а не с уравнениями
Сложные системы, на описание которых с помощью уравнений могут уйти часы и дни, в пакете MapleSim создаются в куда более короткие сроки. Вместо построения потоковых диаграмм на основе абстрактных математических выражений, MapleSim создает модели, соединяя различные компоненты с явным физическим смыслом, такие, например, как двигатель и коробка передач. Это позволяет среди прочего использовать более сложные примеры при подготовке учебных программ.

Виртуальные эксперименты и физическая верификация
В отличие от натурных экспериментов, моделирование позволяет студентам безопасно исследоватьработу системы в различных условиях, без риска порчи оборудования и за меньшую стоимость. После того, как разработанная модель исследована и оптимизирована, она может быть экспортирована в Simulink или LabVIEW, а также в другие среды, которые могут работать с аппаратной инфраструктурой.

Расписание курсов в Учебном центре Softline

Москва

Код	Название курса	Даты
SERV_DESK	Организация работы службы Service Desk. Управление инцидентами и проблемами (основные элементы подхода)	28-30 мая
20488	Разработка основных решений Microsoft SharePoint Server 2013	25-29 мая
BizTalk Server 2010	BizTalk Server 2010	25-29 мая
20461	Создание запросов к Microsoft SQL Server 2014	25 мая — 5 июня
20462	Администрирование баз данных Microsoft SQL Server 2014	1-5 июня
55009	System Center 2012 Service Manager	1-5 июня
DP0147	Symantec Backup Exec 2012: Администрирование	1-5 июня
20489	Разработка продвинутых решений на базе Microsoft SharePoint Server 2013	1-5 июня
CXA-301I	Citrix XenApp 6.5 Advanced Administration (Углубленное администрирование Citrix XenApp 6.5)	1-5 июня
20412	Дополнительные службы Windows Server 2012 R2	1-5 июня
20687	Конфигурирование Windows 8.1	1-5 июня
20411	Администрирование Windows Server 2012 R2	1-12 июня
20342	Продвинутые решения на базе Microsoft Exchange Server 2013	1-12 июня
20332	Расширенные решения Microsoft SharePoint Server 2013	1-12 июня
VSICM55	VMware vSphere: Установка, настройка, управление (Vmware vSphere: Install, Configure, Manage v.5.5)	1-12 июня
VSDW55	VMware vSphere: Design Workshop [V5.5]	8-10 июня
VICM6	Horizon (совместно с View): Установка, настройка и управление [v6.0]	8-11 июня
10969	Службы Active Directory в Windows Server 2012	8-11 июня
20464	Разработка баз данных Microsoft SQL Server 2014	8-11 июня
20480	Программирование на HTML5 с использованием JavaScript и CSS3	8-11 июня
CNS-207-2I	Implementing Citrix NetScaler 10.5 for App and Desktop Solutions	8-11 июня
20413	Проектирование и реализация серверной инфраструктуры	8-12 июня

Москва

Код	Название курса	Даты
20688	Администрирование и поддержка Windows 8.1	8-11 июня
55004	Установка и конфигурирование System Center 2012 Operations Manager	8-11 июня
20462	Администрирование баз данных Microsoft SQL Server 2014	8-19 июня
CCSA-R77	Управление безопасностью средствами Check Point R77	15-17 июня
CCSE-R77	Проектирование безопасности средствами Check Point R77	18-20 июня
20409	Виртуализация серверов с использованием Hyper-V и System Center	15-19 июня
20463	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	15-19 июня
20486	Разработка ASP.NET MVC 4 веб-приложений	15-19 июня
VSICM55	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.5)	15-19 июня
DP0159	Symantec NetBackup 7.5 for Windows: Administration	15-19 июня
CNS-205I	Citrix NetScaler 10 Essentials and Networking (Основы и сетевая архитектура Citrix NetScaler 10)	15-19 июня
20414	Реализация продвинутой серверной инфраструктуры	15-19 июня
10747	Администрирование System Center 2012 Configuration Manager (SCCM)	15-19 июня
VSWN6	VMware vSphere: Нововведения [с версии 5.5 до 6.0]	15-18 июня
20412	Дополнительные службы Windows Server 2012 R2	15-26 июня
10747	Администрирование System Center 2012 Configuration Manager (SCCM)	15-26 июня
20466	Работа с моделями данных и отчетами в Microsoft SQL Server 2014	22-26 июня
20487	Разработка служб Windows Azure и веб-служб	22-26 июня
CNS-301-2I	Citrix NetScaler 10.5 Advanced Implementation	22-26 июня
20415	Внедрение инфраструктуры рабочих столов	22-26 июня
20417	Обновление навыков для MCSA Windows Server 2012	22-26 июня
10748	Внедрение System Center 2012 Configuration Manager	22-24 июня
50331	Техническая поддержка Windows 7 в корпоративной среде	22-26 июня
ICND1	Использование сетевого оборудования Cisco. Часть I (Interconnecting Cisco Networking Devices v.2.0 Part 1)	22 июня – 3 июля
20463	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	22 июня – 3 июля
VICM6	Horizon (совместно с View): Установка, настройка и управление [v6.0]	22 июня – 1 июля
20467	Проектирование бизнес – аналитики для самообслуживания и решений Big Data	29 июня – 4 июля
11gDBA1	Oracle Database 11g: Administration Workshop I	29 июня – 3 июля
CXD-203-6I	Managing App and Desktop Solutions with Citrix XenApp and XenDesktop 7.6	29 июня – 3 июля
CCNAX	Создание сетей на базе оборудования Cisco: Ускоренный курс (Interconnecting Cisco Networking Devices: Accelerated)	29 июня – 3 июля
20331	Базовые решения Microsoft SharePoint Server 2013	29 июня – 3 июля
20416	Создание инфраструктуры клиентских приложений	29 июня – 3 июля
20410	Установка и конфигурирование Windows Server 2012 R2	29 июня – 3 июля
10961	Автоматизация администрирования с использованием Windows PowerShell	29 июня – 3 июля
20341	Базовые решения с использованием Microsoft Exchange Server 2013	22 июня – 3 июля
VSOS5.5	VMware vSphere: Оптимизация и масштабирование (VMware – Optimize & Scale v.5.5)	22 июня – 3 июля

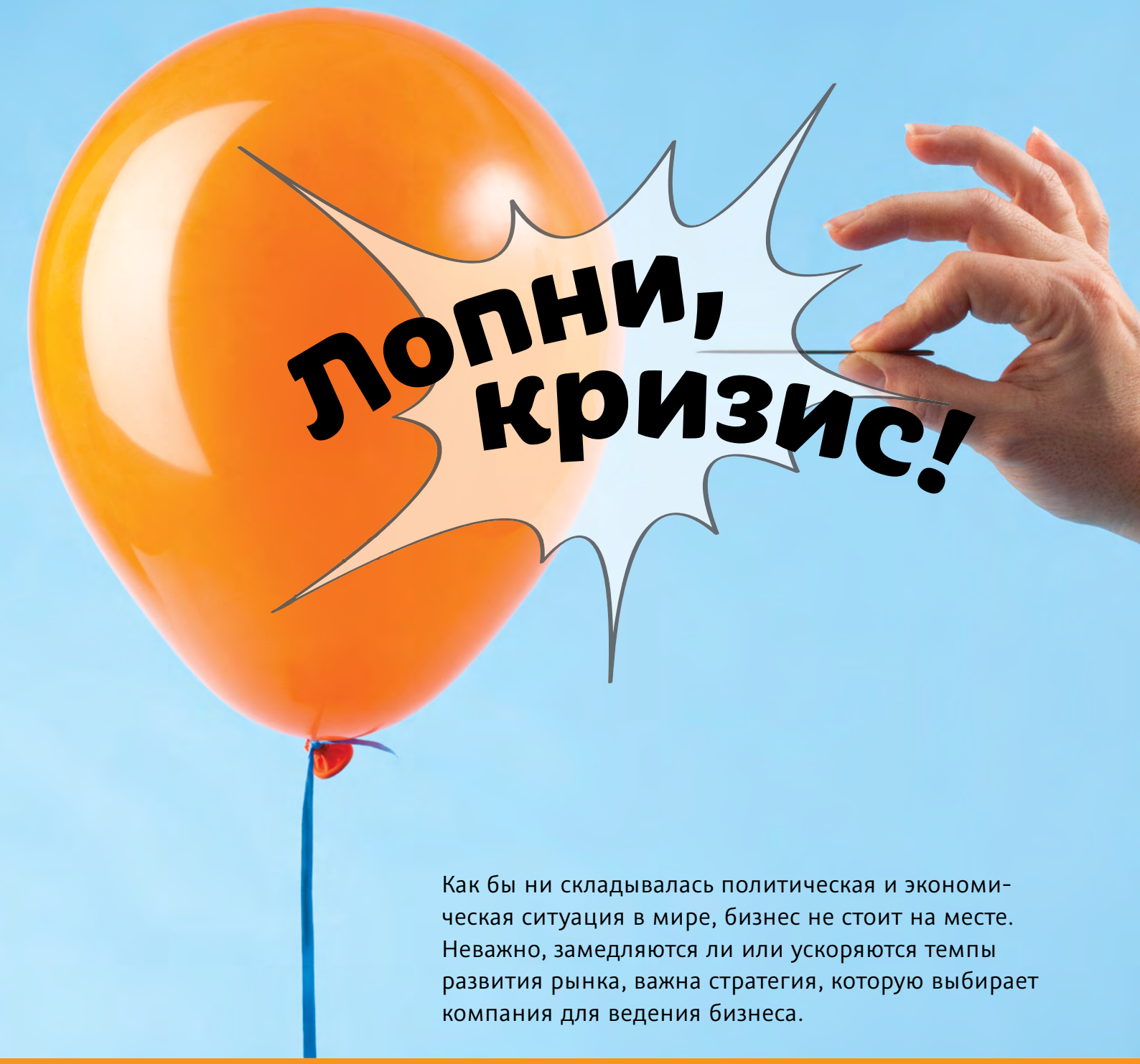
Дистанционные курсы

Код	Название курса	Даты
DP0147	Symantec Backup Exec 2012: Администрирование	1-5 июня
55009	System Center 2012 Service Manager	1-5 июня
20462	Администрирование баз данных Microsoft SQL Server 2014	1-5 июня
20341	Базовые решения с использованием Microsoft Exchange Server 2013	8-15 июня
20413	Проектирование и реализация серверной инфраструктуры	8-12 июня
20688	Администрирование и поддержка Windows 8.1	8-11 июня
CNS-207-2I	Implementing Citrix NetScaler 10.5 for App and Desktop Solutions	8-11 июня
20480	Программирование на HTML5 с использованием JavaScript и CSS3	8-11 июня
20464	Разработка баз данных Microsoft SQL Server 2014	8-11 июня
10969	Службы Active Directory в Windows Server 2012	8-11 июня
55004	Установка и конфигурирование System Center 2012 Operations Manager	8-11 июня
VICM6	Horizon (совместно с View): Установка, настройка и управление [v6.0]	8-11 июня
VSDW55	VMware vSphere: Design Workshop [V5.5]	8-10 июня
20341	Базовые решения с использованием Microsoft Exchange Server 2013	8-15 июня
CNS-205I	Citrix NetScaler 10 Essentials and Networking (Основы и сетевая архитектура Citrix NetScaler 10)	15-19 июня
DP0159	Symantec NetBackup 7.5 for Windows: Administration	15-19 июня
VSICM55	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.5)	15-19 июня
10747	Администрирование System Center 2012 Configuration Manager (SCCM)	15-19 июня
20486	Разработка ASP.NET MVC 4 веб-приложений	15-19 июня
20463	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	15-19 июня
20342	Продвинутые решения на базе Microsoft Exchange Server 2013	16-22 июня
20342	Продвинутые решения на базе Microsoft Exchange Server 2013	16-22 июня
10748	Внедрение System Center 2012 Configuration Manager	22-24 июня
CNS-301-2I	Citrix NetScaler 10.5 Advanced Implementation	22-26 июня
50331	Техническая поддержка Windows 7 в корпоративной среде	22-26 июня
20487	Разработка служб Windows Azure и веб-служб	22-26 июня
20466	Работа с моделями данных и отчетами в Microsoft SQL Server 2014	22-26 июня
10747	Администрирование System Center 2012 Configuration Manager (SCCM)	23-29 июня
10747	Администрирование System Center 2012 Configuration Manager (SCCM)	23-29 июня
20341	Базовые решения с использованием Microsoft Exchange Server 2013	29 июня – 3 июля
20331	Базовые решения Microsoft SharePoint Server 2013	29 июня – 3 июля
CXD-203-6I	Managing App and Desktop Solutions with Citrix XenApp and XenDesktop 7.6	29 июня – 3 июля
20416	Создание инфраструктуры клиентских приложений	29 июня – 3 июля
10961	Автоматизация администрирования с использованием Windows PowerShell	29 июня – 3 июля
VSOS5.5	VMware vSphere: Оптимизация и масштабирование (VMware – Optimize & Scale v.5.5)	29 июня – 3 июля
CCNAX	Создание сетей на базе оборудования Cisco: Ускоренный курс (Interconnecting Cisco Networking Devices: Accelerated)	29 июня – 3 июля
20467	Проектирование бизнес-аналитики для самообслуживания и решений Big Data	29 июня – 4 июля
10748	Внедрение System Center 2012 Configuration Manager	30 июня – 2 июля

Регионы

Код	Город	Название курса	Даты
RH-255	Санкт-Петербург	Red Hat — Системное администрирование III и экзамены RHCSA и RHCE (7-версия)	25-29 мая
VSICM55	Нижний Новгород	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.5.5)	25-29 мая
БПД	Нижний Новгород	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	25-30 мая
10961	Самара	Автоматизация администрирования с использованием Windows PowerShell	25-29 мая
10747	Тюмень	Администрирование System Center 2012 Configuration Manager (SCCM)	25-29 мая
20414	Омск	Реализация продвинутой серверной инфраструктуры	25-29 мая
10775	Красноярск	Администрирование баз данных Microsoft SQL Server	25-29 мая
10775	Красноярск	Администрирование баз данных Microsoft SQL Server	25-29 мая
6425	Новосибирск	Конфигурирование службы каталогов Windows Server 2008 Active Directory (R2)	15-19 июня
2778	Нижний Новгород	Создание запросов в Microsoft SQL Server 2008 с использованием языка Transact-SQL	22-24 июня
20463	Омск	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	22-26 июня
10775	Нижний Новгород	Администрирование баз данных Microsoft SQL Server	29 июня — 3 июля

Лицензирование Microsoft SPLA



Как бы ни складывалась политическая и экономическая ситуация в мире, бизнес не стоит на месте. Неважно, замедляются ли или ускоряются темпы развития рынка, важна стратегия, которую выбирает компания для ведения бизнеса.

Если вы задумываетесь о привлечении новых клиентов и поддержании лояльности уже существующих, или же стремитесь оптимизировать IT-бюджет собственной компании, работа по программе лицензирования Microsoft SPLA — одна из лучших опций, которые можно выбрать в условиях кризиса.

SPLA для оказания услуг клиентам

Многие эксперты уверены, что именно кризисные периоды оптимальны для того, чтобы начать свое дело: конкуренция уменьшается, среди рабочей силы можно найти высококвалифицированные кадры за приемлемую стоимость, клиенты выделяют бюджет только под действительно качественные продукты и услуги. Соответственно, в кризис выигрывает тот, кто может воспользоваться этими факторами, предложив заказчикам именно то, что им действительно нужно. Используя программу SPLA для оказания услуг своим клиентам, вы можете начать или расширить бизнес за счет облачного лицензирования, помогая клиентам оптимизировать их расходы на IT.

Программа SPLA позволяет использовать лицензии Microsoft для предоставления пользователям услуг доступа к IT-решениям — при этом услуги оплачиваются только постфактум и только в соответствии с объемом предоставления. SPLA может применяться для создания частных и публичных облаков, создания SaaS-решений, а также для сдачи в аренду ПК/серверов с предустановленным ПО. Таким образом, программа SPLA предоставляет выгодные возможности работы с ПО Microsoft для компаний, принадлежащих к телекоммуникационной отрасли, интернет-провайдеров, поставщиков услуг, системных интеграторов, ЦОДов, независимых разработчиков ПО (ISV), а также для компаний, которые осуществляют техническое обеспечение технопарков и бизнес-центров.

Работая по программе лицензирования SPLA, вы сможете предложить своим клиентам IT-решения, которые, прежде всего, будут оптимальны по стоимости. Поскольку по SPLA ПО не приобретается в собственность, а используется по мере необходимости, ваши клиенты смогут перевести затраты на IT из капитальных в операционные.

Это означает, что даже в условиях кризиса, при отсутствии «свободных» средств в бюджете ваши клиенты смогут использовать именно то ПО, которое позволяет наиболее эффективно решать стоящие перед бизнесом задачи. Возможность работать с теми IT-решениями, которые при стандартной модели приобретения были бы недоступны из-за высокой стоимости, обеспечивается тем, что постфактическая помесячная оплата значительно ниже разовой платы за приобретение стандартных лицензий. Также здесь существенно и то, что ваши клиенты смогут попробовать новые инструменты, то есть на практике оценить эффективность и целесообразность определенного ПО для своего бизнеса. Кроме того, поскольку стоимость лицензии на программный продукт не зависит от версии продукта, ваши заказчики смогут свободно варьировать используемые версии, пробовать новейшие и возвращаться к старым без дополнительных затрат.

При этом сами операционные расходы ваших клиентов станут максимально гибкими, поскольку оплачивая только фактически использованное в работе ПО, компания не переплачивает за те решения, которые по каким-то причинам не были задействованы. К примеру, программное обеспечение, которое требуется для решения узкоспециализированных или сезонных задач, в определенные периоды может попросту простаивать – использование облачных решений нивелирует эту проблему: компания может задействовать IT-инструментарий на необходимое время (месяц, два, полгода и т. д.), а затем перестать его использовать или значительно уменьшить число сотрудников, работающих с ним. Подобные колебания в объемах используемого ПО не влекут за собой никаких финансовых издержек.

Еще одна выгодная опция, которую вы сможете предложить клиентам, работая по SPLA, — возможность сохранить часть лицензий из актива компании при переходе к облачной модели работы с ПО (подробнее об этом рассказано в майском номере Softline Direct за 2014 год).

Используя SPLA, вы

- свободны от первоначальных вложений в ПО и авансовых платежей,
- отчитываетесь перед Microsoft только за фактически использованное ПО,
- можете использовать для развертывания необходимых продуктов платформу Azure,
- можете использовать последние версии продуктов,
- можете предоставлять услуги по всему миру,
- получаете бесплатные лицензии для демонстраций, тестирования и администрирования,
- можете использовать лицензии для обеспечения внутренней работы вашей организации в пределах 50% от числа лицензий, использованных для предоставления услуг конечным заказчикам,
- получаете квалифицированную поддержку Softline: от выбора стратегии работы по SPLA (на основе уникальной статистики Softline по наиболее востребованным сервисам) до составления отчетности.

SPLA для холдинговых организаций

Работая по программе SPLA, вы можете использовать лицензии Microsoft для предоставления услуг доступа к IT-решениям не только внешним клиентам, но и пользователям внутри вашей собственной компании. Такой вариант возможен, если услуги оказываются сервисной компанией (неаффилированным лицом) в составе холдинговой организации.

Выделив сервисную компанию и начав работать по SPLA, вы получите доступ практически ко всем продуктам Microsoft без авансовых платежей и начальных инвестиций в ПО. Эти продукты могут быть развернуты на вашем собственном оборудовании, на арендованном оборудовании или же на облачной платформе Azure. При любом варианте вы будете совершать

отчисления Microsoft только за то ПО, которое фактически использовалось вашей сервисной компанией для оказания услуг в подотчетный период.

Широкий спектр доступных по SPLA продуктов обеспечит вам практически неограниченные возможности построения IT-среды и ее максимальную гибкость. Так, можно развернуть частное облако для компании, что позволит снизить стоимость поддержки рабочих мест сотрудников и быстро реагировать на любые изменения в инфраструктуре за счет внедрения сервисно-ориентированной модели потребления ПО. Или же можно создать комплексное коммуникационное решение на базе Microsoft Exchange Server и Lync Server, которое обеспечит ваших сотрудников удобным инструментом для координации работы, управления взаимодействием и т. д. При этом по программе SPLA любой из необходимых вам продуктов будет доступен в самой последней версии. А для демонстраций, предоставления пробного доступа и администрирования ваших услуг и решений вы сможете использовать лицензии бесплатно.

IT-среда, созданная на основе продуктов, лицензируемых по SPLA, будет, во-первых, отличаться мобильностью: ваши сотрудники будут иметь доступ к требуемому ПО из любой точки, где есть Интернет. Во-вторых, такая среда сможет легко и динамично меняться, подстраиваясь под ваши текущие потребности и обеспечивая необходимые IT-мощности для тех задач, которые действительно требуют этого. Наконец, гибкость IT-среды позволит вам не беспокоиться о возможном изменении числа сотрудников: происходит ли в вашей компании сокращение штата или набор сотрудников — благодаря SPLA вы сможете использовать строго необходимое число лицензий.

Все перечисленные возможности доступны по SPLA при минимальных затратах. Работа с необходимыми вашему бизнесу IT-решениями не потребует значительных разовых инвестиций в ПО — только ежемесячных платежей и только за те продукты, которые реально использовались вашими сотрудниками. Оплата за фактическое использование означает, в том числе, отсутствие «набора продуктов» (типа ProfessionalDesktop, CoreCAL) — пула ПО, который обязателен к приобретению, даже если компания планирует использовать только один продукт из всего набора. А также отсутствие требований по стандартизации ПО или закупке ПО на весь парк ПК — требований, которые предъявляются многими корпоративными программами лицензирования, предусматривающими рассрочку оплаты ПО или его аренду.

Наконец, отдельно следует сказать о возможностях, которые SPLA открывает для организаций, стремящихся использовать один домен для неаффилированных структур или часто меняющих состав юридических лиц. Большая часть программ лицензирования позволяет работать с ПО только приобретшей его компании и ее аффилированным лицам; для подключения неаффилированного лица по таким программам требуется покупать специальные дорогостоящие лицензии. В свою очередь, SPLA позволяет неаффилированным лицам вести совместную работу без дополнительных ограничений и затрат. Что же касается ситуаций, особенно часто случающихся в кризисные периоды, когда одно юридическое лицо закрывается, а вновь открывающееся юрлицо никак не связано с закрывшимся — здесь корпоративные программы лицензирования, как правило, не позволяют передавать лицензии от одного юрлица другому. Однако программа SPLA не предусматривает подобных ограничений, позволяя работать с развернутым и лицензируемым по SPLA решением разным юридическим лицам.

Все это делает SPLA одним из наиболее выгодных и оптимальных путей качественного преобразования работы с IT в условиях кризиса. К тому же, в отличие от прайса других корпоративных программ лицензирования Microsoft, прайс программы SPLA остался неизменным после февральского повышения цен.

Получить дополнительную информацию о программе SPLA и принять в ней участие вам поможет:

Игорь Балашов,
директор по развитию бизнеса Softline

+7 (495) 232-00-23, доб. 2500

spla@softline.ru

http://softline.ru/spla/

Выставки и мероприятия

Связь-Экспокомм-2015

Информационная инфраструктура, сети, услуги связи, теле- и радиовещание, IT-услуги, интернет-технологии и многое другое. Масштаб экспозиции — 25 000 кв. м.! Более 500 участников из 22 стран, всего — более 22 000 специалистов.
Большой Медиа-Коммуникационный Форум:

- E-commerce, почта и услуги, доставка;
- ЦОДы, дата-центры и мобильные технологии;
- импортозамещение, отечественный софт, цифровое телевидение России.

12–15 мая 2015 г., Москва, ЦВК «Экспоцентр».

Мир Безопасности

С 19 по 21 мая 2015 г. в Волгоградском Дворце Спорта профсоюзов состоятся две специализированные выставки, организуемые Волгоградским Выставочным Центром «Регион»: XVIII-я выставка технических систем и средств безопасности, информационной безопасности, специальных средств связи «Мир Безопасности» и XVIII-я выставка оборудования, технических и специальных аварийно-спасательных средств, противопожарных систем, оборудования и материалов «СпасПожТех».

май

Конференция DOCFLOW 2015

19 мая в Москве не пропустите главное событие в области управления информацией — конференцию DOCFLOW 2015! Участие бесплатное при регистрации на www.docflow.ru/2015
В программе более 40 бизнес-кейсов, практикумов и дискуссий по новинкам в области технологии управления корпоративной информацией: СЭД, Data Capture, ECM, BPM, BI, CRM, Collaboration, Big Data. Регистрация уже открыта.
19 мая, Москва, Рэдиссон Славянская.

Сибирская строительная неделя

С 20 по 22 мая 2015 года в Омске состоится 20-я выставка «Сибирская строительная неделя».
Тематические разделы выставки: современные строительные материалы, инструменты, оборудование и конструкции, энергосберегающие технологии, строительная химия, монтажные и проектные работы, предметы интерьера, ремонт и содержание дорог, спецтехника и др.
Дополнительная информация на сайте http://intersib.ru/
Звоните: (3812) 22-04-59

Современные системы безопасности — Антитеррор

XI Всероссийский специализированный форум-выставка систем и средств безопасности, охраны и противопожарной защиты, полицейской и криминалистической техники, аварийно-спасательного оборудования. В программе выставки конференции, круглые столы, семинары и мастер-классы от ведущих компаний отрасли.
XI Всероссийский специализированный форум-выставка «Современные системы безопасности — Антитеррор» пройдет в Красноярске с 27 по 29 мая 2015 года в выставочном центре «Сибирь».

Тайные знания и инструменты
инженеров-дорожников
в журнале

САПР и ГИС
автомобильных дорог

cadgis.ru

АВТОМАТИЗАЦИЯ РАБОЧИХ ПРОЦЕССОВ ДЛЯ ГОСУДАРСТВА И БИЗНЕСА

NOVACOM®
a Softline Company

РОССИЯ: 8 800 23 200 23 info@nvcm.net

БЕЛАРУСЬ: +375 17 328 329 4 info@novacom.by