

softline direct

СПЕЦИАЛЬНЫЙ ВЫПУСК: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ #4 2016

Подход Softline к проектированию ИБ-систем

Аналитика ИБ с IBM QRadar Security

Intelligence Platform

Защищенное облако

Есть ли жизнь после DLP?



Бизнес-погода: СОВЕРШЕННО ЯСНО И БЕЗОПАСНО



**Autodesk Maya 2017:
большие перемены**



STATISTICA

Контроль качества Анализ процессов Планирование экспериментов

Продукты серии Statistica – это мощнейшие инструменты для анализа данных, визуализации, прогнозирования, нейросетевых вычислений, data mining, контроля качества, big data.

Statistica Quality Control (QC) – набор инструментов для контроля качества, который полностью соответствует стандартам ISO/DIN, включает специализированные модули и разнообразные инструменты для реализации методологии Шесть сигм.

- Statistica Quality Control Charts (Карты контроля качества) – полностью настраиваемые (вызываемые из других приложений), простые, доступные и гибкие карты с набором опций автоматизации для упрощения ежедневных пользовательских задач.
- Statistica Process Analysis (Анализ процессов) – модуль для анализа пригодности процесса, построения карты пригодности R&R и запуска других процедур контроля и улучшения.
- Statistica Design of Experiments (Планирование экспериментов) – набор методов планирования экспериментов и соответствующих технологий визуализации, включая интерактивные профили желательности.

Все модули блока Statistica QC доступны в любом программном продукте линейки Statistica.

Statistica Enterprise Server – интегрированная многопользовательская система, объединяющая в себе эффективный интерфейс для доступа к центральному многопользовательскому репозиторию данных, средства для совместной работы пользователей и мощный функционал статистического анализа данных, доступный в различных продуктах линейки Statistica.

Преимущества корпоративной системы

- Средства для совместной работы групп пользователей, функциональные возможности обмена знаниями между пользователями
- Совместимость со всеми распространенными СУБД
- Автоматическая генерация отчетов в заданном формате (pdf, html, doc), задание шаблона отчета
- Возможность управления данными с удаленных серверов "на месте"
- Автоматический мониторинг и анализ данных, выявление ошибок, автоматическое оповещение, фильтрация данных
- Простые инструменты администрирования, настройка различных интерфейсов для разных групп пользователей

Курсы Академии Анализа Данных по промышленной аналитике

- Лекции по управлению качеством (SPC)
- Анализ промышленных данных: исследование зависимостей, классификация, прогноз
- Интенсивный тренинг по управлению качеством на современном предприятии
- Углубленный курс по промышленной аналитике и управлению технологическими процессами на современном предприятии

Узнать о наших курсах подробнее вы можете, на сайте www.statsoft.ru или же позвонив по нашему телефону.

Видеоуроки
www.statsoft.ru



ВСМП

Statistica является мощной аналитической системой для профессионального анализа, что позволяет решать широкий круг задач любой сложности...

Биокад

Замечательное ПО, позволившее значительно упростить проведение анализа данных. Statistica – незаменимый помощник!

КиК

Использование пакета такого уровня позволяет с минимальными затратами времени получать отличные результаты при анализе производственных данных...

Professional

Полный набор мощных аналитических инструментов для анализа, прогнозирования данных, средства для построения линейных/нелинейных моделей, проведения многомерного анализа, а также новейшие инструменты Dashboards для удобной визуализации результатов анализа и их графического представления.

Expert Manufacturing

Инструмент обладает расширенным функционалом для извлечения, преобразования и загрузки данных, управления сложными производственными процессами и их оптимизации, а также средствами для связи с PI-системами предприятий, включает все аналитические инструменты версии Professional.

Expert Data Science

Эффективная и удобная в использовании система для предиктивной аналитики со встроенной экспертизой data scientists, содержит инструменты для всего процесса Data Mining – от построения запросов к БД до создания итоговых отчетов, а также обеспечивает создание гибких правил в проектах обработки данных.

Enterprise

Система позволяет проводить мониторинг процессов, идентифицировать и предотвращать внештатные ситуации на производстве. Продукт совмещает все возможности Statistica QC (карты контроля качества, анализ процессов, планирование экспериментов, инструменты Шесть сигм), технологии Data Mining, а также средства визуализации Dashboards.

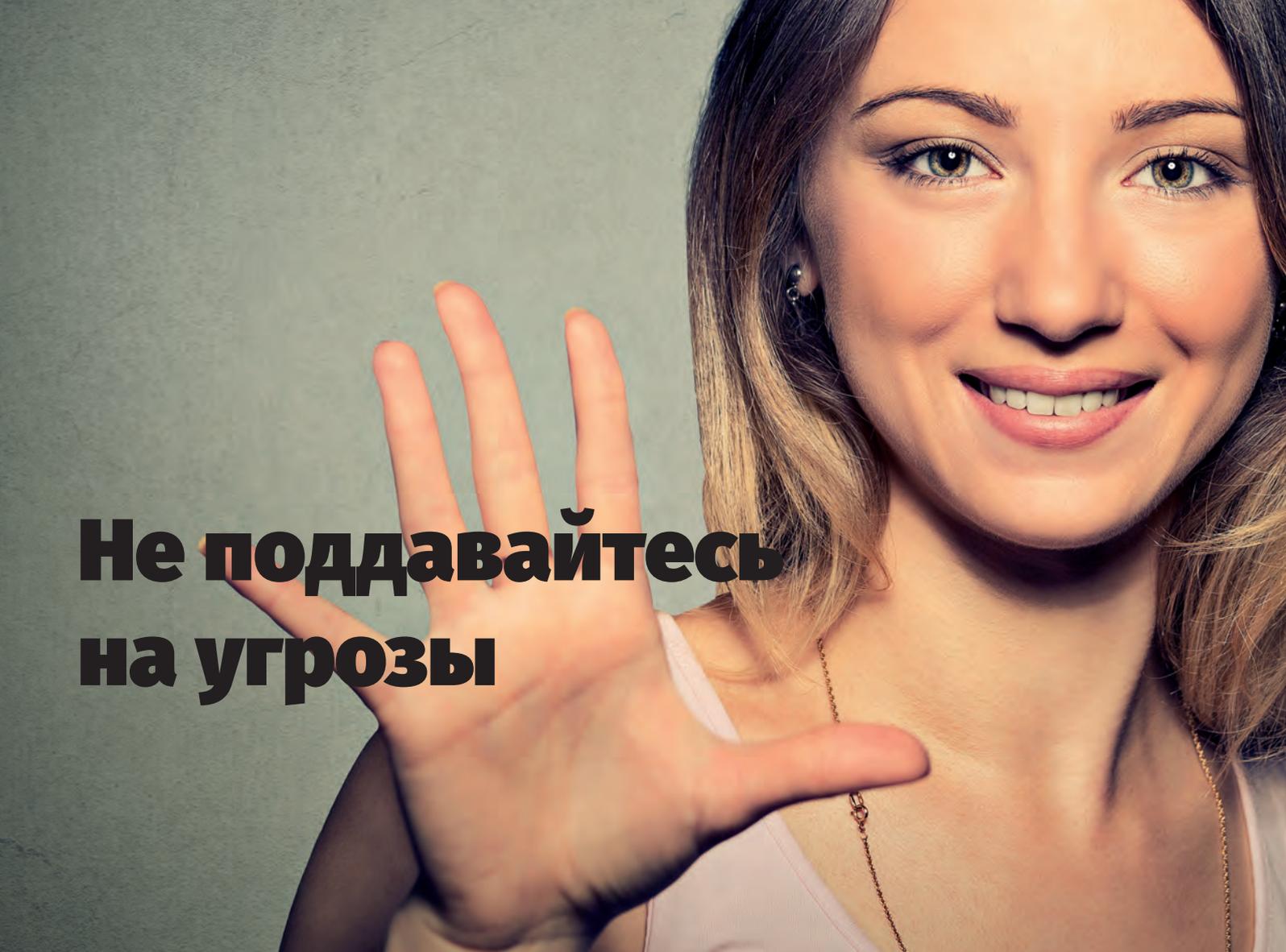


StatSoft® Russia

(495) 787-77-33

info@statsoft.ru

www.statsoft.ru



Не поддавайтесь на угрозы

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

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

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

В области информационной безопасности непрерывно происходят 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 внедрения в информационные системы, которые еще недавно могли использовать разве что представители спецслужб, стали доступны рядовым злоумышленникам, использующим их с целью финансового обогащения.

Все это определяет следующий виток противостояния, в котором бизнесу необходимо выработать новые способы противодействия изменившимся угрозам. Давайте делать это вместе. Только так мы будем способны ответить на любые вызовы – а все необходимые средства уже есть в арсенале Softline.

Мы желаем вам приятного чтения и успехов в делах!



34

12

18

27

42

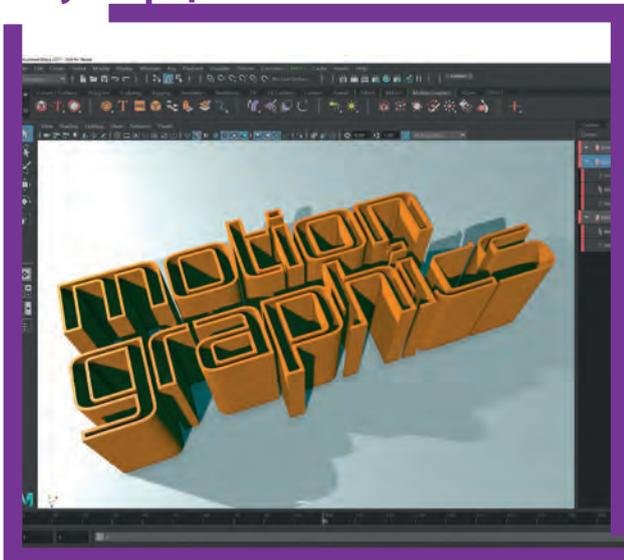
Эффективность бизнеса

Лучшие продукты.....	8
Автоматизация бизнес-процессов «Электронной торговой площадки Газпромбанка».....	10

Производство

Autodesk Maya 2017. Перемены за год.....	42
MapInfo Pro и MapInfo Pro Advanced.....	52
Softline обеспечила управление мобильными устройствами в магазинах «Кораблик».....	53

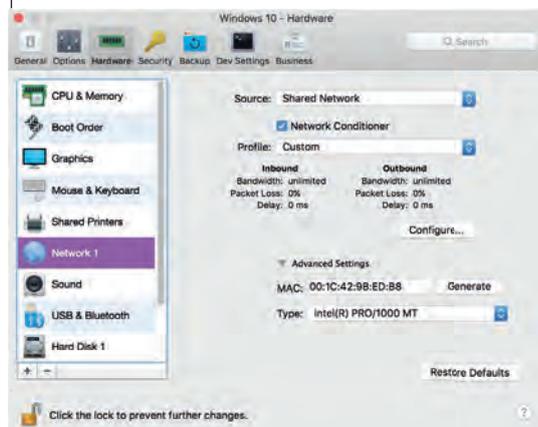
Разработчики подразделения Media&Entertainment компании Autodesk выпустили новую версию своего ведущего решения для анимации и эффектов — Maya. Стр. 42



СОДЕРЖАНИЕ

Маркетинг

Новый Parallels Desktop 12.....	54
---------------------------------	----



Обучение

Расписание курсов в Учебном центре Softline.....	56
Авторизованные курсы Microsoft.....	58
Центры тестирования и сертификация IT-специалистов.....	60
Вкладывайтесь в знания.....	61
Новости Учебного центра Softline.....	62
Учебный центр поможет внедрить профстандарты.....	63

Аппаратные решения

Эволюция блейд-систем Flex System Lenovo.....	64
---	----

Наука и искусство

Платформа MAPS от компании Scienomics.....	68
PerkinElmer. Решения для химии и биологии.....	70
Решения Webex.....	72



Каталог
IT-решений
и сервисов для
бизнеса

Softline
direct

#4-2016

2016-04(167)-RU
Учредитель: ЗАО
«СофтЛайн Трейд»

Издатель:
Игорь Боровиков

Главный
редактор:
Лидия Добрачева

Выпускающий
редактор:
Антонина Татчук

Редакторы:
Яна Ламзина,
Максим Туйкин

Дизайн
и верстка:
Юлия
Константинова,
Юлия Аксенова,
Григорий Стерлев,
Вадим Владов

Над номером
работали:
Светлана Ситина,
Татьяна Гапоненко,
Ирина Щербакова,
Алла Зайцева,
Наталья Татулова,
Кристина
Меламед, Ирина
Галактионова,
Николай Антипов,
Екатерина Франк,
Евгений Акимов,
Дмитрий Ковалев
и др.

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

Перепечатка
материалов только по
согласованию
с редакцией
© Softline-direct,
2016

Softline
в соцсетях



SoftlineCompany



Softlinegroup



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Карта решений: подход Softline к проектированию ИБ-систем .. 12
У вас есть выбор. Выбирайте для себя лучшее 18
DataBase Firewall 22
Зачем нужен антифрод? 25
Конфиденциальные данные – под надежный контроль! 26
Есть ли жизнь после DLP? 27
Enterprise Mobility Suite: корпоративные данные в безопасности 28
Veeam Availability Suite 30
Kaspersky Security для бизнеса 32
IBM QRadar Security Intelligence Platform..... 34
ИТ-инфраструктура «Горного» под защитой! 36
Врачи на страже персональных данных вместе с Softline 37
Модернизация системы защиты персональных данных Нижегородского водоканала.. 38
Softline провела аттестацию производителя защищенной полиграфической продукции . 39
Стратегия защиты..... 40

Все чаще появляются новости о взломах систем крупных, хорошо защищенных компаний. Злоумышленники, действуя в составе хорошо организованной группы, получают привилегированный доступ к бизнес-системам.
Стр. 22



Solar Dozor дает специалисту все необходимые инструменты для выявления признаков экономических преступлений в организации и проведения полномасштабных расследований.
Стр. 27

По вине облачных провайдеров утечек практически не бывает. Практика зарубежных исследований доказывает, что в большинстве случаев утечка информации происходит внутри компании из-за сотрудников.
Стр. 18



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

1

Весь спектр решений и сервисов

Softline — лидирующий глобальный поставщик ИТ-решений и сервисов. Мы предлагаем комплексные технологические решения, лицензирование программного обеспечения, поставку аппаратного обеспечения и сопутствующие ИТ-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 800 инженеров и технических специалистов обслуживают наших клиентов и помогают им выбрать оптимальные ИТ-решения. По итогам 2015 финансового года Softline достигла оборота около \$741 млн, а за последние 11 лет совокупный среднегодовой темп роста продаж (CAGR) составил 37%.

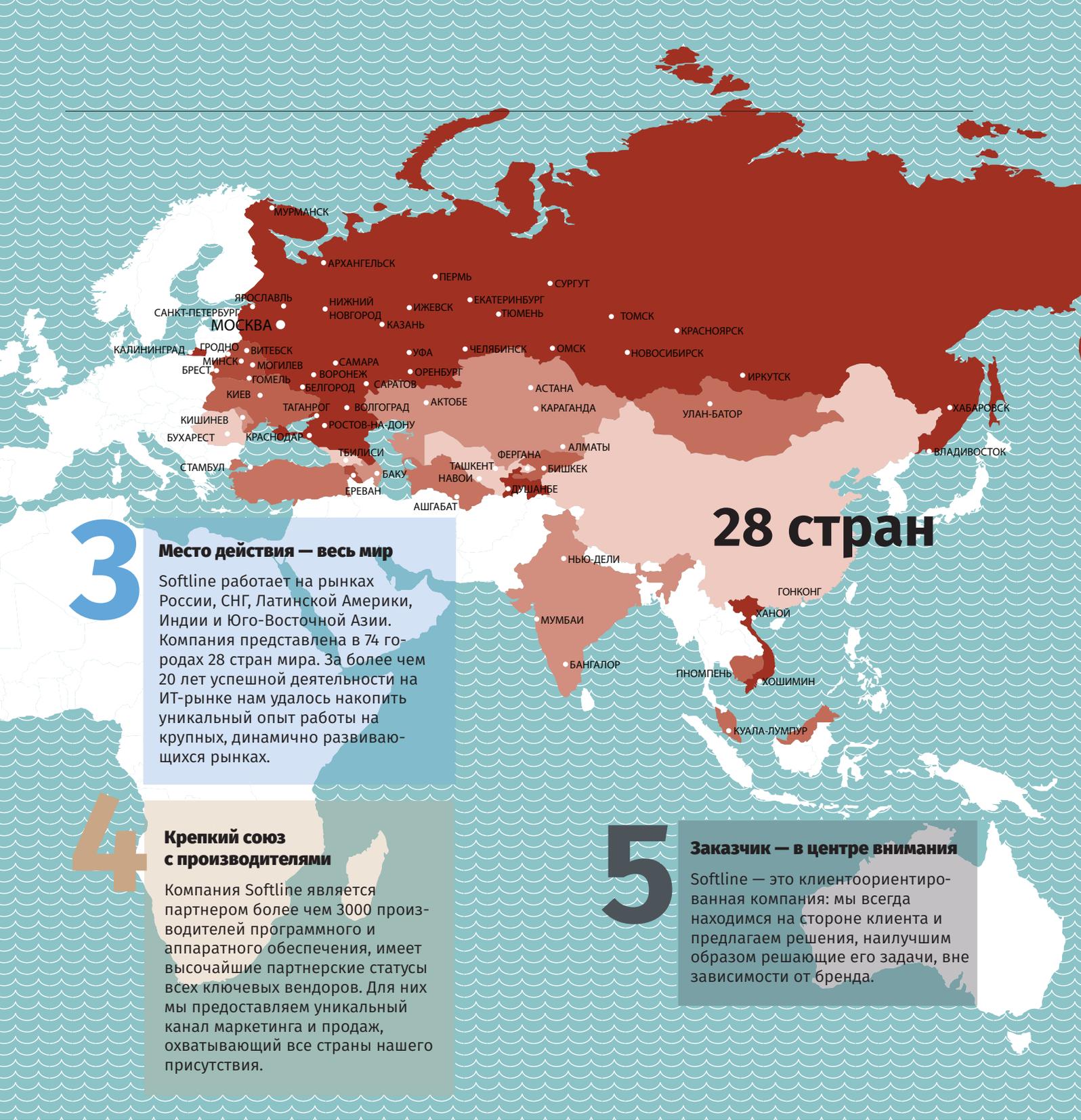
Статусы Softline

74 города

Microsoft Partner

- Gold Messaging
- Gold Business Intelligence
- Gold Small Business
- Gold Collaboration and Content 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
- Gold Learning
- Silver Application Development
- Silver Hosting
- Silver Project and Portfolio Management





28 стран

3

Место действия — весь мир

Softline работает на рынках России, СНГ, Латинской Америки, Индии и Юго-Восточной Азии. Компания представлена в 74 городах 28 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

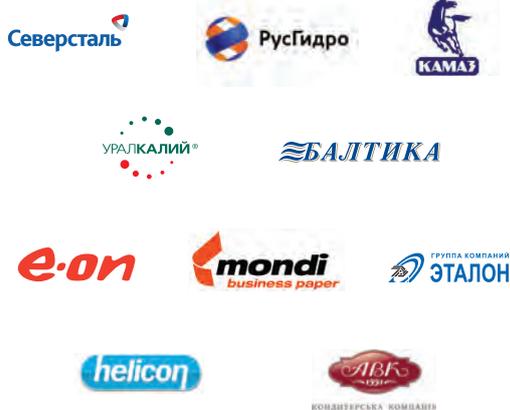
Softline — это клиентоориентированная компания: мы всегда находимся на стороне клиента и предлагаем решения, наилучшим образом решающие его задачи, вне зависимости от бренда.



Global IT Solution and Service Provider

Портрет компании

Промышленность



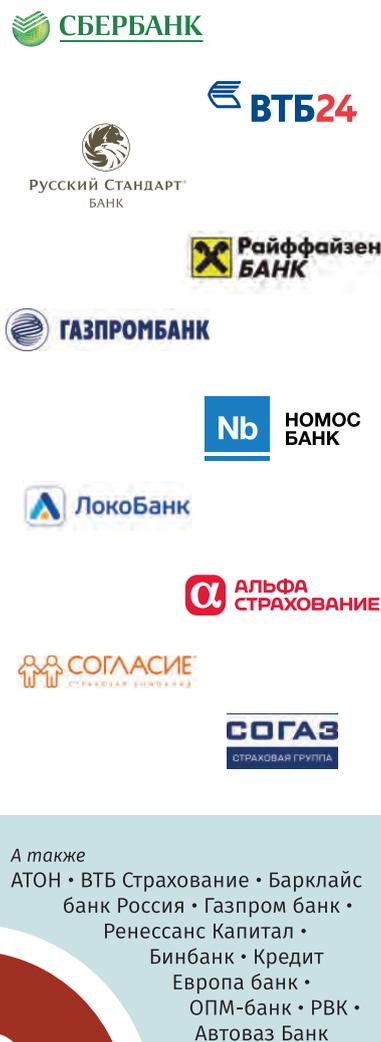
А также
РУСАЛ • STADA CIS •
Акрихин •
Трансмашхолдинг •
Совкомфлот • Sollers •
GM-Avtovaz • СО ЕЭС •
Трансмашхолдинг ОАО
«Камчатскэнерго» •
Вимм-Билль-Данн •
МРСК Северного
Кавказа

Розница, услуги



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

Банки и финансовые организации



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

20+
лет в ИТ

3 000+

поставщиков программного и аппаратного обеспечения

softline®

800+

технических
специалистов

Телекоммуникации, СМИ, развлечения



TELE2



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

Госзаказчики



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 • «Башкиргражданпроект» • ПИПРО • САФУ им. М.В. Ломоносова • Администрация Иркутска

1 300+

менеджеров по продажам

Нефтегазовая отрасль



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

Лучшие продукты

ESET NOD32 Business Edition 5

Этот антивирус разработан для файловых серверов, рабочих станций и почтовых шлюзов средних и крупных организаций. Система NOD32 Business Edition обнаруживает и блокирует вирусы, шпионские программы, рекламные приложения, программы типа rootkit и другие интернет-угрозы. ESET NOD32 Business Edition обеспечивает надежную защиту, не снижая производительность рабочих станций на сервере.

С помощью мощной многоуровневой структуры управления ESET Remote Administrator обеспечивается удаленное администрирование и поддержка тысяч систем NOD32 в крупных распределенных корпоративных сетях.

Новое в версии 5: оперативное сканирование, контроль конфиденциальной информации, сканирование веб-контента, компоненты ESET SysInspector и SysRescue, создание «загрузочного диска» для восстановления системы и многое другое.



eToken 3.60

Электронные ключи, представляющие собой персональные средства аутентификации и безопасного хранения данных. Аппаратно поддерживают работу с цифровыми сертификатами и электронной цифровой подписью. Линейка продуктов eToken включает в себя USB-ключи, смарт-карты, комбинированные устройства и автономные генераторы одноразовых паролей.

Подобно обычному компьютеру АПК eToken содержат процессор и модули памяти, функционируют под управлением собственной операционной системы и выполняют необходимые прикладные программы. Устройства фактически являются миниатюрными ПК, реализующими защищенное хранение персональных данных и предотвращающими несанкционированный доступ.



Security Studio Endpoint Protection 7.7 1

Сертифицированная система защиты ПК от сетевых вторжений, спама и вредоносного ПО. С ее помощью организации могут полностью выполнять требования Федерального закона «О защите персональных данных» относительно поддержания безопасности информации в информационных системах с применением межсетевых экранов, антивирусов, служб обнаружения и предотвращения вторжений, при обработке информации, которая содержит персональные данные. Общее назначение продукта – защита сетевых рабочих мест, обрабатывающих персональные данные и иную конфиденциальную информацию. Сертификаты ФСТЭК России на компоненты решения Security Studio Endpoint Protection позволяют использовать его для защиты информационных систем персональных данных до класса К1 включительно и автоматизированных систем до класса 1Г включительно.



Kerio Control 9.0

Это мощное и универсальное решение, включающее в себя межсетевую экран, системы IDS/DPS, контроль и антивирусное сканирование интернет-трафика, функцию MAC-фильтрации и возможность работы по VPN с двухфакторной проверкой удаленных пользователей. Оно может стать идеальной альтернативой популярным, но устаревшим решениям. Kerio Control 9.0 – сертифицированный продукт, который можно использовать в государственных, образовательных, медицинских и других учреждениях (сертификация ФСТЭК по 3-му классу защищенности).

Kerio Control 9.0 отличается простотой администрирования и гибкостью развертывания и может использоваться в любой ИТ-среде. Хороший выбор для малых и средних предприятий.



tekmi
облачная телефония
a Softline Company

**ВИРТУАЛЬНЫЙ ОФИС
И ОБЪЕДИНЕННЫЕ
КОММУНИКАЦИИ**

**ПОЛНОФУНКЦИОНАЛЬНАЯ
ВИРТУАЛЬНАЯ АТС**

Используйте
в любой точке мира,
где есть Интернет!

14
дней

**БЕСПЛАТНО
демо-версия**

Включено 50 руб. на проверку качества связи

hello@tekmi.ru

www.tekmi.ru

8 (800) 505-50-70



АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ «ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ ГАЗПРОМБАНКА»

О ПРОЕКТЕ

Заказчик:

«Электронная торговая
площадка Газпромбанка»

Отрасль:

банковская

Деятельность:

обеспечение обслужива-
ния ключевых клиентов
при организации закупоч-
ных процедур

Штат:

более 50 человек

Ситуация:

требовалось создать
единое информационное
пространство

Решение:

ELMA BPM

Softline объявляет о завершении проекта по развертыванию системы управления бизнес-процессами для «Электронной торговой площадки Газпромбанка». Это позволило заказчику повысить эффективность работы сотрудников и улучшить обработку и анализ деловой информации.

О компании

«Электронная торговая площадка Газпромбанка» предоставляет пользователям инструменты для моделирования бизнес-процессов и полностью совместима с существующими ERP-, SRM-, CRM-системами.



СИТУАЦИЯ

В связи с активным развитием платформы и наращиванием конкурентных преимуществ, заказчику потребовалась информационная система, которая смогла бы автоматизировать ключевые бизнес-процессы и создать единое информационное пространство. Партнером проекта была выбрана компания Softline, специалисты которой обладают большим опытом внедрения систем автоматизации бизнес-процессов.

РЕШЕНИЕ

Специалисты Softline предложили заказчику российский программный продукт ELMA BPM, оптимальный по функционалу и стоимости. ELMA BPM – система управления бизнес-процессами, повышающая эффективность взаимодействия сотрудников компании посредством автоматизации контроля и выполнения рабочих задач. В ней осуществляется моделирование бизнес-процессов на базе графических моделей, производится их оптимизация с использованием поступающих предложений. Решение состоит из таких блоков, как «Бизнес-процессы» и «Внутренний портал», на последнем отображаются задачи, сообщения, инструменты и настройки.



Результаты:
обеспечена координация работы специалистов различных подразделений, сократилось время принятия управленческих решений

ПРОЕКТ

В ходе реализации проекта специалистами Softline и ELMA был проведен анализ бизнес-процессов заказчика, разработана схема внедрения программного продукта. Кроме того, были определены роли пользователей системы, зоны функциональной ответственности персонала.

РЕЗУЛЬТАТ

В результате была произведена автоматизация 50 рабочих мест сотрудников «Электронной торговой площадки Газпромбанка», налажены ключевые процессы в модулях управления взаимоотношениями с клиентами, документооборотом, проектами (CRM, ECM и PRJ), настроены системы управленческого учета и напоминаний, реализованы основные этапы обслуживания клиентов.



«Внедрение системы ELMA BPM позволило нам автоматизировать управление бизнес-процессами, что обеспечило координацию работы специалистов различных подразделений и сократило время принятия управленческих решений».

Валерий Орехов,
советник генерального директора по ИТ «Электронной торговой площадки Газпромбанка»

ВРМ. ПРИНЦИП РАБОТЫ

Проектирование



Системы управления бизнес-процессами пришли в Россию с Запада, где этот класс программ называется BPMS (Business Process Management System) или BPM-системы. Задача этого ПО – осуществить программную поддержку концепции процессного управления организацией. Работа системы управления бизнес-процессами основана на простой идее: на этапе внедрения системы осуществляется моделирование бизнес-процессов организации с помощью наглядных диаграмм. Затем эти диаграммы загружаются в компьютерную систему и становятся исполнимыми, то есть программа позволяет отследить и проконтролировать исполнение бизнес-процессов в реальной практике работы предприятия. Такой подход позволяет максимально приблизить реальное выполнение бизнес-процессов в организации к их идеальной модели, которая изначально разрабатывалась. Приложение ELMA BPM реализует концепцию BPM, что позволяет строить гибкие адаптивные информационные системы, способные оперативно меняться вместе с изменением бизнес-процессов компании. Благодаря использованию приложения ELMA BPM можно навести порядок в бизнес-процессах организации, сделать их выполнение четким и формальным.

«Организациям приходится иметь дело с большими объемами информации, поступающей из различных источников. Российская система ELMA BPM позволила сотрудникам заказчика сделать прозрачной любую совместную деятельность, упростить корпоративное взаимодействие и максимально гибко организовать рабочий процесс».

Искендер Шестопал,
руководитель направления продаж бизнес-решений компании Softline

Карта решений:

подход Softline к проектированию ИБ-систем

Softline не только продает те или иные программные или аппаратные продукты. Мы умеем и любим создавать сложные и функциональные системы, в которые вкладываем опыт и знания как отдельных экспертов, так и компании в целом.



Анализ и оценка информационной безопасности компании

Аудит информационной безопасности

Можно провести полный аудит всех инфраструктурных и прикладных ИТ-систем и процессов в организации, а можно обследовать отдельные системы: web-ресурсы, сетевую инфраструктуру, бизнес-системы ERP и CRM, платежные, биллинговые, бухгалтерские и банковские системы и другие компоненты ИТ. В итоге оценивается текущий уровень и перспективы развития процессов ИБ для согласования с требованиями бизнеса.

Наша методология предусматривает использование ряда отраслевых стандартов:

- ISO 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.
- ISO 27002. Информационные технологии. Свод правил по управлению защитой информации.
- ISO 27005. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
- ФЗ-152 «О персональных данных» и др.

Разработка концепции информационной безопасности

В концепции информационной безопасности фиксируются направления дальнейшего развития ИБ, определенные на основе аудита текущего состояния системы, описываются стратегические цели и задачи построения системы обеспечения ИБ организации, приоритетность выполнения задач, план работ и распределения ресурсов и инвестиций. Концепция развития составляется с учетом специфики бизнеса заказчика и приоритетов развития бизнеса и ИТ.

Внедрение и управление политикой безопасности и рисками

Только лишь внедрение средств и систем ИБ не гарантирует защищенность компании. Для поддержания уровня безопасности необходимо внедрение политик и регламентов ИБ и правильное управление ими. Внедрение политик помогает снижать капитальные и эксплуатационные расходы, делать работу непрерывной и защищенной.

Мы создаем решения с высокой интеллектуальной составляющей



Анализ и оценка информационной безопасности компании



Внедрение системы обеспечения информационной безопасности



Центры реагирования ИБ (SOC)



Соответствие требованиям и стандартам, защита конфиденциальной информации (ПДн, аттестация)



Защита сети, АТР



Защита от мошенничества



Защита критичной инфраструктуры и АСУТП



Защита информации



Поддержка

Внедрение системы обеспечения информационной безопасности

Защита онлайн-сервисов

• Защита веб-приложений (WAF)

Разнообразие и интерактивность – весомые плюсы web-приложений. Однако из-за этого они подвергаются целому ряду угроз, от которых не могут защитить традиционные межсетевые экраны. Здесь на помощь может прийти WAF, Web Application Firewall, защитный экран для приложений, обменивающихся данными через HTTP и HTTPS. Современные WAF работают не только на уровне сигнатур (это позволяет надежно определять известные виды атак), но и на уровне бизнес-логики.

• Защита от DDoS-атак

Для защиты корпоративных интернет-ресурсов от DDoS-атак мы предлагаем заказчикам не только обширный портфель программных и аппаратных решений нескольких уровней, но и услуги по налаживанию организационных процессов, необходимых для поддержания постоянного уровня защищенности.

Нам хорошо знакомы все категории DDoS-атак: объемные атаки, атаки на уровне протоколов, на уровне приложений. Эффективные способы защиты от них различаются в зави-

симости от типа атаки и расположения защищаемого интернет-ресурса: это фильтрация трафика на площадке заказчика или на уровне дата-центра, либо специализированные внешние сервисы защиты, обладающие достаточными канальными мощностями и вычислительными ресурсами.

К профилактическим практикам мы относим резервное копирование, своевременное устранение программных брешей в безопасности и наличие договоренности с сервисом защиты от DDoS, знание нормальной активности на ваших ресурсах, способное помочь идентифицировать аномальные события, наличие плана спасения.

• Технический анализ защищенности, тесты на проникновение

Каждый год мы проводим более 50 тестов: проверяем защищенность отдельных систем, веб- или мобильных приложений, делаем комплексный аудит информационной безопасности крупнейших систем международного уровня. Нам доверяют тысячи клиентов по всему миру. Наиболее глубокий анализ защищенности обеспечивают тесты на проникновение.



▪ **Анализ кода**

Для анализа кода сложных современных систем, состоящих из множества взаимосвязанных компонентов, мы предлагаем инструментальные средства анализа по требованиям ИБ. Большинство из них можно применять как в процессе разработки ПО, так и для аудита уже готовых программных систем.

Защита веб и почты

▪ **Защита веб-трафика**

Мы предлагаем системы, которые динамически анализируют контент, ограничивая доступ к нежелательным ресурсам, категоризируют сайты, мгновенно обнаруживают и блокируют угрозы.

▪ **Защита почтового трафика**

Электронная почта организации – самая простая цель для злоумышленников. Мы предлагаем действующие механизмы внедрения политик обработки почты, мониторинг и отчетность. Администрирование станет простым, дешевым и будет соответствовать нормам права.

Защита серверов, рабочих станций, виртуальной инфраструктуры, мобильных устройств

▪ **Защита серверов, конечных точек**

Услуга предусматривает классическую защиту рабочих станций и серверов антивирусным ПО, брандмауэрами и при необходимости контролирует целостность для серверов с редко изменяемыми конфигурациями.

▪ **Защита виртуальной инфраструктуры**

Виртуальным серверам присущи те же уязвимости, что и физическому оборудованию. Кроме того, в их отношении могут быть реализованы специфические сценарии вторжений. Компания Softline предлагает решения по управлению безопасностью в виртуальной среде. Они соответствуют требованиям российского законодательства, защищают сведения, содержащие государственную тайну, конфиденциальную информацию: коммерческую тайну или персональные данные. Мы поможем предотвратить:

- атаки на гипервизор с виртуальной машины;
- атаки на гипервизор из физической сети;
- атаки на диск виртуальной машины;
- атаки на средства администрирования виртуальной инфраструктуры;
- атаки на виртуальную машину с другой виртуальной машины;
- атаки на сеть репликации виртуальных машин;

- неконтролируемый рост числа виртуальных машин.
- Защита мобильных устройств
- Защита СУБД

Решения класса DBF (DataBaseFirewall) – комплексный инструмент защиты корпоративных СУБД, предотвращающий основные угрозы для доступности, целостности и конфиденциальности данных.

Управление доступом

▪ **IDM, SSO, PKI**

Системы Identity Management (IDM) обеспечивают управление учетными записями, работая на стыке задач ИБ, управления ИТ-ресурсами и бизнеса. Отслеживая неактуальные учетные записи и учетные записи с избыточными полномочиями, IDM-системы позволяют повысить уровень информационной безопасности и одновременно упростить бизнес-процессы. С помощью такой системы ИТ-специалисты смогут оперативно реагировать на прием, увольнение, должностные перемещения персонала, появление новых информационных систем, изменения ролевых политик.

В дополнение к IDM используется технология единого входа – Single Sign-On (SSO). Единжды войдя в сеанс работы, пользователь работает со всеми приложениями без необходимости дополнительно подтверждать личность. Для управления доступом также используется инфраструктура открытых ключей, Public Key Infrastructure (PKI). С ее помощью механизмы двухключевой криптографии безопасно применяются в распределенных системах.

▪ **PIM**

Решения класса Privileged Identity Management (PIM) используются для того, чтобы предотвратить потенциально опасные действия системных администраторов, инженеров, занимающихся настройкой сетевого оборудования, и специалистов на аутсорсинге, выполняющих обслуживание ИТ-инфраструктуры по договору.

▪ **Аудит доступа к файловым ресурсам**

Для защиты файловых ресурсов необходимо назначать и разграничивать права на доступ и изменение документов по пользователям и ролям, а также отслеживать и протоколировать все действия с файлами. Мы предлагаем решения, способные помочь организовать контроль за файловыми ресурсами за счет назначения и разграничения прав доступа к данным. Заинтересованным лицам будет также доступна подробная отчетность обо всех фактах чтения или изменения файлов, изменения атрибутов и т.д.

Защита от мошенничества

Antifraud

Антифрод-системы дают возможность автоматически обнаруживать попытки мошенничества (со стороны сотрудников, клиентов и третьих лиц) по цифровому следу, который они неизбежно оставляют в информационных системах, и своевременно поднимать тревогу. Хотя наиболее известно применение ИТ в борьбе с мошенничеством в финансовой сфере (защита ДБО и процессинга, защита АРМ КБР), ИТ-решения можно и нужно применять для выявления и расследования инцидентов в других отраслях.

Мы хорошо знаем схемы мошенничества в таких отраслях как банки, ритейл, энергетика, страхование. Это позволяет нам создавать действенные системы защиты от мошенничества, настроенные на обнаружение актуальных угроз и способные сопоставлять самую разную информацию – данные видеонаблюдения, кассовые данные, геопозиционирования транспортных средств и т.д.

Защита сети, АТР

Межсетевые экраны нового поколения

Межсетевые экраны прошлых лет фильтровали сетевой трафик на низком уровне, по портам и адресам. Современной альтернативой им стали комплексные брандмауэры, объединяющие все компоненты защиты – системы обнаружения и предотвращения вторжений, межсетевой экран, VPN, антивирус, антиспам, контент-фильтр, балансировку нагрузки, средства отчетности и даже DLP. Такие межсетевые экраны представлены как программными решениями, так и программно-аппаратными комплексами UTM (Unified Threat Management). Брандмауэры нового поколения управляются из единого центра и способны учитывать, какие именно приложения и пользователи генерируют трафик.

Защита от целевых атак и атак «нулевого дня»

Современные кибератаки все чаще ориентированы на конкретную отрасль (банки, ритейл, промышленность, гос. сектор, интернет-магазины и т.п.) или конкретную компанию. Уникальный характер таких угроз позволяет с легкостью обходить классические средства защиты – антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы и т.д. Мы предлагаем услуги по внедрению

Сервис детектирования взлома хостов (определение зараженности ПК)

Мы предлагаем заказчикам решения, позволяющие удаленно, через интернет, обнаруживать зараженные ПК и мобильные устройства пользователей и скомпрометированные идентификаторы клиентов. Это позволяет гарантировать обращение к онлайн-сервису только с «чистых» устройств, что особенно важно в сфере онлайн-платежей. Решения позволяют своевременно прекратить обслуживание через зараженные устройства и предотвратить таким образом попытки взлома или мошенничества.

Системы проверки контрагентов

Внедрение такой системы позволяет в автоматическом режиме проверять много контрагентов, сопоставляя данные из имеющихся внешних (СПАРК, Интегрум, ЕГРЮЛ и т.д.) и внутренних (например, черные и белые листы) источников.

специализированных средств обнаружения современных атак («песочницы», детекторы аномалий, мониторинг процессов на рабочих станциях), а также услуги по выстраиванию необходимых процессов эффективного противодействия целевым атакам (аналитика по инцидентам, локализация заражения в сети, действия по предотвращению атаки и исключению повторных инцидентов).

Firewall management

В большой и распределенной сети может быть установлено множество программных и аппаратных межсетевых экранов разных производителей, при этом настроенные на них правила, запреты и прочие особенности конфигурации могут образовывать запутанную и противоречивую структуру. Внедрение специализированного решения по анализу, контролю конфигурации и аудиту управления брандмауэрами поможет разобраться в существующем положении дел и наладить процесс автоматизированного и оптимизированного управления.

Мы умеем внедрять такие интеллектуальные решения и поможем не только развернуть решение, но и провести анализ, выявить циклы и противоречия маршрутизации, составить рекомендации по оптимизации.





Защита критической инфраструктуры и АСУТП

Защита АСУТП

Основная задача ИБ в промышленности – обеспечение непрерывности и безопасности производственного процесса. В последнее время становятся актуальными риски, которые несет проникновение в АСУТП традиционных сетевых и программных технологий (Ethernet, Windows). Наш сервис обследования защищенности промышленных систем подразумевает быстрое и недорогое создание эскизного проекта защиты АСУТП без деталей реализации и рекомендаций тех или иных вендоров. В проекте учитываются требования Приказа ФСТЭК России №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, по-

тенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Решения по однонаправленной передаче данных

Для минимизации риска постороннего вмешательства в бизнес-сети и инфраструктуру, компания Softline предлагает решение по однонаправленной передаче данных (дата-диод). Это программно-аппаратный комплекс, обеспечивающий доступ к критической информации и процессам. В основе – однонаправленная передача данных, обеспечивающая поддержку различных протоколов (особенно SCADA-протоколов, в силу специфики применения). В таком случае риск обратного влияния на защищаемую сеть отсутствует.



Защита информации

Шифрование

Необходимость в криптографической защите данных для их хранения или передачи возникает в самых разных областях. Компания Softline предлагает криптографические решения для самых разных сценариев с участием различных информационных систем, серверов, корпоративных рабочих станций, мобильных устройств. Никто посторонний, даже получив доступ к устройствам или перехватив трафик, не прочитает закрытые данные.

тальной базы, а также расследования инцидентов безопасности.

IRM

Эффективное дополнение DLP – система Information Right Management (IRM), которая разграничивает права доступа к информации (обычно файлам) внутри компании и позволяет восстановить всю историю обращений к данным.

DLP

Задача DLP-системы (Data Leak Prevention) – контролировать информацию, покидающую пределы компании. Решения DLP анализируют почту, веб-трафик, программы обмена сообщениями, облачные хранилища, съемные носители и т. д. Есть два подхода к перехвату информации – мониторинг и уведомление ответственной службы компании или метод активной блокировки, когда информация, классифицированная как конфиденциальная, будет заблокирована в момент отправки, вывода на печать или записи на съемный USB-носитель.

Защищенный обмен данными

Для надежного и безопасного обмена данными мы предлагаем следующие решения:

- централизованный обмен файлами: данные находятся в безопасности на серверах компании или в облачном хранилище;
- системы защищенных коммуникаций: защита передаваемой информации (файлы, текстовые сообщения, голосовые и видеокommunikации) как на устройствах, так и в процессе передачи через интернет.

Мы расскажем, как грамотно сочетать оба. При этом вы получите удобную и полноценную систему управления, не требующую специальных технических знаний для управления системой, сбора отчетности и доказа-

Классификация информации

Существует определенный класс систем, которые позволяют автоматизировать процесс классификации информации и вовлечь в него бизнес-пользователей. Под разворачиваемые средства защиты информации попадут только те данные, которые необходимо защищать.

Центры реагирования ИБ (SOC)

SIEM

SIEM (Security information and event management) – это специализированная аналитическая система, предназначенная для управления событиями систем безопасности в организации. Решения этого класса просматривают данные от всех систем ИБ и по определенным критериям отслеживают отклонения от нормы. Если по данным анализа происходит отклонение, система создает инцидент, а затем помогает в его расследовании, предоставляя все необходимые данные.

SECaaS

Безопасность как услуга (Security as a Service) – это логичное и выгодное решение для компаний, которые уже вынесли в облако часть своей инфраструктуры и бизнес-систем.

Помимо того, что эти решения адаптированы к угрозам, специфическим для облачных окружений, они обладают такими преимуществами, как моментальные обновления, быстрое внедрение и, конечно, низкая стоимость за счет оплаты по подписке.

Security Intelligence

Security Intelligence нужно внедрять, если вашей компании необходимо глубокое понимание состояния всех систем ИБ. Решения этого класса помогут выстроить архитектуру для сбора всей информации о работе систем безопасности. Это данные SIEM, отчеты об аномальных ситуациях, реагирование и анализ инцидентов, управление журналами и настройками, устранение уязвимостей.



Соответствие требованиям и стандартам, защита конфиденциальной информации (ПДн, аттестация)

Многим нашим заказчикам необходимо доказывать соответствие своей деятельности нормам законодательства с точки зрения ИБ, в том числе с точки зрения защиты персональных данных. Особенно это касается организаций, которые работают в государственном и финансовом секторе, в здравоохранении.

Мы можем обеспечить подбор и внедрение сертифицированных инструментов ИБ, проведение необходимых мероприятий организационного характера, регламентацию бизнес-процессов, прохождение аттестаций и проверок регуляторов (Роскомнадзор, ФСБ России, ФСТЭК России).



Поддержка

Softline – клиентоориентированная компания. Мы готовы оказать вам помощь на любом этапе пользования нашими услугами, дать исчерпывающие консультации по корпоративной информационной безопасности.

Техническая поддержка и сопровождение систем ИБ

Мы можем обеспечить техническую поддержку выбранных вами решений в формате 24x7. В нашем штате – квалифицированные специалисты по информационной безопасности, которые имеют широкую экспертизу по работе с ведущими вендорами. Как правило, наши услуги обходятся дешевле, чем работа штатных специалистов. Кроме того, к нам можно обращаться за помощью в сложных ситуациях.



Система мониторинга и отчетности использования информационных ресурсов

Внедрение такой системы позволит контролировать процесс работы всей системы предприятия с акцентом на безопасность и непрерывность бизнеса в реальном времени. Мониторинг охватывает все аспекты ИБ: от простых отчетов о пользовании файлами до выявления мошеннических действий внутри компании и внешних угроз. Это позволит снизить риски утечки конфиденциальных сведений, а значит минимизирует возможность репутационных потерь и финансовых издержек.

Обучение специалистов заказчика

Курсы по информационной безопасности в Учебном центре Softline помогут вашим сотрудникам быть в курсе актуальных тенденций в этой сфере. Как работать так, чтобы соблюдались интересы бизнеса и требования закона, расскажут опытные преподаватели.

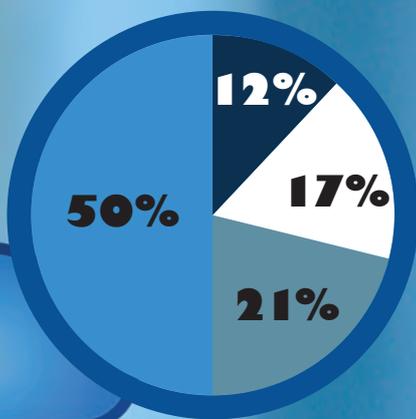
Масштабы облачных проектов растут: если три-четыре года назад это были относительно небольшие задачи, то теперь к нам идет большой поток обращений от крупных компаний с интересными запросами. Рынок значительно вырос, и за последние пять лет, можно сказать, изменился кардинально.

У вас есть выбор. Выбирайте для себя лучшее

Вы можете строить локальные защищенные контуры внутри организации, покупать софт, СХД, средства защиты, строить серверные — но ничто не мешает вам принять решение «идти в облака». Выбрать облако вместо того, чтобы без конца обновлять парк «железа» — значит знать, что с точки зрения информационной безопасности разницы в построении систем в облаке и локально нет.

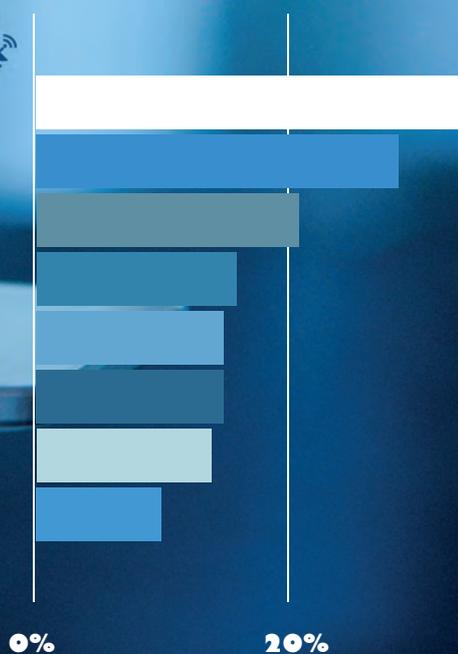
Что мешает распространению облаков в России

Облака как возможность расширения бизнеса



Облако как альтернативу традиционной инфраструктуре всерьез рассматривают и государственные учреждения. Еще в 2012 году Министерство Финансов Российской Федерации перевело ряд отраслевых информационных систем в облако. Это еще раз показывает, что облачный рынок созрел и облака интересуют всех.

Возражения заказчиков против работы с облаками



- 34%** Утрата конфиденциальных данных
- 29%** Зависимость от провайдера
- 21%** Нехватка навыков
- 16%** Несоответствие требованиям регуляторов
- 15%** Несоответствие потребностям компании
- 15%** Вопросы интеграции с инфраструктурой
- 14%** Качество поддержки провайдера
- 10%** Незрелость облачных технологий

Любое решение или требования по информационной безопасности могут быть выполнены в облаке.

По вине облачных провайдеров утечек практически нет. Практика зарубежных исследований доказывает, что в большинстве случаев утечка информации происходит внутри компании из-за сотрудников. В облаке и локальной инфраструктуре используются одни и те же средства защиты. Клиенты Softline

Облачные технологии априори безопасны. Особенно, если сравнивать их с хранением данных в локальной инфраструктуре. Почему многие компании хранят свое оборудование в сторонних ЦОДах? Потому что доверяют им.

всегда знают, на базе каких технологий создано облако, в том числе и с точки зрения безопасности. Все процессы прозрачны, ведется полное логирование всех действий сотрудников, SLA дает лучшую гарантию безопасности.

По закону и стандарту

То, что облако и законодательство в области хранения и обработки персональных данных «не дружат» — сегодня, пожалуй, самый неуместный миф. Ряд проектов уже выполнен и доказано на практике: любые требования закона можно выполнить в рамках частных облаков.

Технические меры защиты для развертывания безопасного облака

- Обеспечение безопасности каналов связи с применением средств криптографической защиты информации.
- Защита среды виртуализации от несанкционированного доступа на базе сертифицированных операционных систем или иных средств.
- Обеспечение защищенности ресурсов от внешних атак средствами межсетевое экранирования и обнаружения вторжений.
- Защита системы от вредоносного кода.
- Предоставление распределенной системы хранения данных и резервирования.
- Соответствие дата-центров стандарту не ниже Tier 3 в РФ.
- Гарантированный уровень доступности сервисов до 99,95% SLA.

Преимущества проектов, выполненных компанией Softline

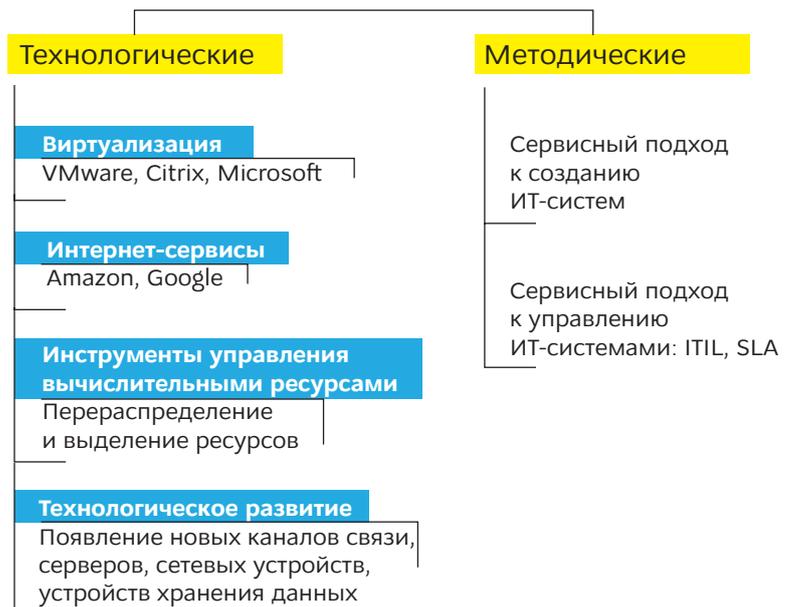
- Работы по защите информации проводятся компанией, имеющей лицензии ФСТЭК и ФСБ, сертификат PCIDSS и другие.
- Финансовая ответственность провайдера, фиксируемая в SLA.
- Круглосуточная техническая поддержка 24/7/365.
- Консалтинг и техническая поддержка в части выполнения требований законодательства и отраслевых стандартов по защите информации (актуализация документации, настроек СЗИ и др.).

Разместите в нашем защищенном облаке информационные системы, обрабатывающие персональные данные (ПДн): наши сервисы безопасности гарантируют обеспечение того уровня ИБ, который требует действующее законодательство РФ (ФЗ «О персональных данных» от 27 июля 2006 года № 152-ФЗ, приказы и требования ФСТЭК и ФСБ в части обеспечения безопасности ПДн) к информационным системам персональных данных (ИСПДн). Softline имеет сертификат на облачную инфраструктуру PCI DSS. Это подтверждено тщательным аудитом, проведенным международной консалтинговой компанией, и означает, что инфраструктура компании полностью соответствует европейским стандартам. Будучи одним из крупнейших системных интеграторов и предоставляя услуги дата-центров, Softline постоянно совершенствует механизмы обеспечения информационной безопасности их ИТ-инфраструктуры. Согласно заключению сертифицированного аудитора, Softline может размещать в облаке ИТ-сервисы организаций, которым необходим повышенный уровень конфиденциальности данных и обеспечения безопасности.

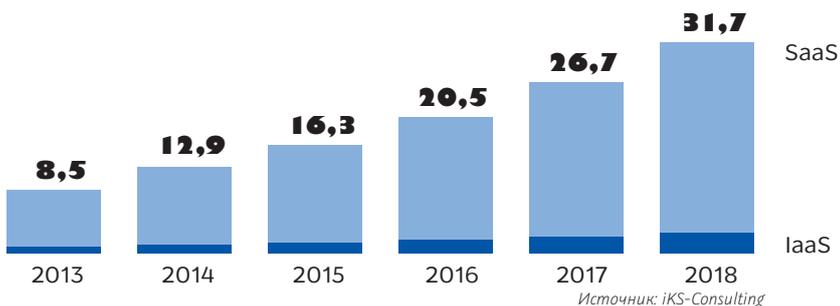
Cloud для всех!

Облачные технологии актуальны для компаний любых размеров и всех отраслей, от малого бизнеса до самого крупного. Так, специально для стартапов уже придуманы особые предложения, которые позволяют молодому бизнесу значительно экономить. Иногда никакая локальная инфраструктура не нужна компании вообще! Покупать лицензии и оборудование не нужно – все берется в аренду с ориентиром на количество пользователей – сразу же можно работать. А что по ценам? Зачастую организация любой локальной ИТ-инфраструктуры обходится в любом случае дороже облачной. Кроме того, при использовании облачных технологий деньги не выводятся из оборота, а значит, приносят дополнительную прибыль. Понять, в какую сумму обходится бизнесу то или иное ПО, позволяет категория «совокупная стоимость владения» (Total Cost of Ownership, TCO), которая учитывает стоимость серверов, их обслуживания и прочих работ персонала, затраты на развертывание системы, на обновление ПО, на электроэнергию и т.д. Если посчитать TCO для классической схемы и для облака, станет

Предпосылки для создания облачной инфраструктуры



Динамика рынка облачных услуг в России, млрд руб. (прогноз)



ясно, что реальная экономия за три года может составлять от 20 до 60%! Но все же бывают случаи, когда дешевле создать свою небольшую инфраструктуру нежели использовать облачную модель построения ИТ-инфраструктуры. Как правило это проекты, которые мало требовательны к отказоустойчивости и производительности ИТ-ресурсов.

История успеха

Не так давно один из заказчиков Softline выиграл тендер Министерства Здравоохранения Москвы – подряд на обслуживание 64 поликлиник, которое заключается в обработке и хранении МРТ- и КТГ-данных. Сейчас все снимки – а это колоссальная база изображений, которая постоянно пополняется и весит очень много – хранятся в облаке Softline. Инфраструктура состоит из серверной части, хранилища информации и софта. Softline предоставляет в данном случае серверную часть и хранение, софтом занимается другой провайдер, специализирующийся на медицинском ПО. Снимки представляют собой персональные данные, они хранятся зашифрованным виде, и в этой связи Softline совместно с компанией-клиентом запускает проект по соответствию требованиям ФЗ-152. Все то, что раньше делалось локально, а именно: защита платформ виртуализации, каналов связи, VPN, антивирусная защита в соответствии с ФСТЭК, – будет реализовано на базе нашего облака.

Грядущие перспективы

Специалисты Softline разрабатывают выделенный облачный сег-

мент, защищенный по стандарту безопасности уровня 3. Все клиенты, которые примут решение размещать данные в этом сегменте, будут получать защиту третьего уровня автоматически. Softline будет предоставлять защиту платформы виртуализации, каналов связи, антивирусную защиту и пакет документации. Сейчас заказчикам предоставляется этот же набор, но в рамках отдельных проектов. Облака отлично совмещаются с требованиями ФЗ-152, и за последний год количество клиентов, которые обращаются к нам с проектами такого рода, выросло вдвое. Многие из них уже интересовались, можем ли мы предложить готовое универсальное решение. Отвечаем: скоро оно будет разработано для вашего удобства, и мы приступим к реализации!

Облачные технологии нужны вашему бизнесу

И специалисты Softline могут реализовать их для вас! По желанию клиента мы организуем инфраструктуру не только в России, но и за рубежом, используя дата-центры в Европе, а также облачную платформу Windows Azure. У нас богатая экспертиза в области виртуализации и опытные сотрудники. Будьте с Softline и не бойтесь облаков!

Что нужно учесть при переезде в облако

Комплексно решить задачу создания (переноса) защищенных сервисов в облаке может только интегратор, имеющий опыт как в области применения облачных технологий, так и в области защиты информации. Такой интегратор должен обладать:

- ресурсами, позволяющими построить современную отказоустойчивую архитектуру облачного сервиса;
- штатом квалифицированных специалистов;
- лицензиями ФСБ России и ФСТЭК России, позволяющими проводить работы по обеспечению требуемого уровня безопасности информации;
- опытом взаимодействия с регулятором в рамках проведения проверок.

Одними из важнейших составляющих в подготовке к переносу сервисов в защищенные облака являются:

- аудит информационных систем заказчика с целью определения технических требований;
- анализ инфраструктуры для подготовки проекта переноса сервисов в облако и обеспечению информационной безопасности;
- разработка индивидуального решения по размещению инфраструктуры клиента в защищенном облаке;
- установка и настройка предложенного решения;
- поддержка (SLA-облако) и поддержка (сопровождение) в актуальном состоянии нормативной документации.

Стоимость выполнения этих мероприятий должна быть учтена при оценке стоимости реализации проекта и может составлять его существенную часть.

Хотите задать вопрос?

@ Sergey.Samoukin@softlinegroup.com

+7 (495) 232-00-23,
доб. 1065

Data Base Firewall

Доступы для СУБД

Большая часть информации компании содержится в ее базах данных. Как правило, именно данные из СУБД становятся целью атаки злоумышленников. Продукты класса DBF (DataBase Firewall) 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, 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 неэффективным.

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. Логируются 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 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 сканеры 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 лагуна 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 ACFEЕ, 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 отличие 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.

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 ИТ-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 исследований;
- оперативно оповещает об инцидентах.

Выгоды от внедрения антифрод решения для ритейл-бизнеса:

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

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АНТИФРОД-РЕШЕНИЙ.

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

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

КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ – ПОД НАДЕЖНЫЙ КОНТРОЛЬ!

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННОЙ DLP-СИСТЕМЫ ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ

Технологический прогресс и консьюмеризация корпоративных ИТ способствуют развитию целого класса новых угроз и рисков ИБ невиданных доселе опасности и масштабов. Эти угрозы стали результатом сближения ряда факторов, а именно:

- Легкодоступность и простота использования съемных накопителей и других подключаемых устройств хранения данных.
- Большинство сервисов социальных сетей, приложений облачных хранилищ и мессенджеров игнорируют корпоративные средства защиты и границы инфраструктуры. Модель их информационной безопасности основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь.
- Активно развивающаяся виртуализация корпоративных ресурсов и использования арендуемых корпоративных облачных сервисов.

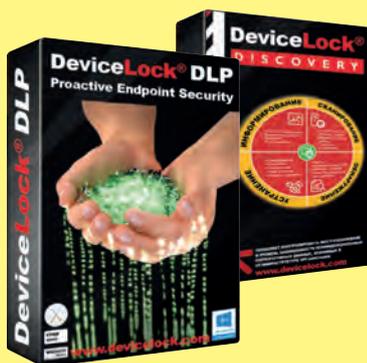
На рынке DLP-решений заслуженной популярностью пользуется программный комплекс российской разработки DeviceLock DLP 8, обеспечивающий избирательный контроль пользователей, предотвращение утечек и регистрацию фактов передачи данных через локальные порты и устройства, сетевые сервисы и протоколы, а также автоматическое сканирование компьютеров и корпоративных сетевых ресурсов в целях выявления нарушений политик безопасного хранения документов и

данных. DeviceLock DLP реализует перехват и инспекцию содержимого передаваемых данных в каналах утечки, принимая решение о возможности передачи данных или протоколировании этого события непосредственно на контролируемом компьютере, а не на уровне сервера или шлюза. Это обеспечивает эффективный контроль мобильных сотрудников, не использующих корпоративную сеть.

С помощью DeviceLock DLP реализуются разнообразные сценарии противодействия утечкам корпоративных данных – от тотального запрета использования отдельных каналов до пассивного режима наблюдения. Между этими крайностями лежат сочетания блокировки и протоколирования, включающие выборочное разрешение или блокировку передачи файлов по контролируемым службой ИБ каналам для отдельных пользователей и групп в сочетании с контентной фильтрацией. В арсенале продукта также теневое копирование только представляющих интерес для службы ИБ файлов, оповещения по ключевым инцидентам и др.

DeviceLock DLP позволяет обеспечить защиту от утечек данных для виртуальных сред и модели BYOD, основанной на виртуализации рабочих сред и приложений, а также гибком контроле терминальных сессий – буфера обмена и перенаправленных в терминальную сессию устройств и принтеров. Реализованная в DeviceLock технология Virtual DLP является универсальной.

Предоставляемая DeviceLock DLP возможность обеспечить избирательный контроль различных каналов утечки в сочетании с контролем хранимых на рабочих станциях конфиденциальных документов открывает организациям безопасный путь для разрешения своим сотрудникам контролируемо использовать различные устройства и сетевые сервисы в целях повышения эффективности работы без угрозы утечки данных вне зависимости от места работы сотрудников.



В целях обеспечения контроля хранимых данных используется DeviceLock Discovery, отдельно лицензируемый компонент комплекса, который обеспечивает автоматическое сканирование рабочих станций и сетевых хранилищ, обнаруживая на них документы и файлы, содержимое которых нарушает политику безопасного хранения корпоративных данных, после чего осуществляет с ними заданные опциональные превентивно-защитные действия.

DeviceLock®
Proactive Endpoint Security

ЕСТЬ ЛИ ЖИЗНЬ ПОСЛЕ DLP?

Рынок защиты данных от утечки зародился, когда службы безопасности были озабочены защитой конфиденциальной информации. Поэтому такой инструмент контроля данных, как DLP, нашел большое количество поклонников. Ведь так здорово определиться с перечнем защищаемых фрагментов информации и запретить их выход за пределы защищаемого контура.

Что стоит за утечками информации

Но прогресс не стоит на месте, и ИБ-специалисты стали замечать, что утечки являются только «симптомами» более серьезных нарушений. Сотрудник не просто так ворует данные у работодателя — работает ли он на конкурентов или же придумал схему мошенничества, признаки которой, как оказывается, можно проследить через анализ коммуникаций и действий сотрудника.

Отдельные «безопасники» выработали для себя лучшие практики по работе с DLP-системами, через которые им удавалось расследовать утечки и выявлять их реальные причины. Эта тенденция, по сути, связана с тем, что руководителей бизнеса не интересуют сами утечки данных, важна только прибыль и риски, связанные с ее снижением. А корпоративное мошенничество, признаками которого становятся утечки, серьезно бьет по карману бизнесменов.

И вот вызовы перед службой безопасности стоят самые актуальные, а инструментарий по борьбе с новыми угрозами в лице корпоративного мошенничества изрядно отстает.

Идет расследование

Традиционно DLP-системы фиксировали нарушения, связанные с выходом информации за периметр организации. Т.е. в фокусе внимания оказывались только инциденты, на которые срабатывала политика безопасности в данный момент. Другое дело, когда угрозой является злонамеренный инсайдер, давно ведущий незаконную деятельность на предприятии. И отдельные инциденты могут быть только сигналами к началу расследования. В этом случае большую ценность для офицера ИБ будут иметь события, которые произошли в прошлом.

Таким образом, на первый план выходят не технологии перехвата трафика, а функционал

создания долгосрочного архива коммуникаций, а также аналитические инструменты для работы с большими объемами данных.

В ходе проектирования 6-й версии Solar Dozor удалось четко понять, какой именно функционал требуется специалисту по безопасности чаще всего и какие элементы управления должны быть всегда под рукой.

Solar Dozor

Получить полную картину происшествия поможет современный веб-интерфейс Solar Dozor, разработанный в логике ситуационного центра, где в центре внимания находятся: а) события информационной безопасности, б) информационные объекты; в) персоны. Пользователь системы может взглянуть на одно и то же нарушение с трех разных точек зрения.

Проводя оперативный мониторинг, специалист по безопасности может быстро выявлять в потоке событий критичные в данный момент инциденты и назначать ответственного сотрудника для расследования нарушения. Тут же отображаются сообщения, передача которых была заблокирована системой, они всегда находятся на главном экране для обеспечения непрерывности бизнеса.

Взглянуть на инцидент глазами самого нарушителя в Solar Dozor помогает «Досье» на сотрудников и группы лиц, требующих особого контроля. Используя «Граф связей» можно быстро выявить сообщников подозреваемого. А быстрый поиск в течение считанных секунд выдает всю необходимую информацию, при этом работа с ним не требует специальной подготовки.

Solar Dozor дает специалисту все необходимые инструменты для выявления признаков экономических преступлений в организации и проведения полномасштабных расследований. И все это упаковано в современный интуитивно понятный и дружелюбный интерфейс, в котором каждое действие требует пары кликов для получения результата.



+7 (499) 755-07-70
solarsecurity.ru

Какие угрозы таит в себе незащищённое мобильное устройство?



Ненадёжный пароль

Банковские приложения, личные финансы

Личные данные, социальные сети, фотографии и документы

Корпоративные учётные данные открывают доступ к другим устройствам компании

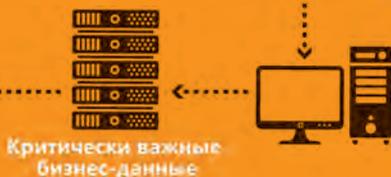
Корпоративные документы и сервисы

Рабочая почта и мессенджеры

Корпоративные приложения

Контакты коллег и партнеров

Файлы на смартфоне



Критически важные бизнес-данные

Корпоративные данные – это деньги вашей компании!

Вы заботитесь о стационарных ПК и ноутбуках в пределах организации? Это далеко не всё.

Мобильные устройства тоже требуют вашего внимания!

Да, они помогают обеспечить высокую продуктивность коллектива, но телефон или планшет сотрудника могут стать ключом к корпоративным данным компании для злоумышленника.

Работники чаще всего не делают разницы между корпоративными и личными данными. Они могут переписываться в корпоративной почте по личным вопросам или использовать сторонние сервисы для размещения важной информации.

Проблема

Создается угроза случайной утечки данных или намеренной атаки.

Что делать?

Разграничить личные и корпоративные данные. Ввести правила. Обязать коллег соблюдать их.

Решение проблемы

Enterprise Mobility Suite: корпоративные данные в безопасности

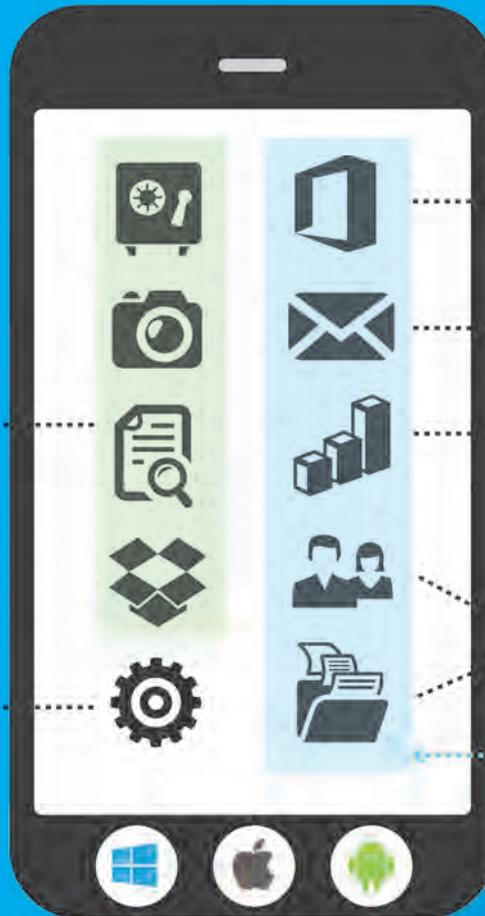


8Ni82*#

Надёжный пароль

- Управление списком приложений, доступных пользователю
- Запрет на передачу корпоративных данных через личные приложения
- Надёжный пароль обязателен для пользования устройством

Доставка приложений на устройства



Двухфакторная аутентификация для доступа к корпоративным сервисам

Защита корпоративной переписки

Сценарии single sign on для корпоративных сервисов

Шифрование данных и файлов

Защищённый контейнер для корпоративных данных

Используйте решение Microsoft Enterprise Mobility Suite!

Контролируйте корпоративные данные, даже если они используются совместно с другими лицами внутри организации и за ее пределами. Какие технологии используются?

AADP – обеспечивает единый вход в систему для облачных приложений, включает в себя функции многофакторной аутентификации, контроль доступа и отчёты по безопасности.

Intune – централизованное управление обновлениями и политиками безопасности, мониторинг и поддержка пользователей.

RMS – служба управления правами доступа к информации.

ATA – решение на основе машинного обучения, позволяющее обнаруживать подозрительную активность и атаки злоумышленников.

Что в итоге? Сотрудники всегда на связи и могут трудиться из любой точки мира, не теряя продуктивности. Вы спокойны за безопасность компании.

Где можно посмотреть и попробовать?

Андрей Изотов
Руководитель направления корпоративной мобильности

Andrey.Izotov@softlinegroup.com
+7 (495) 232 00 23 доб. 1347

VEEAM AVAILABILITY SUITE

РЕШЕНИЕ VEEAM AVAILABILITY SUITE РЕАЛИЗУЕТ ПРИНЦИПИАЛЬНО НОВУЮ КОНЦЕПЦИЮ ДОСТУПНОСТИ ДАННЫХ ДЛЯ НЕПРЕРЫВНОЙ РАБОТЫ БИЗНЕСА AVAILABILITY FOR THE ALWAYS-ON ENTERPRISE ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ИНВЕСТИЦИЙ В ВИРТУАЛИЗАЦИЮ СЕРВЕРОВ, СОВРЕМЕННЫЕ СИСТЕМЫ ХРАНЕНИЯ И ОБЛАЧНЫЕ ТЕХНОЛОГИИ.

Veeam Availability Suite глазами пользователей

Согласно недавнему аналитическому отчету компании ESG1 пользователи Veeam Availability Suite отмечают следующее:

- В 96% случаев восстановление данных с Veeam выполняется в пределах предусмотренного SLA допустимого времени восстановления (RTO). В то время как для других решений аналогичный показатель составляет не более 78%.
- 83% заказчиков Veeam более уверены в своих резервных копиях, чем это было во время использования других решений.
- 71% пользователей Veeam отмечают высокую надежность резервных копий по сравнению с работой других решений.
- 65% пользователей виртуальной лаборатории Veeam экономят время и избегают проблем при развертывании.
- 71% пользователей инструментов мониторинга и отчетности Veeam отмечают, что стали лучше разбираться в возможных рисках по сравнению с опытом использования других продуктов.

Доступность всех приложений и сервисов

Veeam Availability Suite объединяет преимущества Veeam Backup & Replication, — лидера в области резервного копирования, восстановления и репликации виртуальных сред, — с современными возможностями мониторинга, создания отчетов и планирования ресурсов Veeam ONE. Veeam Availability Suite обеспечивает постоянный доступ к данным в дата-центре и надежно защищает виртуальные среды VMware vSphere и Microsoft Hyper-V.

Организации модернизируют свои ЦОД для повышения скорости предоставления IT-сервисов и обеспечения высокого уровня контроля и безопасности, а также для снижения операционных издержек и повышения адаптируемости бизнеса. При строительстве современных ЦОД средства инвестируются в виртуализацию серверов, современные приложения для работы с системами хранения данных и облачные технологии. Но пользователям нужно больше — им требуется кру-



Высокая скорость восстановления. Быстрое восстановление нужных данных удобным вам способом.



Предотвращение потерь данных. Низкие показатели целевой точки восстановления (RPO) и оптимизированное послеаварийное восстановление.



Гарантия восстановления данных. Гарантированное восстановление каждого файла, приложения или виртуального сервера.



Эффективное использование резервных копий.

Снижение рисков при развертывании за счет предварительного тестирования обновлений в изолированной копии рабочей среды.



Комплексный контроль. Мониторинг в режиме реального времени и упреждающее оповещение о проблемах.

гласуточная доступность данных и приложений, отсутствие простоев и потерь информации.

Ограниченная доступность и концепция Always-On Enterprise

По мере роста требований к доступности данных компании приходят к мысли о внедрении концепции Always-On Enterprise. Но традиционные решения для бэкапов по-прежнему широко распространены, несмотря на их явные недостатки:

- показатели допустимого времени (RTO) и целевой точки (RPO) восстановления составляют несколько часов и даже дней;
- ежеквартально тестируется менее 6% резервных копий;
- более 16% резервных копий непригодны для восстановления;
- 59% обновлений приложений приводят к сбоям и перерывам в работе;
- ограничена возможность выявлять проблемы до того, как они помешают работе.

Таким образом, возникает проблема ограниченной доступности — несоответствие между требованиями концепции Always-On Enterprise и возможностями ИТ по обеспечению доступности данных. 82% ИТ-директоров утверждают, что существует заметный разрыв между тем уровнем доступности, который необходим пользователям, и тем, который компании в состоянии обеспечить.

Решение Veeam Availability Suite обеспечивает доступность данных и позволяет предоставлять гарантированный уровень обслуживания с показателями допустимого времени и целевой точки восстановления (RTPO) < 15 минут для всех приложений и данных.

Пять составляющих концепции Always-On Enterprise Veeam Availability Suite обеспечивают все пять важнейших составляющих концепции Always-On Enterprise.

Что нового в версии 9

Veeam Availability Suite v9 реализует концепцию Always-On Enterprise и предлагает новые возможности эффективного использования средств, вложенных в СХД и облако. Кроме того, новая версия содержит ряд новшеств.

Veeam Explorer для Storage Snapshots и резервное копирование с помощью аппаратных снимков EMC. Гибридные массивы EMC VNX, VNX2 и VNXe для сверхбыстрого бэкапа из аппаратных снимков позволяют быстро восстановить нужный объект приложения или ВМ целиком.

Veeam Cloud Connect и инфраструктура провайдера облачных услуг обеспечивают возможность быстрого и безопасного послеаварийного восстановления.

Veeam Explorer для Oracle. Базы данных Oracle легко восстанавливаются по состоянию на нужный момент времени и с точностью до транзакции. Бэкап журнала транзакций доступен без использования агентов.

Масштабируемый репозиторий Veeam — это виртуальный пул ресурсов хранения, который объединяет различные СХД и позволяет расширить хранилище бэкапов.

Veeam Explorer для Microsoft Exchange, Active Directory, SharePoint и SQL Server Discovery для Exchange. Восстановление объектов групповых политик и интегрированных записей DNS для Active Directory. Восстановление веб-сайтов и их коллекций для SharePoint. Восстановление данных на уровне таблиц для SQL Server.

Тестовая среда из аппаратных снимков. С помощью аппаратных снимков можно создавать изолированные копии рабочей среды для тестирования и диагностики неполадок.

Режим передачи данных при бэкапе Direct NFS Access. Direct NFS Access позволяет ускорить бэкап ВМ в среде VMware и снизить воздействие на рабочую среду. Данные можно копировать прямо с основной системы хранения, минуя хосты.

Kaspersky Security для бизнеса



Kaspersky Security для бизнеса — это единая платформа безопасности, с помощью которой администраторы могут централизованно контролировать и защищать корпоративную ИТ-инфраструктуру.



СТАРТОВЫЙ

Kaspersky Endpoint Security для бизнеса

Базовая защита рабочих станций



СТАНДАРТНЫЙ

Kaspersky Endpoint Security для бизнеса

Контроль и защита рабочих станций, мобильных устройств и файловых серверов



РАСШИРЕННЫЙ

Kaspersky Endpoint Security для бизнеса

Защита устройств сотрудников, дополненная инструментами системного администрирования



TOTAL

Kaspersky Endpoint Security для бизнеса

Комплексная безопасность ИТ-инфраструктуры на различных уровнях сети

Основные возможности

- **Защита рабочих станций.** Надежная и простая в управлении защита от вредоносного программного обеспечения.
- **Контроль программ, устройств и веб-ресурсов.** Контроль над программами, устройствами и доступом сотрудников к интернету для повышения безопасности и производительности.
- **Шифрование.** Безопасность файлов, дисков или устройств, даже если они попадут в чужие руки.
- **Защита мобильных устройств.** Безопасность личных и корпоративных мобильных устройств и управление ими.
- **Защита файловых серверов.** Надежная защита файловых серверов, снижающая риск распространения по сети вредоносных программ.
- **Управление мобильными устройствами.** Настройка безопасности личных и корпоративных мобильных устройств и создание политик их использования.
- **Системное администрирование.** Централизованная установка исправлений, систем и программ, управление программным и аппаратным обеспечением.
- **Защита электронной почты.** Защита электронной почты от вредоносных программ и фильтрация спама.
- **Защита интернет-шлюзов.** Защита интернет-шлюзов для обеспечения безопасной работы в интернете.
- **Защита серверов совместной работы.** Защита от вредоносных программ, контентная фильтра-

ция для серверов совместной работы Microsoft SharePoint.

- **Единая консоль управления.** Централизованное управление упрощает обеспечение безопасности и системное администрирование.

С ростом числа используемых устройств и программ ценные данные компании подвергаются все большему риску. Справиться с этим поможет Kaspersky Security для бизнеса — единая платформа для обеспечения безопасности корпоративных данных. Линейка продуктов, состоящая из нескольких уровней с нарастающим функционалом, а также ряд специализированных решений, обеспечит безопасность отдельных узлов сети. С помощью Kaspersky Security для бизнеса администраторы могут централизованно контролировать и защищать корпоративную ИТ-инфраструктуру.

Единая консоль управления. Администратор может наблюдать за состоянием защиты всех физических, виртуальных и мобильных устройств, а также управлять их безопасностью с помощью единой консоли администрирования.

Единая платформа. Все используемые в продуктах «Лаборатории Касперского» ключевые технологии, функциональные компоненты и модули разрабатываются внутри компании на собственной технологической базе. Благодаря этому растет эффективность, снижается нагрузка на систему и повышается стабильность работы приложений.

Единая лицензия. Kaspersky Security для бизнеса — это единое комплексное решение, которое можно гибко настраивать в соответствии поставленными с бизнес-целями.

Калейдоскоп решений «Лаборатории Касперского»

Kaspersky Anti-Virus

Kaspersky Anti-Virus — это решение для базовой защиты компьютера от основных видов интернет-угроз. В решение входят новейшие технологии защиты от основных вредоносных программ, в том числе от эксплоитов, использующих уязвимости в операционной системе и приложениях.

- Антивирусная защита от вредоносных программ.
- Проверка сайтов, файлов и сообщений.
- Высокая скорость работы.
- Анти-фишинг для защиты личных данных.



Kaspersky Internet Security для всех устройств

Kaspersky Internet Security для всех устройств — единое комплексное решение для защиты любых устройств на платформах Windows, Android и Mac OS со специальными инструментами защиты платежей, аккаунтов социальных сетей и конфиденциальных данных.

- Простой способ защитить все устройства.
- Блокирование любых интернет-угроз.
- Безопасные онлайн-платежи.
- Защита общения в интернете и SMS.
- Родительский контроль.



Kaspersky Small Office Security

Kaspersky Small Office Security — решение, разработанное специально для небольших компаний. Продукт сочетает инструменты, предназначенные для защиты от вредоносного ПО, со специальными технологиями, обеспечивающими надежную защиту серверов, компьютеров и ноутбуков на базе Windows и Mac OS, а также мобильных устройств на платформе Android.

- Защита компьютеров Windows и Mac, файловых серверов Windows и мобильных устройств Android.
- Защита финансовых операций в интернете.
- Контроль использования интернета сотрудниками и ограничение доступа к социальным сетям.
- Шифрование для защиты конфиденциальных данных.
- Технологии анти-фишинга.
- Фильтрация спама.
- Автоматическое резервное копирование файлов в Dropbox.

Kaspersky Safe Kids

Kaspersky Safe Kids — мультиплатформенное решение «Лаборатории Касперского» для защиты детей.

- Защита ребенка от нежелательной информации.
- Контроль времени использования устройств.
- Ограничение времени на игры и социальные сети.
- Подробные отчеты о действиях ребенка в интернете.
- Отслеживать посты с упоминанием ребенка и изменений списка друзей в Facebook и ВКонтакте.
- Получение информации о местоположении ребенка и его выходе из разрешенного периметра.
- Контроль скачивания приложений.
- Получение статистики звонков и смс (функция доступна только для Android-устройств).



IBM QRadar Security Intelligence Platform

Система аналитики информационной безопасности

Серьезные компании предпринимают целый комплекс мер, чтобы обезопасить свои данные. Работают антивирусы и межсетевые экраны, системы предотвращения утечек информации и обнаружения вторжений, контролируются APM пользователей, маршрутизаторы и серверы. Но злоумышленники уже давно не атакуют «в лоб». В условиях, когда ИТ-инфраструктура разветвлена и объем информации огромен, нужен своевременный анализ всех инцидентов, происходящих в системе.

Конечно, вручную просмотреть отчеты со всех систем ИБ невозможно, а глобальную угрозу с отложенным воздействием может представлять внешне безобидное событие. Выход есть: углубиться в источники информации, довериться сбор и анализ информации специализированной системе. Она поможет не только накопить объединенную статистику с систем ИБ, но и постоянно анализировать ее в комплексе, создавая новые правила и выводы, которые защитят данные компании в будущем. А также выдаст понятную отчетность и создаст доказательную базу по инцидентам.

IBM QRadar: комплексный подход к защите информационной инфраструктуры

Комплексный подход

Платформа QRadar Security Intelligence – это специализированная система сбора и аналитики событий информационной безопасности, которая дает готовое, простое в использова-

нии и отличающееся низкой стоимостью владения решение серьезных и больших задач по ИБ. QRadar Security Intelligence Platform предоставляет единую архитектуру для интеграции информации о безопасности и управления событиями (SIEM), управления журналами, определения аномальных ситуаций, анализа инцидентов, реагирования на инциденты, управления настройками и устранением уязвимостей. Продукт использует передовой механизм Sense Analytics Engine для обнаружения новейших угроз. Используя разные редакции и дополнения QRadar, можно решать различные, в том числе узконаправленные задачи. QRadar SIEM помогает отличать реальные угрозы, требующие дополнительного расследования, от ложных срабатываний по



результатам миллиардов анализируемых порций данных.

Преимущества и возможности

- Прозрачная ИТ-инфраструктура, обнаружение угроз в реальном времени.
- Приоритизация подозрительных событий.
- Создание подробных отчетов по доступу к данным и действиям пользователей.
- Возможность использования как в локальной, так и в облачной среде.
- Управление соответствием стандартам.
- Возможность для поставщиков управляемых услуг предоставлять решения для аналитики в области безопасности при низких затратах.

QRadar Incident Forensics помогает получать неоспоримые доказательства в ходе расследования инцидентов. Пакеты перехватываются целиком, а программа сама выводит проиндексированные данные в понятном визуализированном формате.

Преимущества и возможности

- С помощью Incident Forensics время расследования нарушений значительно сокращается: во многих случаях вместо нескольких дней требуется всего несколько часов или минут.
- Восстановление последовательности действий киберпреступников для получения полного представления о масштабе вторжения и предотвращения его в будущем.
- Преобразование данных, связанных с инцидентом безопасности, в исходный формат для лучшего понимания ситуации.
- Интеграция с IBM QRadar Security Intelligence Platform и совместимость с средствами перехвата пакетов сторонних производителей.

QRadar QFlow Collector выявляет аномальные ситуации с помощью углубленной проверки пакетов, анализируя поток данных до 7-го уровня OSI.

Преимущества и возможности

- Распознавание и выявление новых угроз безопасности без использования сигнатур уязвимостей.
- Управление соответствиями политикам и нормативным документам, контроль их соблюдения.
- Возможность отслеживания и анализа действий в социальных сетях и

мультимедийных приложениях для выявления потенциальных сетевых угроз.

- Расширенные средства анализа инцидентов.
- Непрерывное профилирование ресурсов с возможностью отправки уведомлений в случае изменений.

QRadar Risk Manager проводит мониторинг систем, симулирует и визуализирует угрозы. Превентивное решение снижает риски и обеспечивает соответствие нормативным требованиям регуляторов.

Преимущества и возможности

- Предоставление средств визуализации топологии сети и соединений для изучения текущих и возможных шаблонов сетевого трафика.
- Сопоставление уязвимости ресурсов с данными о конфигурации и трафике для выявления имеющихся возможностей для атаки и ресурсов с высокой степенью риска.
- Имитация сетевых угроз, включая возможное распространение атаки.
- Отслеживает сетевой трафик, чтобы улучшить соблюдение требований политик.

QRadar Vulnerability Manager выявляет уязвимости в сети и определяет те, которые нужно исправить в первую очередь в зависимости от их влияния на критичные объекты.

Преимущества и возможности

- Возможность распознавать более 70 000 известных опасных настроек, ошибок в конфигурации, недочетов программных продуктов.
- Формирование сводной картины уязвимостей всех продуктов и технологий, в которых уязвимости встречаются чаще всего.
- Использование передового решения IBM Sense Analytics для добавления контекста, распознавания уязвимостей и определения приоритетности действий по устранению последствий.
- Интеграция с IBM QRadar Security Intelligence Platform для обеспечения быстрой установки, сокращения времени ввода в эксплуатацию и снижения затрат на внедрение.
- Интеллектуальное, настраиваемое сканирование по расписанию и при наступлении определенных событий
- Обнаружение и профилирование ресурсов для формирования полной картины всей корпоративной сети.

Возможности IBM QRadar в области безопасности

- Защита от внешних и внутренних угроз, предотвращение атак и финансовых потерь
- Сокращение времени реагирования на угрозы всех типов, оповещение и контроль
- Расследование и восстановление работоспособности систем, приоритизация угроз
- Выполнение требований регуляторов, сбор данных, подготовка отчетов для аудита

При необходимости платформа QRadar Security Intelligence может быть дополнена расширениями других разработчиков, которые обеспечивают расширенную визуализацию, тесную интеграцию, совместную борьбу с угрозами и предоставляют технологии реагирования на инциденты. Они доступны в IBM Security App Exchange.



Остались вопросы?

За информацией о моделях лицензирования, вариантах приобретения и внедрения обращайтесь к специалистам компании Softline.

Илья Белов:

+7 (495) 232 00 23 доб. 1804
IL.Bel@softlinegroup.com

Евгения Медведева:

+7 (495) 232 00 23 доб. 1497
evgeniya.medvedeva@softlinegroup.com



ИТ-ИНФРАСТРУКТУРА «ГОРНОГО» ПОД ЗАЩИТОЙ!

О ПРОЕКТЕ

Заказчик:

Санкт-Петербургский
Горный Университет

Отрасль:

Образование

Ситуация:

Для модернизации информационной сети учебного заведения нужно было современное решение, защищающее от интернет-угроз, кибер-атак и утечки данных

Решение:

Специалисты Softline предложили заказчику выбрать Kaspersky Endpoint Security для бизнеса. Это решение обеспечивает полноценную защиту ИТ-инфраструктуры любого масштаба

Результаты:

Университет получил комплексное средство для защиты всех узлов имеющейся информационной системы



О заказчике

Национальный минерально-сырьевой университет «Горный» является одним из ведущих научно-образовательных центров в России. ВУЗ готовит специалистов для всех отраслей металлургической и газовой промышленности, геологической службы, гражданского строительства. В нем обучаются более 16,5 тыс. студентов, преподавательский состав насчитывает более 120 докторов наук, 400 кандидатов наук, 30 академиков.



СИТУАЦИЯ

В рамках модернизации системы защиты информационной сети учебного заведения перед ИТ-специалистами была поставлена задача по внедрению решения, защищающего от интернет-угроз, кибер-атак и утечки данных. При этом важно было обеспечить свобод-

ный обмен данными как по внутренней сети, так и при осуществлении внешних коммуникаций. На конкурсной основе в качестве поставщика была выбрана компания Softline, обладающая высшим партнерским статусом Enterprise Partner «Лаборатории Касперского».

РЕШЕНИЕ

Для решения задач, поставленных заказчиком, специалистами Softline было предложено использовать Kaspersky Endpoint Security для бизнеса. Продукт «Лаборатории Касперского» обеспечивает целостную защиту ИТ-инфраструктуры любого масштаба от вирусных угроз, шпионских программ, спама, модуль защиты от утечек предотвращает передачу конфиденциальной информа-

ции через электронную почту и серверы совместной работы, кроме того, продукт исключает вероятность несанкционированного доступа на всех уровнях корпоративной сети. Kaspersky Endpoint Security для бизнеса также включает в себя компоненты для повышения уровня защиты рабочих станций и мобильных устройств, доступа пользователей к интернет-ресурсам.

РЕЗУЛЬТАТЫ

В результате университет получил комплексное средство для защиты всех узлов имеющейся информационной системы. Решение Kaspersky Endpoint Security для бизнеса предоставило

ИТ-специалистам инструменты для централизованного администрирования и обеспечило доступ к детальной информации об уровне безопасности корпоративной сети.

«Построение надежной и безопасной ИТ-инфраструктуры имеет для нашего вуза большое значение, так как интернет-угрозы могут приводить к сбоям в сети, что осложняет доступ преподавателей и студентов к ИТ-сервисам. Именно поэтому мы сделали выбор в пользу программного продукта «Лаборатории Касперского» и уже успели убедиться в удобстве и надежности данного решения».

Евгений Карасев,
начальник центра новых информационных технологий
и средств обучения Горного университета.



ВРАЧИ НА СТРАЖЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ВМЕСТЕ С SOFTLINE

О ПРОЕКТЕ

Заказчик:

Группа компаний «Медицина человеку»

Отрасль:

Здравоохранение

Ситуация:

Компании необходимо было обновить ИТ-системы для того, чтобы они соответствовали требованиям законодательства в области защиты персональных данных

Решение:

Разработан комплекс организационно-технических мер по внедрению легко администрируемого, масштабируемого решения. Проведено обучение персонала заказчика

Результаты:

Процессы обработки сведений о пациентах и распределение обязанностей между персоналом регламентированы, случайная или умышленная утечка персональных данных предотвращены

РЕШЕНИЕ

Для того, чтобы повысить уровень защищенности информационных ресурсов организации, специалистами Softline было проведено обследование существующих ИТ-решений и подготовлена организационно-распорядительная документация, полностью описывающая систему защиты персональных данных, схему ее внедрения и перечень предлагаемых средств. Полученные заказ-

чиком рекомендации по повышению уровня сохранности информации были разработаны с учетом требований действующего законодательства, возможных угроз безопасности, бизнес-процессов компании и включали приказы, положения и инструкции по организации процесса защиты персональных данных.

РЕЗУЛЬТАТЫ

Разработанный Softline комплекс организационно-технических мер по внедрению легко администрируемого, масштабируемого решения полностью соответствует необходимым требова-

ниям и нормам в области обеспечения информационной безопасности и предотвращает несанкционированный доступ к персональным данным пациентов компании.

«Описанные в разработанной специалистами Softline документации программные и технические средства оптимально подойдут к существующей ИТ-инфраструктуре. Также для наших сотрудников было проведено обучение с предоставлением сведений о средствах защиты информации, особенностях их функционирования, обязанностях администраторов системы».

Александр Богомяков,
ИТ-специалист компании «Медицина человеку»

«Готовность специалистов заказчика к взаимодействию на всех этапах позволили максимально быстро разработать необходимые решения. Подготовленные рекомендации включают в себя регламентированный процесс обработки сведений о пациентах и распределение обязанностей между персоналом, что позволяет предотвратить случайную или умышленную утечку сведений».

Денис Поршин,
менеджер по продаже решений департамента развития бизнеса в регионах РФ компании Softline



О заказчике

Компания «Медицина человеку» занимается разработкой и продвижением новых технологий в лечении и реабилитации больных с травмами и заболеваниями опорно-двигательного аппарата. Организация сотрудничает с муниципальными и федеральными учреждениями Новосибирска в области внедрения современных имплантатов и операционных методик, является представителем международной ассоциации по изучению переломов (AO/ASIF).





МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НИЖЕГОРОДСКОГО ВОДОКАНАЛА

О ПРОЕКТЕ

Заказчик:

ОАО «Нижегородский водоканал»

Отрасль:

Государственная, ЖКХ



Ситуация:

Предприятию необходимо соблюдать ФЗ № 152 «О персональных данных». Была необходима доработка нормативно-методической документации

Решение:

Создать решение, соответствующее требованиям нормативных документов в области обеспечения ИБ и исключающее несанкционированный доступ к персональным данным потребителей услуг

Результаты:

Процессы обработки персональных данных предприятия соответствуют актуальным требованиям законодательства Российской Федерации



«Основной задачей проекта было внедрение средств защиты персональных данных, так как большая часть организационно-распорядительной документации у нас уже была разработана, но изменения в законодательстве и указы регуляторов в области ПДн диктовали новые правила. В рамках проекта мы получили рабочую систему защиты данных абонентов. В результате мы повысили качество управления информационной безопасностью в части защиты персональных данных. Программные и технические средства защиты, установленные и настроенные специалистами Softline, оптимально подходят к существующей ИТ-инфраструктуре предприятия».

Михаил Фомин, директор по информационным технологиям ОАО «Нижегородский водоканал»

СИТУАЦИЯ

В соответствии с действующим законодательством все организации, обрабатывающие персональные данные, обязаны обеспечить их безопасность. Перед руководством Нижегородского водоканала стояла задача модернизации системы защиты информации в соответствии с требованиями ФЗ № 152 «О персональных данных» и доработки нормативно-методической документации.

РЕШЕНИЕ

На начальном этапе проекта при участии сотрудников Нижегородского водоканала специалистами Softline был проведен аудит текущего состояния информационных систем, задействованных в обработке ПДн; актуализированы модели угроз безопасности при автоматизированной обработке данных; разработана концепция защиты ПДн. В ходе дальнейших работ после проведения стендовых испытаний было осуществлено внедрение необходимых средств защиты информации (инструменты защиты от

РЕЗУЛЬТАТЫ

Создано легко администрируемое, масштабируемое аппаратно-техническое решение, которое соответствует требованиям нормативных документов в области обеспечения информационной безопасности. По итогам проведенных

Победителем конкурса на выполнение работ по проекту стала компания Softline, обладающая большим опытом в реализации подобных задач, имеющая в штате сертифицированных специалистов в области ИБ и необходимые лицензии на выполнение работ по проектированию и внедрению системы защиты персональных данных.

несанкционированного доступа двухфакторной аутентификации с использованием личных электронных ключей и системы однократного входа, а также антивирусное ПО, средства криптографической защиты) для приведения ИС заказчика в соответствие требованиям законодательства Российской Федерации в области защиты ПДн. При построении системы были использованы решения таких разработчиков как «Код безопасности», «Лаборатория Касперского» и др.

работ для сотрудников Нижегородского водоканала было проведено обучение с предоставлением информации о СЗИ, особенностях ее функционирования, внесенных изменениях и работе с системой защиты персональных данных.

SOFTLINE ПРОВЕЛА АТТЕСТАЦИЮ ПРОИЗВОДИТЕЛЯ ЗАЩИЩЕННОЙ ПОЛИГРАФИЧЕСКОЙ ПРОДУКЦИИ

О ПРОЕКТЕ

Заказчик:

ЗАО «СИБПРО»

Отрасль:

Производство, полиграфия



Ситуация:

Компании было необходимо провести оценку соответствия программно-аппаратных комплексов требованиям ФСТЭК РФ.

Решение:

Провести аттестационные мероприятия, проверить защиту предприятия от несанкционированного доступа при помощи тестирующих средств, сертифицированных ФСТЭК

Результаты:

Аттестация пройдена успешно

СИТУАЦИЯ

ЗАО «СИБПРО» занимается изготовлением защищенной от подделок полиграфической продукции для субъектов РФ и стран СНГ. К предприятиям такого профиля предъявляются повышенные требования государственных регуляторов. ЗАО «СИБПРО» было необходимо провести оценку соответствия

программно-аппаратных комплексов требованиям ФСТЭК РФ. Реализацией проекта занялась компания Softline, обладающая подтвержденными полномочиями на проведение аттестации объектов информатизации и большим опытом в сфере обеспечения ИТ-безопасности.

РЕШЕНИЕ

Специалистами компании был произведен сбор необходимых данных о составе аттестуемых средств объекта информатизации, включающего в себя программно-аппаратные комплексы, после чего были разработаны программа и методика испытаний.

Аттестационные мероприятия включали в себя экспертно-документальный метод и проверку комплекса функций защиты информации от несанкционированного доступа при помощи тестирующих средств,

сертифицированных ФСТЭК. В ходе проведения технических и программных средств организации были изучены процессы хранения и обработки защищаемых сведений, произведен анализ информационных потоков и вероятных каналов утечки данных, методы распределения ответственности за выполнение требований в части их защиты и уровень подготовки кадров. Помимо этого, был проведен ряд испытаний подсистем управления доступом, регистрации и учета.

РЕЗУЛЬТАТЫ

Аттестация объектов информатизации является неотъемлемой частью работ по обеспечению ИТ-безопасности. Она позволяет в реальных условиях эксплуатации оценить соответствие применяемого комплекса мер по обеспечению защиты информации требуемому уровню. Высокая степень подготовки сотрудников ЗАО «СИБПРО» в области ИБ, отсутствие несоответ-

ствий требованиям и каких-либо замечаний значительно ускорило прохождение аттестации.

По результатам мероприятий заказчику был передан комплект аттестационной документации, аттестат соответствия системы требованиям ИТ-безопасности, который подтвердил эффективность имеющейся у «СИБПРО» системы защиты данных.



«Успешное прохождение аттестации является важным этапом в деятельности нашей организации, так как соответствие всем требованиям в сфере информационной безопасности и лицензионным требованиям на изготовление защищенной полиграфической продукции позволит привлечь новых заказчиков в государственном и коммерческом секторах рынка. Специалисты Softline тщательно провели необходимые исследования и в короткие сроки предоставили полный пакет документов».

Сергей Мезенцев,
начальник отдела информационных технологий ЗАО «СИБПРО»

Стратегия защиты

Как нельзя сделать качественный ремонт в квартире без хорошего дизайн-проекта, так и невозможно построить эффективную систему информационной безопасности в компании, не имея четкого плана действий, согласованного с планом развития компании. Стратегия информационной безопасности — это именно тот документ, в котором обозначены основные планы по реализации защиты бизнес-процессов компании.

Автор: Виктория Иванова, консультант аналитического отдела Департамента сервисных услуг и технической поддержки Softline

Во многих компаниях процессы обеспечения информационной безопасности рассматриваются в рамках функций ИТ-подразделений и планируются при разработке ИТ стратегии. Однако процессы обеспечения информационной безопасности являются важной частью деятельности по поддержке бизнеса. В связи с этим многие компании нуждаются в разработке отдельных от ИТ стратегий информационной безопасности, в рамках которых обеспечивается поддержка бизнес-целей компании. При разработке ИБ-стратегии, как правило, используется поэтапный подход. Разбиение деятельности на ряд стадий со строго очерченными задачами поможет не упустить из виду множество скрытых деталей, что в конечном счете позволит создать ИБ-стратегию, соответствующую и способствующую решению бизнес-задач конкретной компании. Процесс разработки ИБ-стратегии включает:

- анализ целей и стратегии развития бизнеса и ИТ;
- аудит текущей ситуации ИБ в компании;
- анализ требований законодательства и стандартов, действующих в отношении компании, в сфере информационной безопасности;
- анализ требований заинтересованных лиц, как в компании, так и вне ее (клиенты, партнеры, поставщики и др.);
- определение основных стратегических целей ИБ;

- определение задач, решение которых необходимо для реализации поставленных целей;
- определение критериев достижения стратегических целей и задач ИБ;
- управление стоимостью проектов.

Анализ целей и стратегии развития бизнеса и ИТ

Информационная безопасность, если рассматривать ее применительно к производственным процессам компании, носит исключительно сервисный характер и предназначена для сопровождения основных бизнес и ИТ-процессов, поэтому одним из ключевых факторов успеха разработки ИБ-стратегии являются наличие формализованных бизнес и ИТ стратегий в компании. Отсутствие требований бизнеса и ИТ не значит, что стратегию ИБ разработать невозможно, но стоит понимать, что подготовка документа потребует более глубокой проработки и, как следствие, займет больше времени.

Аудит текущей ситуации ИБ в компании

На самом базовом уровне целью ИБ-стратегии является предоставление правильных, нужных технологий и прикладных систем в правильном месте, поэтому на первом этапе проводится интервьюирование сотрудников ИТ- и ИБ-подразделений. Также должны быть проанализированы требования представителей биз-

нес-подразделений, которые являются определяющими, так как цель ИТ и ИБ – это поддержание бизнеса и способствование достижению именно бизнес-целей. Результатом аудита является формирование общего представления об ИТ-инфраструктуре компании, применяемых мерах информационной безопасности и требованиях, предъявляемых к ИТ-инфраструктуре и системе защиты информации.

Кроме того, при разработке ИБ-стратегии важно четко определить желаемое состояние, в которое придут внутриорганизационные процессы после реализации поставленных задач. Лучший способ определить ожидаемые результаты по итогам выполнения стратегии – это фиксировать требования и работать в непосредственном контакте с высшим управляющим звеном.

Анализ требований законодательства, стандартов и заинтересованных лиц

Влияние регулирующих норм и стандартов зачастую является основным двигателем при разработке ИБ-стратегии. Изучение полного списка требований законодательства, стандартов и заинтересованных лиц является ключевым звеном разработки документа. Кроме того, часто без внимания остается вопрос: до какой степени компания считает необходимым соответствовать требованиям. Множество компаний вкладывают значительные денежные и челове-

ские ресурсы, чтобы соответствовать тем или иным регулирующим нормам и стандартам, не соотнося при этом размеры вложений и возможных последствий. Такой подход может привести к высоким издержкам. В связи с этим, необходимо предварительно оценить последствия, которые ожидают компанию, если она не будет соответствовать или частично следовать требованиям.

Определение основных стратегических целей ИБ

Определение целей ИБ-стратегии основывается на представлении желаемого и потенциально достижимого будущего состояния информационной безопасности в компании.

Помимо влияния бизнеса и ИТ при определении целей ИБ-стратегии следует учитывать специфику внешней среды, наличие внутренних возможностей, амбиции и квалификацию руководителей бизнеса, ИТ и ИБ.

Итоговый набор целей ИБ-стратегии должен удовлетворять следующим требованиям:

- должна быть четкая логическая связь между целями ИБ, ИТ и бизнес-целями, на достижение которых они направлены;
- должны быть четко определены цели. Например, можно использовать критерии методологии SMART, в соответствии с которой цели должны быть конкретными, измеримыми, значимыми, достижимыми и соотноситься с определенным сроком.

Определение задач ИБ-стратегии

Для достижения поставленных целей ИБ-стратегии необходимо сформулировать стратегические задачи. Под стратегическими задачами следует понимать перечень проектов, их цели, задачи, результаты и основные этапы.

Для оценки эффективности реализуемых в рамках ИБ-стратегии задач рекомендуется использовать метрики значимости.

В дополнение к метрикам значимости рекомендуется описать целевое состояние системы защиты

Правильно составленная ИБ-стратегия обеспечит эффективное использование ресурсов для реализации мероприятий по информационной безопасности.

информации. В этом случае стратегический план – это план перехода от существующей системы защиты к целевой.

Метрики значимости задачи позволят сформировать перечень первоочередных и второстепенных проектов.

В итоге, определив цели и задачи стратегии информационной безопасности, перечень первоочередных и второстепенных проектов, компания имеет формальный документ, задающий вектор достижения целевого состояния системы информационной безопасности, достойный называться «ИБ-стратегией».

Управление стоимостью проектов

В рамках финального этапа разработки ИБ-стратегии необходимо использовать средства, методы и инструменты, обеспечивающие управление стоимостью проектов на разных стадиях их реализации.

Управление стоимостью должно обеспечиваться посредством реализации в ходе каждого проекта следующих процессов:

- оценка стоимости;
- формирование бюджета проекта;
- контроль стоимости проекта.

Формирование процессов управления стоимостью проекта должно обеспечивать:

- понимание прогнозируемой стоимости отдельных работ, пакетов работ и всего проекта (процесс оценки стоимости);
- четкое понимание сроков, стоимости и распределения денежных средств на проекте (процесс формирования бюджета);
- отсутствие в проекте непредвиденных расходов, минимизацию количества изменений и отклонений фактического бюджета от утвержденного базового бюджета (процесс контроля стоимости).

При этом, указанные процессы, как и любые процессы в ходе выполнения проекта, могут быть итеративными и выполняться на принципах последовательной разработки.

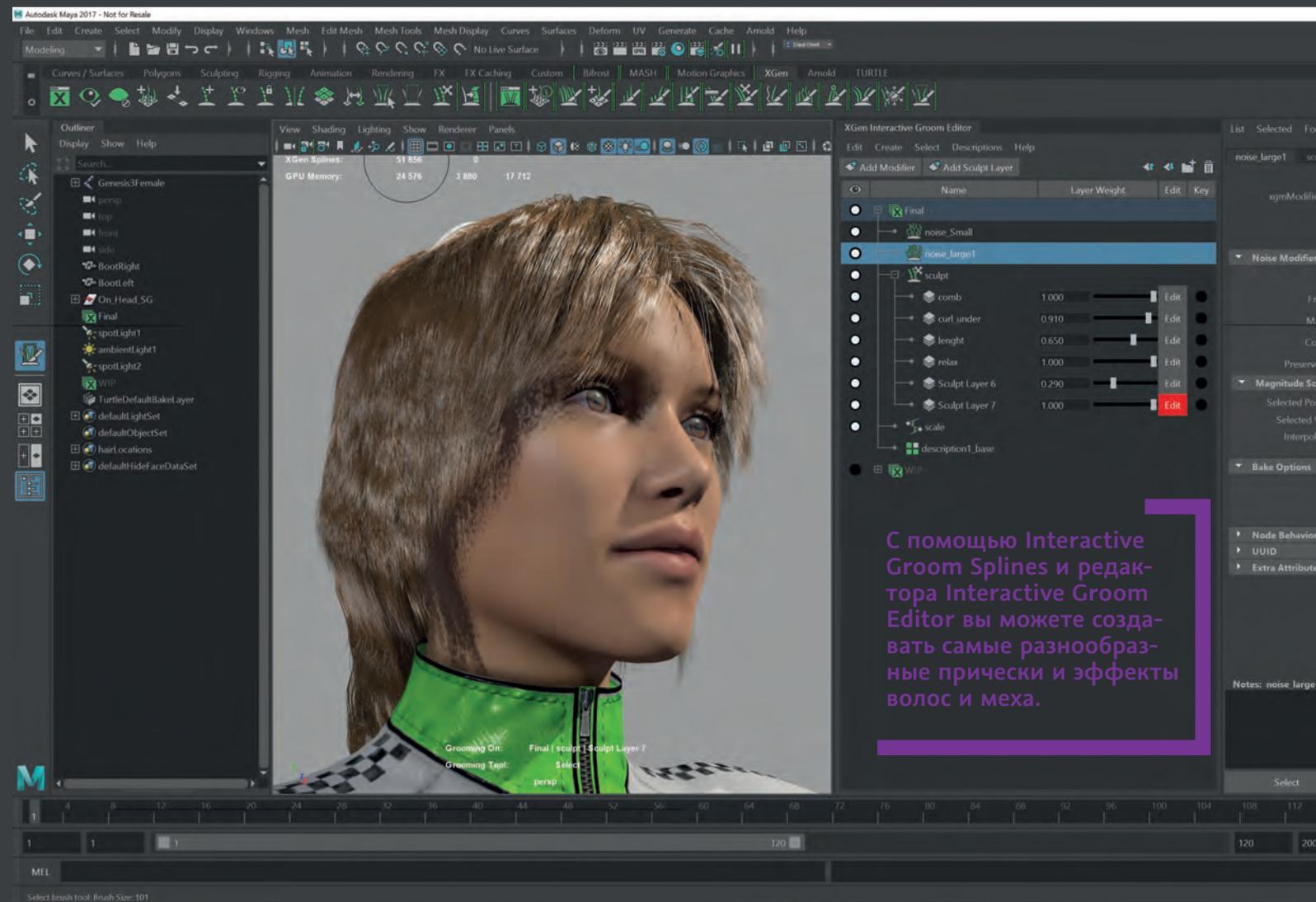
Заключение

Процессы обеспечения информационной безопасности в компании могут рассматриваться с негативных позиций ее руководством и сотрудниками, и не принесут ощутимой выгоды, если не будет разработан четкий алгоритм их внедрения и поддержания. Таким образом, разработка ИБ-стратегии является ключевым элементом повышения уровня зрелости процессов ИБ в компании.

Так как целью обеспечения безопасности информации является поддержка бизнеса и ИТ, документ должен разрабатываться с учетом интересов всех ключевых бизнес- и ИТ-подразделений.

Насколько успешна принятая в организации ИБ-стратегия, можно понять из того, насколько эффективно бизнес и ИТ использует ее в своей повседневной деятельности. Если процессы информационной безопасности полностью интегрированы в процессы принятия всех ключевых решений в компании, значит, стратегия «попала в точку». Если же бизнес негативно относится к использованию инструментов информационной безопасности, такая ИБ-стратегия нуждается в существенной переработке.

Компания Softline предоставляет услуги по разработке стратегий информационной безопасности. Наши специалисты имеют опыт разработки ИБ-стратегий для организаций различных сфер деятельности: медицинских, государственных, финансовых, транспортных и других. Подход к каждой организации – индивидуальный, этого важного принципа компания Softline придерживается в рамках любого проекта.



С помощью Interactive Groom Splines и редактора Interactive Groom Editor вы можете создавать самые разнообразные прически и эффекты волос и меха.

Autodesk Maya 2017

Перемены за год

Новое лицо,
НОВЫЕ
ВОЗМОЖНОСТИ
для воплощения
смелых идей

Разработчики подразделения Media&Entertainment компании Autodesk выпустили новую версию своего ведущего решения для анимации и эффектов — Maya. Значимым релизом была Autodesk Maya 2016 с пакетами Extension 1 и Extension 2. В каждом из пакетов расширений были предоставлены новые функции, инструменты и решения, вошедшие в новейший релиз — Autodesk Maya 2017. О многих новых функциях и инструментах мы писали в предыдущих номерах.

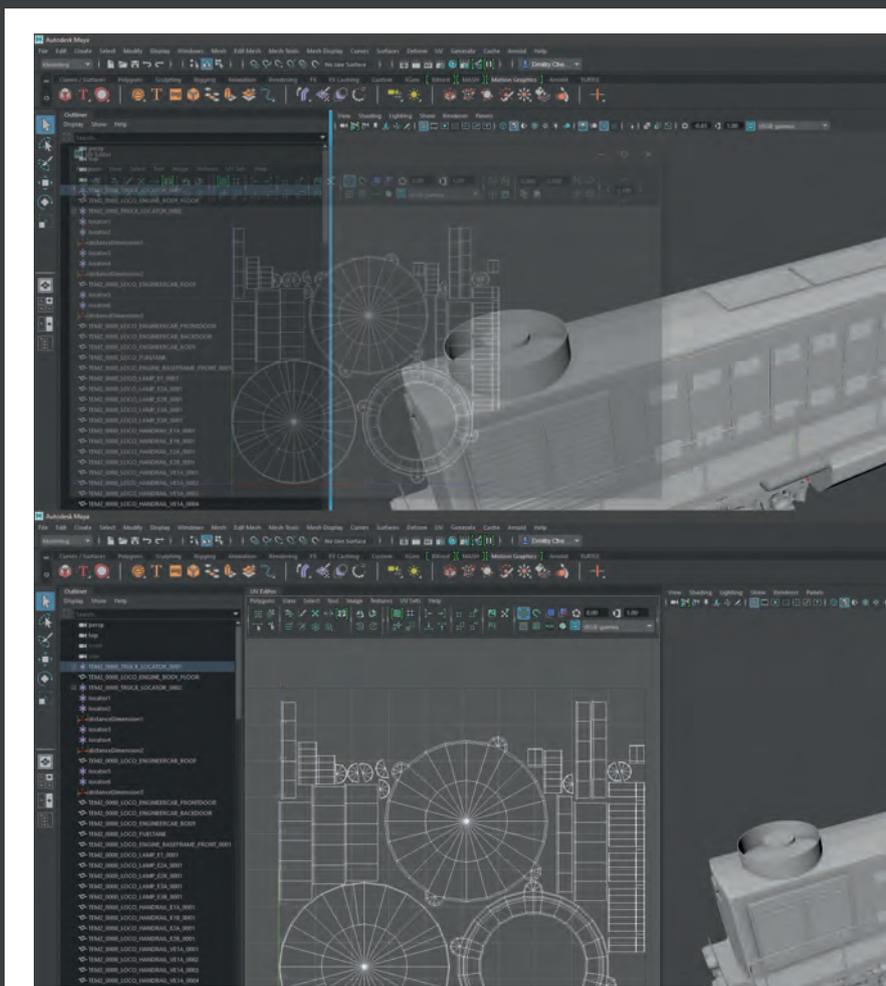
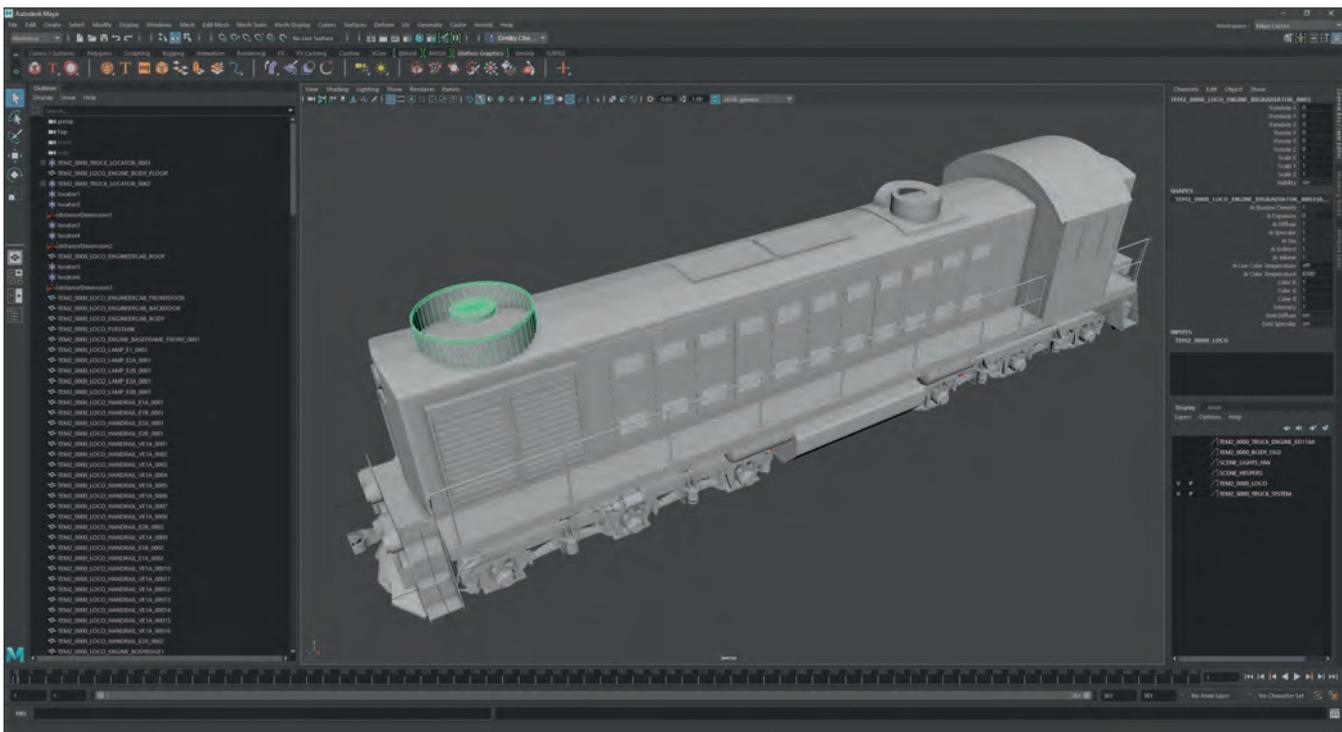


Рис.2. Диалоговое окно любого редактора, которое вы откроете в Маю, может быть представлено в виде плавающего окна, панели/вкладки.

Рис. 1. Улучшенный по стилистике и в деталях интерфейс Autodesk Maya 2017.



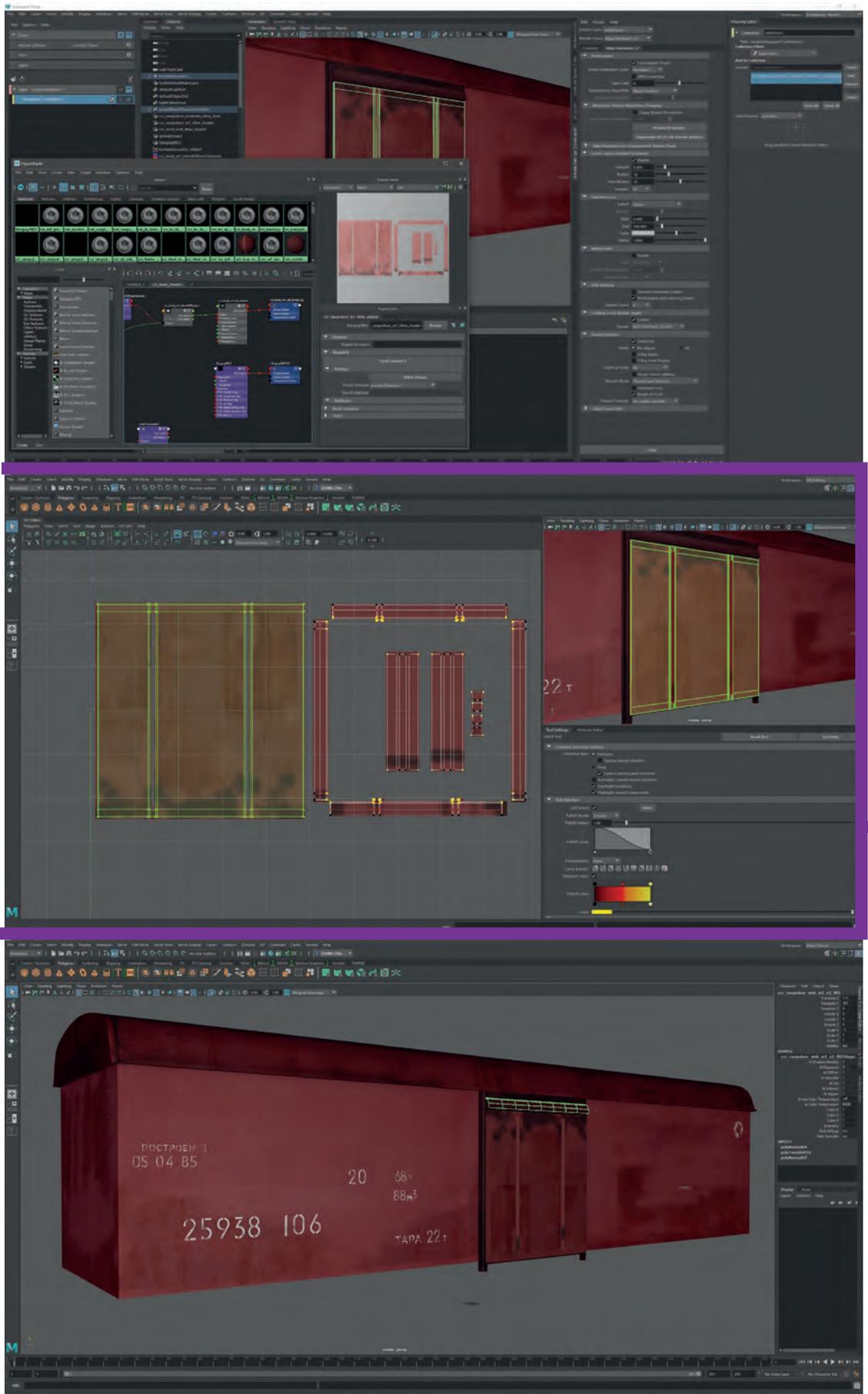


Рис. 3. Рабочие пространства в Autodesk Maya 2017.

Лицо. Обновленный интерфейс и рабочие пространства

Пакет Autodesk Maya всегда славился превосходно настраиваемым графическим интерфейсом, даже в те далекие времена, когда техническим директорам приходилось день и ночь сидеть за сотнями строк кода языка MEL. С переходом Maya на возможности платформы и библиотеки Qt разрабатывать собственные интерфейсы стало гораздо проще и удобнее. А возможности конфигурации элементов интерфейса стали безграничны. Начиная с 2016 года, программа получила поддержку новой версии библиотеки Qt, а также новые иконки с оптимизацией под дисплеи с высоким разрешением и плотностью точек.

Обновленный интерфейс не претерпел кардинальных цветовых изменений, но в новой версии вам доступны несколько важных и долгожданных функций. Первое, на что стоит обратить внимание, — возможность присоединения любого диалогового окна редактора в виде панели или закладки. Это очень удобно, если у экрана большое разрешение, и необходимо расположить в едином окне несколько часто используемых редакторов.

Другое важное и интересное нововведение — рабочие пространства. Они нам знакомы по такому приложению, как Adobe Photoshop, но для Autodesk Maya это новинка. В правом верхнем углу расположен раскрывающийся список с рабочими пространствами, в котором

можно выбрать одно из заранее подготовленных или самостоятельно созданных рабочих пространств.

По умолчанию предоставляется несколько рабочих пространств, заранее подготовленных для работы над тем или иным этапом создания трехмерной модели и сцены: моделированием, анимацией, текстурированием и визуализацией.

Душа. Инструменты анимации

Пакет Maya по праву считается одним из лучших решений для анимации и используется во многих студиях для создания реалистичных цифровых персонажей. Целая группа инструментов претерпела изменения и получила долгожданные обновления. Так, редактор Graph Editor дополнился новыми функциями для управления ключами анимации и их правки. Помимо этого, стало гораздо проще работать с трансформацией ключей и кривых анимации. Это очень помогает в редактировании сложных анимационных кривых с множеством изменений.

Новейший редактор Time Editor — это уникальная разработка. Ее создавали на протяжении полутора лет и изначально планировали включить в один из Extension к Maya 2016, но по итогам пожеланий участников тестирования редактор было решено доработать — для финальной версии Maya 2017.

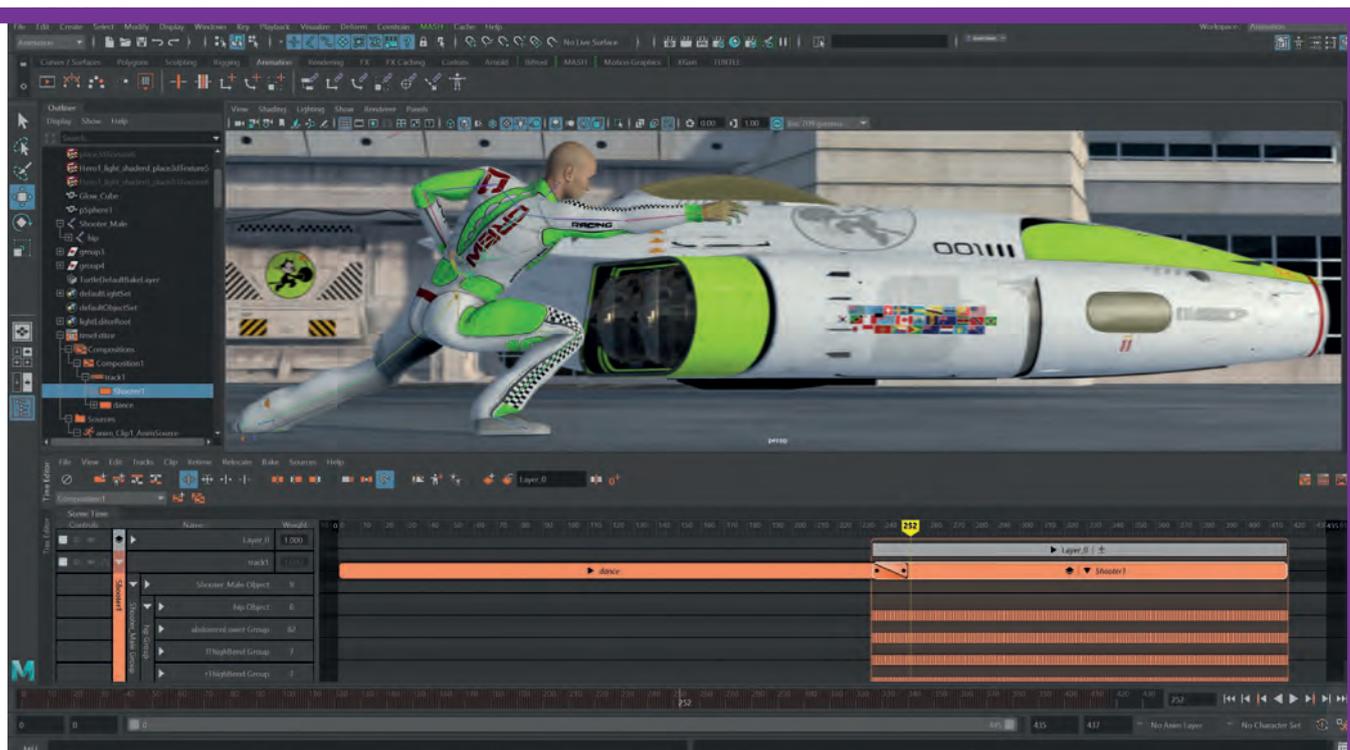


Рис. 4. Редактор Time Editor с блоками нелинейной анимации.

Недеструктивный, основанный на клипах нелинейный редактор анимации Time Editor предоставляет возможности создания и редактирования анимации на более высоком уровне. В отличие от редактора Trax Editor, который требует создания Character Sets, редактор Time Editor дает аниматорам больше свободы, позволяя работать над любым атрибутом с кривой анимации, будь то персонажи, камеры, цвета и т.д. Вы можете просто редактировать ранее созданную анимацию, например, полученную с системы захвата движения, или покадровое движение с интуитивным управлением обрезкой, масштабом, зацикливанием, разделением, группировкой, затуханием. Также с помощью Time Editor можно редактировать звук. Основанные на клипах, рабочие процессы в редакторе Time Editor опираются на концепцию работы стандартного программного обеспечения для сведения звука или монтажа видео и предоставляют возможности сведения различной анимации воедино для создания нового движения. Редактор также поддерживает несколько расширенных рабочих процессов:

- выравнивание движения с различными мировыми пространствами;
- нелинейный ретайминг;
- создание и управление слоями анимации;
- отключенный или соло-режим для треков;
- сохранение различных версий для движения.

Сердце. Повышение производительности ядра программы

Ядро программы является своеобразным сердцем всей системы в целом. В версии пакета 2016 года было представлено обновленное

ядро программы с поддержкой многопоточных вычислений и вычислений на GPU. В версии 2017 года пользователю предоставляется новый инструментальный – Evaluation Toolkit. Это инструменты для отслеживания и отладки, помогающие в диагностике проблем корректности и производительности создаваемых сцен. Инструментарий доступен непосредственно в пакете Maya тем пользователям, которые заинтересованы в понимании результата работы новых режимов оценки и обработки сцены.

Используйте Evaluation Toolkit для повышения производительности в анимации благодаря функциям, которые позволяют управлять всеми аспектами Evaluation Manager, включая активизацию режимов отладки и вывода. А технические директора могут экспортировать списки связей и выполнять визуализацию графов с помощью инструментов пакета программ с открытым исходным кодом Graphviz. Помимо новейшего инструментального для оптимизации производительности разработчики значительно оптимизировали графическую подсистему Autodesk Maya. Ядро Viewport 2.0 получило поддержку множества новых возможностей современных графических ускорителей и оптимизировано для работы с OpenGL 4.X. Это дало существенный прирост производительности программы в работе с комплексными и сложными сценами, а также с анимацией.

Созидание. Обновление инструментов моделирования

Новая версия Maya получила ряд долгожданных и важных изменений в инструментальном моделировании. О многих из них мы писали в предыдущих номерах каталога Softline Direct.

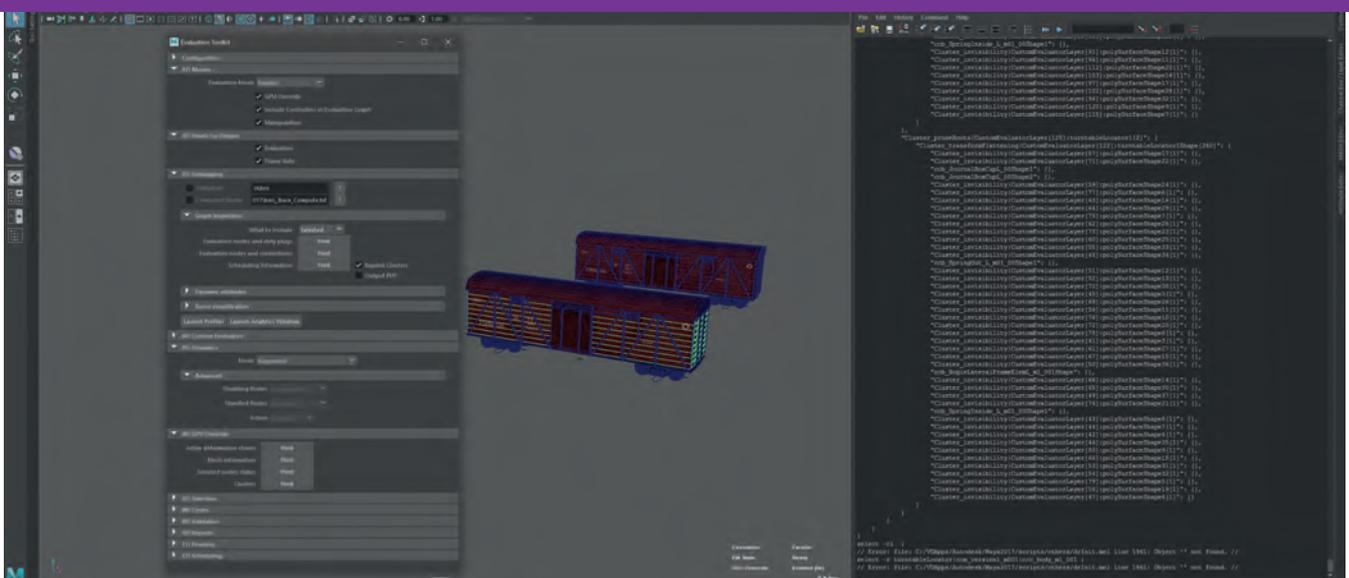


Рис. 5. Редактор Evaluation Toolkit и данные, собранные в процессе воспроизведения анимации, отображаемые в Script Editor.

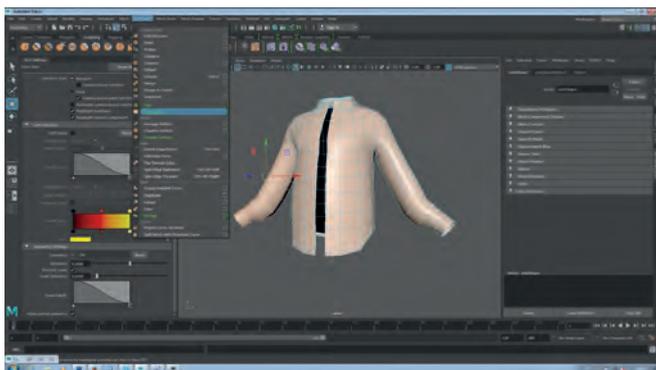


Рис. 6. Обновленные функции симметрии в Maya 2017.

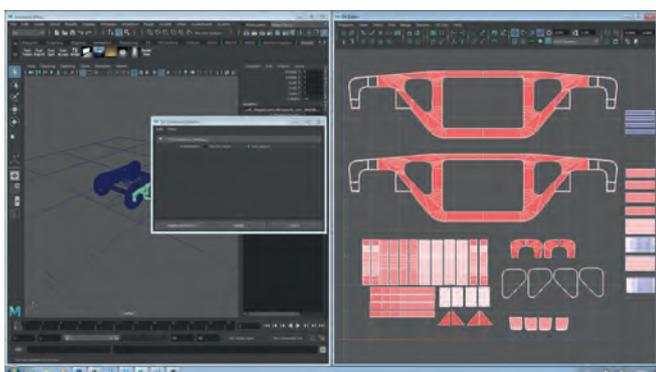


Рис. 7. Функция представления искажений UV-координат в режиме работы Object.

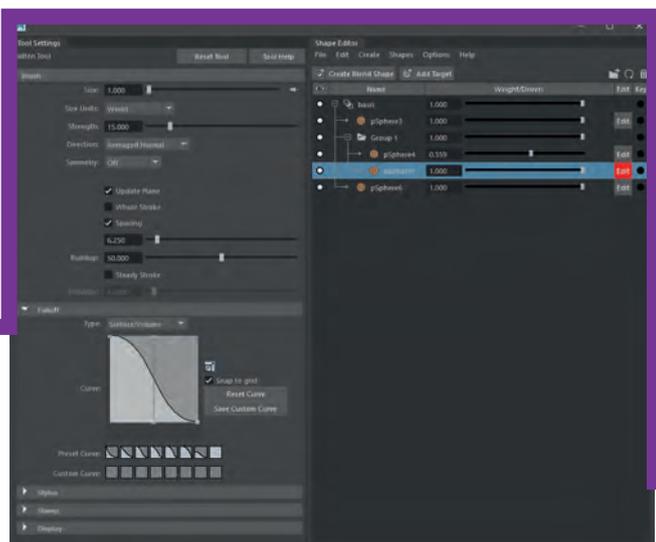


Рис. 8. Новый редактор Shape Editor позволяет создавать и редактировать множество целей для сложных форм.

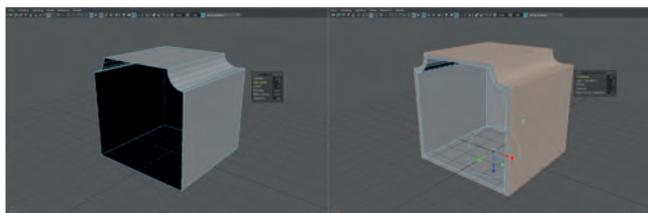


Рис. 9. Новые функции инструментов Bevel и Extrude позволяют точнее формировать форму модели.

В процессе разработки версии 2017 года разработчики акцентировали свое внимание на стабильности работы инструментов и расширении функционала.

При моделировании часто используется функция симметрии. Новая версия предоставляет несколько новых возможностей для упрощения процесса моделирования симметричных моделей. Теперь, когда инструмент симметрии активен, симметричные выделяемые элементы будут подсвечены. Так пользователю легче отслеживать, какие вершины, ребра или грани будут включены в симметрию. Для повышения информативности в панели видового окна при активизации симметрии отображается информационная подсказка.

Вы можете использовать новую команду Flip для переноса позиций компонентов через ось симметрии. Кроме того, поддержка симметрии была реализована во многих инструментах моделирования, доступных в Modelling Toolkit.

В процессе редактирования UV-координат полезно использовать функцию представления искажения UV-координат, а в Maya 2017 данная функция получила дополнительные опции, с помощью которых вы можете выбирать то, как именно отображать искажения координат — по объекту или оболочке.

Пользователи, использующие инструменты цифровой лепки, получили обновленный редактор Shape Editor. Теперь можно редактировать множество целей, создавать группы целей, определять степень их вклада в общую модель, стирать цели, создавать маски целей и сглаживать их.

Благодаря реализации пожеланий пользователей многие инструменты моделирования получили новые функции. Так, инструмент моделирования Bevel теперь имеет новые атрибуты для управления глубиной соединения граней и формой фасок.

Инструмент Bridge получил функцию определения направления, в котором заполняется

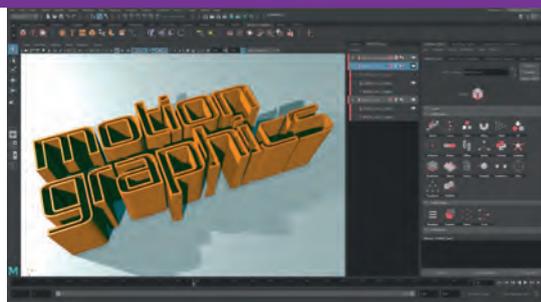


Рис. 10. Набор инструментов MASH позволяет с легкостью создавать сложные анимационные эффекты для титров и заставок с большим количеством процедурных эффектов.

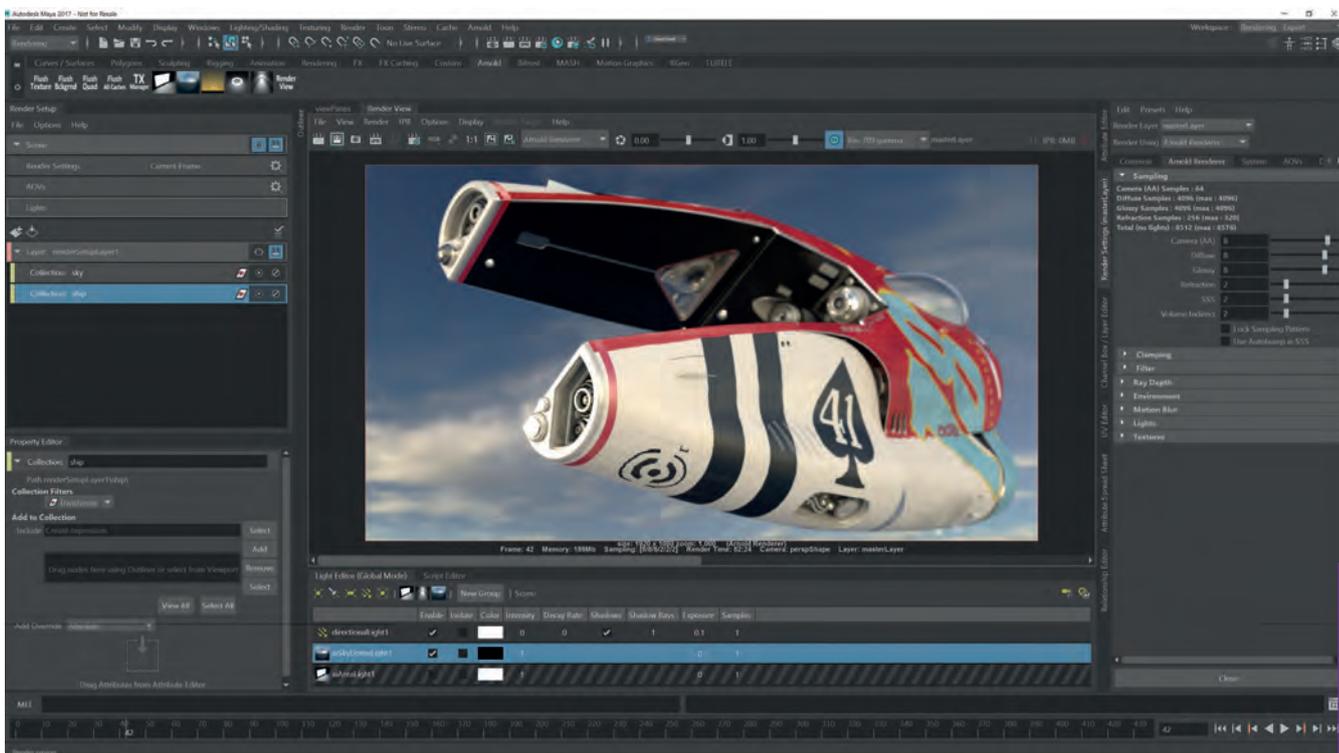


Рис. 11. Система визуализации SolidAngle Arnold Renderer и новая система подготовки сцен к визуализации в Maya 2017.

пространство между исходными и целевыми ребрами/гранями. В инструменте Extrude разработчики постарались реализовать усовершенствованный алгоритм вычисления толщины, что позволяет создавать более предсказуемые результаты при использовании выдавливания для создания толщины в геометрии модели.

Также стало возможным использовать ребра из других объектов в качестве точки для ориентирования граней. Это позволяет использовать временные объекты в качестве направляющих, делая процесс моделирования таких сложных вещей, как трубы или шланги, быстрее и проще.

Если привести все к одному знаменателю, можно сказать, что новейшая версия Autodesk Maya является одним из самых передовых решений, предоставляющим множество разнообразных инструментов и подходов для создания различных моделей и их трансформации.

Фантазия. Motion Graphics with MASH

Индустрия Motion Graphics является молодым направлением компьютерной графики, но в ней уже твердо закрепились такие пакеты, как Cinema 4D и After Effects. Компания Autodesk не остановилась на этом и включила в арсенал инструментов Maya новый пакет инструментов MASH.

Инструментарий MASH предоставляет возможность с помощью нескольких процедур-

ных узлов, сценариев на Python и ключей анимации создавать как простые, так и сложные цикличные эффекты анимации и деформации геометрии.

Для финальной пост-обработки часто используется пакет After Effects CC от компании Adobe. Для работы с данным пакетом разработчики включили специальный инструмент Send to AE, создающий сценарий на языке JSON, в котором представлены камеры, источники света, группы, локаторы и геометрия. Каждый из данных объектов будет содержать данные в виде позиции, вращения, масштаба, интенсивности, угла конуса и цвета (для источников света).

Глаза. Изменения в инструментах визуализации

До версии 2016 года включительно пакет Maya поставлялся с системой визуализации mental ray for Maya, разрабатываемой компанией NVIDIA. Данная система визуализации поставлялась с программой на протяжении 14 лет, но в версии 2017 года все изменилось.

Теперь вместе с пакетом Autodesk Maya будет поставляться система визуализации Arnold Renderer от компании SolidAngle. Это перспективное и гибкое решение для высококачественной визуализации, тесно интегрированное с помощью модуля MtoA и поддерживающее многие функции Maya.

Система визуализации Arnold использует ядро визуализации с расширенными алгоритмами трассировки лучей на основе метода Мон-



те-Карло, разработанное для применения в полнометражных анимационных фильмах и создании визуальных эффектов. Изначально система визуализации была разработана совместно со студией Sony Pictures ImageWorks, где на данный момент является ведущим средством для визуализации анимации и эффектов. Система визуализации Arnold используется в более чем 300 студиях по всему миру, включая Industrial light & Magic (ILM), Framestore, MPC, The Mill и Digic Pictures.

Система визуализации доступна как в виде модулей расширения для Maya, Softimage, Houdini, Cinema4D и Katana, так и в виде standalone-приложения для платформ Linux, Windows и Mac OS.

Как быть, если сцена создана с применением mental ray for Maya? Эта система визуализации целиком разрабатывается компанией NVIDIA, и новейшая версия mental ray 3.14 и mental ray for Maya 2017 будут доступны у дистрибьютеров и партнеров компании NVIDIA, как в виде модулей расширения, так и в качестве standalone-версии, которые могут быть приобретены отдельно.

На протяжении всей разработки новой версии, был добавлен инструментарий для визуализации сложных сцен и визуализации слоев, пришедший на смену устаревшим Maya Render Layers. В поставку Autodesk Maya 2017 включен новый инструментарий получивший имя Render Setup System. Он тесно интегрируется с Arnold Renderer и разработан в партнерстве Autodesk со специалистами из студии Sony Pictures ImageWorks.

С помощью нового инструментария можно создавать множество независимых слоев визуализации и каждому из них назначать «коллекции» объектов, шейдеров материалов и текстур, параметров, а для каждой из коллекций добавлять множество редактируемых атрибутов, связанных с атрибутами узлов сцены.

Для облегчения работы художников по освещению в новую версию был добавлен инструмент Light Editor. С его помощью художники могут выделять и управлять ключевыми параметрами всех источников света в сцене.

Редактор Hypershade получил несколько новых возможностей. Начиная с версии 2016 года данный редактор полностью перерабо-

Рис. 12. Примеры образов, визуализированных с помощью Arnold Renderer.

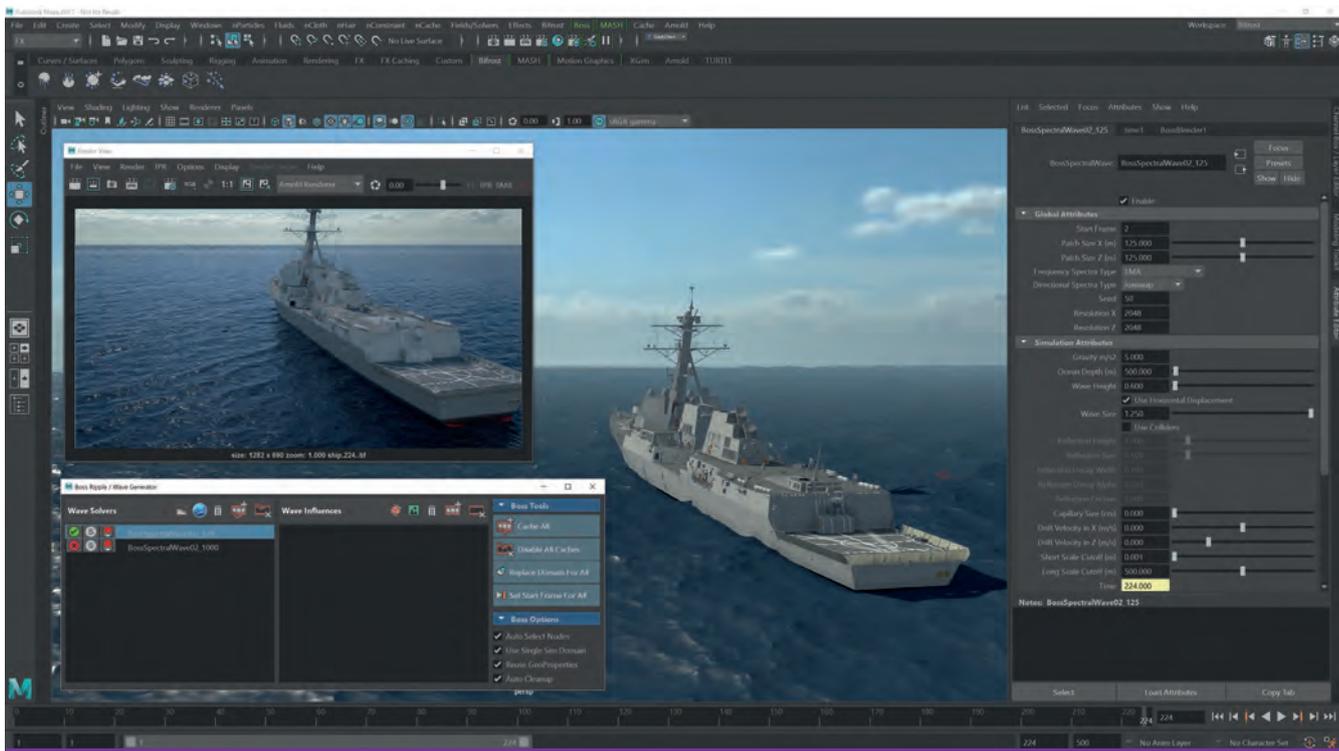


Рис. 14. С Помощью новой системы BOSS стало проще создавать реалистичную поверхность океана.

тан, а новая версия позволяет управлять камерой в Preview Panel аналогично видовому окну, останавливать или запускать процесс интерактивной визуализации образцов материалов. В редакторе Outliner теперь можно включить отображение назначенных объектам сцены шейдеров.

Шейдер Stingray PBS получил возможность создания эффекта подповерхностного рассеивания света, чтобы делать более убедительные образы, моделировать кожу, пластик, листья и выполнять визуализацию данного эффекта в Autodesk Stingray Game Engine.

Движение. Динамика и эффекты

Создание реалистичных причесок и эффектов движения меха и волос всегда считались сильной стороной Maya. Совместно со специалистами Disney Animation Studios компания Autodesk интегрировала в пакет набор инструментов, разработанный студией, — XGen. Таким образом, пользователи получили удобный редактор для интерактивного создания причесок и их редактирования.

Создание причесок для всех типов волос и меха в XGen стало проще и быстрее благодаря Interactive Groom Splines. Этот новый набор функций состоит из интуитивных инструментов на основе кистей, которые обеспечивают больший контроль и точность для осуществления укладки волос и меха. Кроме этого, художники могут использовать модификатор слоев, чтобы лепить и смешивать слои или ключевые

эффекты, созданные с помощью инструментов Interactive Groom.

Для моделирования реалистичных эффектов динамики воды и брызг в Maya был интегрирован новый инструментарий, получивший название Bifrost. В новой версии пакета была добавлена система Bifrost Ocean Simulation System (BOSS), создающая реалистичные поверхности океана с волнами и рябью. Она действует, начиная с плоской геометрии, а затем размещает поверх нее слои и решатели объединения, которые влияют на вершины поверхности.

Ни один элемент системы не зависит от разрешения остальных и может быть помещен в кэш отдельно для более быстрого воспроизведения анимации. Используйте полученную деформированную геометрию напрямую или передавайте результат на другую геометрию.

Объединение. Shotgun 7.0 и Autodesk Maya 2017

Система управления проектами Shotgun, вошедшая в линейку продуктов Autodesk Media & Entertainment, продолжает свое развитие и пополнение функционала. Новая версия Autodesk Maya 2017 интегрируется с Shotgun и RV — инструментом, позволяющим выполнять рецензирование и отслеживание проделанной художниками работы.

В Global Media App добавлен вид Editorial, с которым пользователям проще просматривать и управлять всеми своими данными внутри си-

темы Shotgun. С новым инструментом Cuts Tray в браузере и RV вы быстро увидите свою последнюю работу в контексте нарезки. Реализовано переключение между полным или мини-режимом представления нарезки, фильтр по статусу или ступени производственного процесса, а также просмотр различных версий нарезок.

Приложение Import Cut App публикует редакционную информацию в Shotgun и автоматически генерирует отчет о нарезке сцен и планов, который может быть разослан участникам команды.

Обновление Toolkits для интеграции со сторонними приложениями позволяет пользователям публиковать информацию о редактировании непосредственно в Shotgun из используемых ими приложений, таких как Flame, HIERO и NUKE. Официальные Editorial Schema предоставляют студиям возможности легкой и глубокой интеграции Shotgun в свои редакционные процессы.

Пробуждение. Развитие продолжается

Пакет Autodesk Maya претерпел множество изменений на протяжении пятилетнего цикла разработки, и за последние 6 лет это — одно из серьезнейших обновлений системы в целом. На текущий момент, разработчики завершили обновление множества инструментов, программа обладает обширным набором высокопроизводительных функций для моделирования, анимации, визуальных эффектов и визуализации. Одним из важнейших изменений является смена ключевого инструмента высококачественной визуализации с поддержкой передовых решений для визуализации, затенения и освещения, а также оптимизиро-

ванного для работы с большими массивами данных. Другим важным нововведением является значительное увеличение производительности пакета с заделом на дальнейшее развитие и поддержкой новейших аппаратных и программных технологий. Включение многопоточных вычислений и поддержка ускорения вычислений с помощью GPU во многих функциях ядра программы позволило увеличить скорость реакции системы на действия пользователя и улучшить процесс работы аниматоров.

Возможно, адаптироваться к многочисленным переменам не так-то просто, но мир технологий не перестает развиваться, и на рынке растут требования к качеству выпускаемой продукции и срокам ее реализации. Так что кардинальные перемены неизбежны. Новые решения, которые появились за последние годы на рынке, достаточно свежи и новы, они чисты и не страдают болезнями времени. С ними художники проще и быстрее воплотят свои фантазии в жизнь, создавая потрясающие образы и тем самым оставаясь на гребне технологий.

С переходом на модель подписки порог входа в индустрию компьютерной графики стал гораздо ниже. Нет необходимости платить большие суммы за поддержку и локальную лицензию, а управлять лицензируемыми продуктами стало значительно проще с помощью единого центра управления учетной записью. Новая Autodesk Maya 2017 поддерживает данную опцию, и вы можете пользоваться онлайн-сервисами Autodesk и их партнеров напрямую, из интерфейса программы. В качестве примера вспомним сервис Shotgun и облачные решения Autodesk в виде сервисов A360 или сервиса визуализации ZYNC.

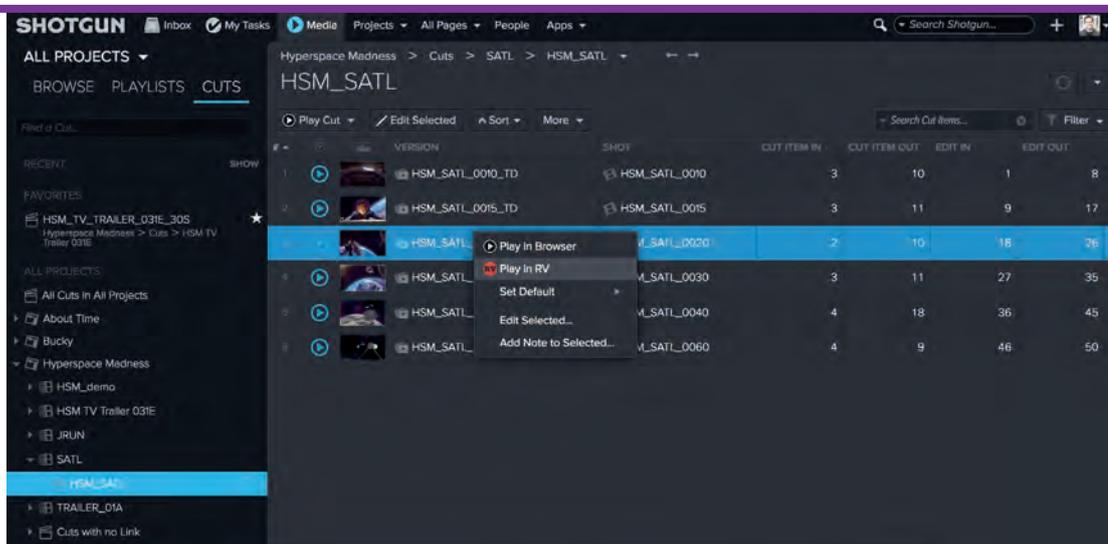


Автор: Дмитрий Чехлов, художник по освещению и затенению, автор книги «Визуализация в Autodesk Maya: mental ray renderer», технический специалист в области компьютерной визуализации, Autodesk Certified Professional и участник программы Autodesk Developer Network.



За подробной информацией о моделях лицензирования, вариантах приобретения и внедрения вы можете обратиться к специалистам Softline.

Рис. 15. Новая версия Shotgun & RV 7.0 делает работу художников более отлаженной и не позволяет упускать детали.





MapInfo Pro и MapInfo Pro Advanced



MapInfo Pro и MapInfo Pro Advanced — географические информационные системы (ГИС), предназначенные для сбора, хранения, отображения, редактирования и анализа пространственных данных.

Сферы применения ГИС MapInfo

Бизнес и наука, образование и управление, социологические, демографические и политические исследования, промышленность и экология, транспорт и нефтегазовая индустрия, землепользование и кадастр, службы коммунального хозяйства и быстрого реагирования, армия и органы правопорядка, а также многие другие отрасли хозяйства.

Функционал MapInfo Pro

MapInfo Pro имеет полный набор средств для создания, редактирования и оформления картографической информации. Предоставляет развитые средства построения тематических карт. Позволяет использовать обширные наборы условных обозначений. Поддерживает все распространённые форматы векторных и растровых пространственных данных. Обеспечивает доступ к картографическим web-службам WMS и WFS и серверам тайлов.

MapInfo Pro может выполнять функции картографического клиента для всех современных СУБД. Предусмотрена возможность хранения и обработки пространственных объектов в базах данных Oracle, MS SQL Server, PostGIS, SQLite без использования дополнительного программного обеспечения.

Встроенный язык запросов SQL, благодаря географическому расширению, позволяет осуществлять выборки объектов с учетом их пространственных отношений. MapInfo имеет функции поиска объекта или группы объектов по различным признакам, а также их сочетаниям.

Сейчас существуют 32- и 64-разрядные версии MapInfo. Они имеют сходную функциональность, используют один и тот же серийный номер и могут использоваться на компьютере одновременно. Отличительные особенности 64-разрядной программы — ленточный интерфейс, поддержка Юникод, TAB-файлов размером более 2 Гб и наличие расширенной версии — MapInfo Pro Advanced.

MapInfo Pro Advanced — векторно-растровая ГИС

MapInfo Pro Advanced — это расширенная версия MapInfo Pro, включающая модуль, предназначенный для создания, обработки, визуализации и анализа растровых поверхностей (гридов). MapInfo Pro Advanced превращает векторную ГИС MapInfo в векторно-растровую ГИС.

В основе MapInfo Pro Advanced лежит совершенно новое высокопроизводительное ядро обработки растра, использующее преимущества 64-разрядной архитектуры и инновационный формат хранения растровых данных Multi-Resolution Raster (MRR). MRR — это формат, специально разработанный для MapInfo Pro Advanced. Он обладает значительными преимуществами по сравнению с существующими растровыми форматами.

Русская версия MapBasic 15

MapInfo MapBasic — язык программирования геоинформационной системы MapInfo Pro.

MapBasic позволяет разрабатывать приложения, расширяющие стандартные возможности MapInfo. Возможность вызова DLL и других программ позволяет создавать сложные специализированные приложения с использованием языков программирования высокого уровня. MapBasic содержит около 400 операторов и функций.

Имеется возможность разработки приложений на языках VB.NET, C# и других языках платформы .NET. Для тиражирования приложений можно использовать MapInfo RunTime.



Компания ЭСТИ МАП
Официальный представитель
Pitney Bowes Software Inc.
в России и СНГ

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

E-mail: sales@mapinfo.ru,
esti-m@mapinfo.ru
www.mapinfo.ru

Функциональные блоки MapInfo Pro Advanced

MapInfo Pro Advanced содержит все основные возможности растровой ГИС, которые можно выделить в три функциональных блока: создание растра, обработка растра и анализ растра.

- Блок создания растра содержит шесть методов создания растровых изображений на основе точечных данных, три метода интерполяции и три метода пространственного моделирования.
- Блок обработки растра включает следующие операции: конвертацию изображений из одного формата в другой; объединение различных растров и хранение их в индивидуальных полях или в нескольких зонах, ассоциированных с одним полем; слияние нескольких растров в один; растеризацию векторных полигональных данных; изменение проекции; изменение размерности растра – ресемплинг и вырезание части грида.
- Блок анализа растра включает следующие инструменты: калькулятор гридов для выполнения математических и логических операций; построение профилей поверхности; построение зон видимости; анализ поверхностей (расчет углов наклона, экспозиции и др.); классификация для переопределения значений ячеек грида; фильтр и инструменты для атрибутирования векторных данных значениями растров.

Дополнения и возможности для ознакомления с продуктами

MapInfo Pro Advanced включает SDK, инструментарий для разработки собственных приложений на основе нового растрового «движка». Ознакомительные версии программ и документация доступны на сайте www.mapinfo.ru.



Компания ЭСТИ МАП

Официальный представитель
Pitney Bowes Software Inc.
в России и СНГ

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

E-mail: sales@mapinfo.ru,
esti-m@mapinfo.ru
www.mapinfo.ru



Softline обеспечила управление мобильными устройствами в детских магазинах «Кораблик»

Завершен пилотный проект по развертыванию и настройке облачного сервиса Microsoft Intune в сети детских магазинов «Кораблик». В результате заказчик получил возможность протестировать функционал решения и настроить необходимые политики, в результате чего было принято решение о внедрении полноценной системы управления корпоративной мобильностью.

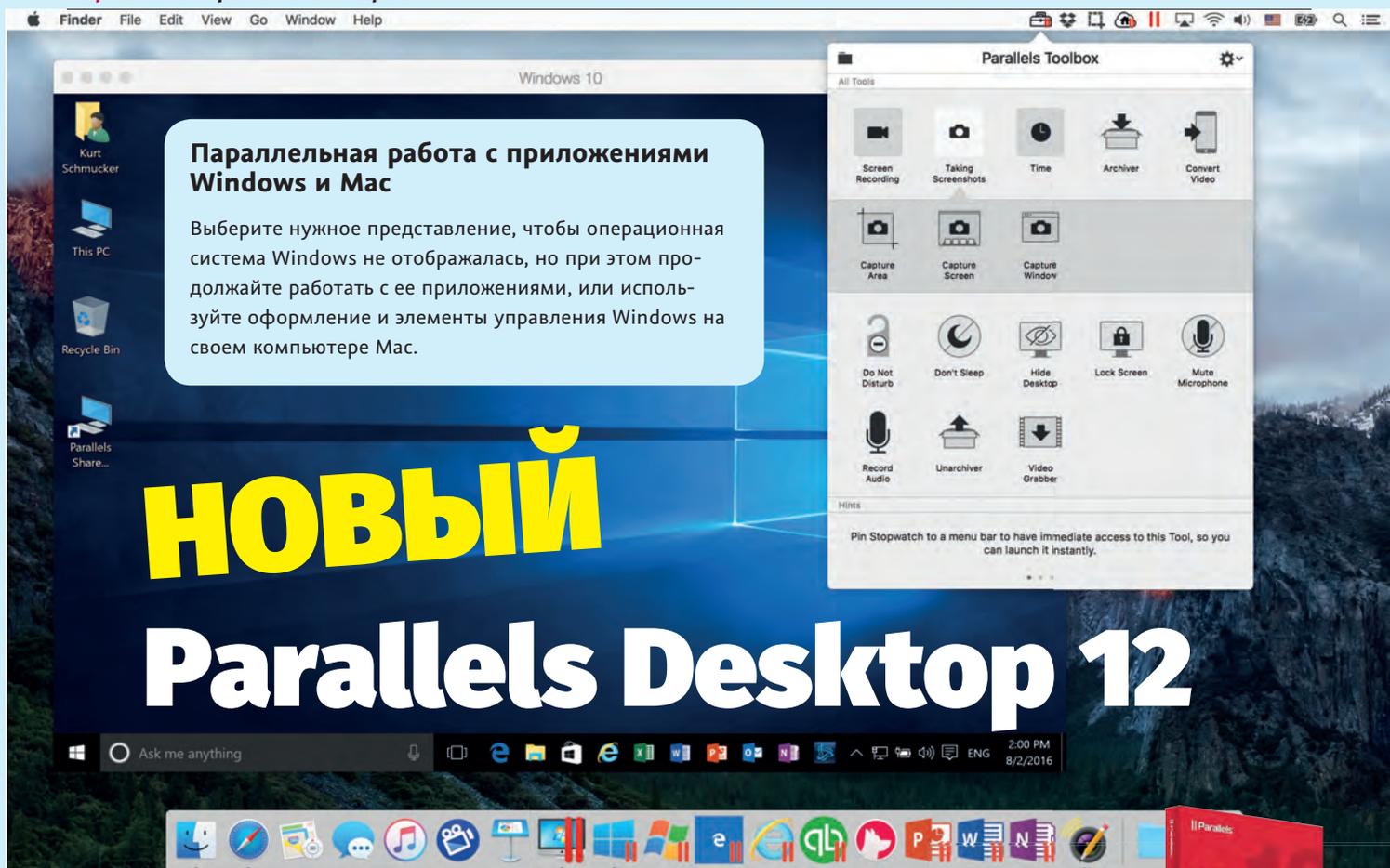
«Кораблик» — одна из крупнейших отечественных сетей детских магазинов, насчитывающая более 150 точек продаж в Москве, Московской области и других городах России.

Специалисты департамента решений Microsoft компании Softline развернули в инфраструктуре заказчика средство по управлению мобильными устройствами Microsoft Intune и интегрировали его с облачным каталогом Azure AD.

За счет публикации корпоративного приложения на облачном портале Intune и его автоматического распространения на мобильные устройства можно сократить время на настройку каждого планшета. Создание профиля Wi-Fi позволяет устройствам автоматически подключаться к корпоративной интернет-сети. Групповая политика распространяет настройки на все планшеты. В результате сотрудники могут оперативно приступить к работе, не посылая запрос на подключение в ИТ-департамент.

«Политики, настроенные в «Кораблике», помогут сотрудникам получить мобильный доступ к корпоративным ресурсам, а системным администраторам автоматически подготавливать мобильные устройства к работе. Intune позволяет защитить данные, находящиеся на планшете, заблокировав устройство в случае его утери или кражи. А гибкое управление учетными записями дает возможность проводить полную или частичную очистку информации, хранящейся на планшетах», — прокомментировал Андрей Изотов, руководитель направления корпоративной мобильности Управления решений компании Softline.





НОВЫЙ Parallels Desktop 12

Parallels Desktop 12 для Mac — это быстрое, простое и эффективное решение для запуска приложений Windows на Mac параллельно, без перезагрузки. Используйте свои любимые приложения Windows в Mac, копируйте и перетаскивайте объекты между приложениями для разных операционных систем.



Вы можете приобрести новый Parallels Desktop 12 в интернет-магазине Allsoft.



Теперь в состав решения входит Acronis True Image Cloud 500 GB и набор утилит Parallels Toolbox, которые позволяют без всяких усилий справляться с десятками самых важных задач на компьютере Mac. Делайте снимки экрана, защищайте важные файлы паролем, преобразовывайте видеоролики с Facebook или YouTube и используйте множество других возможностей.

Теперь с поддержкой Windows 10 и MacOS

Запускайте и Windows 10, и MacOS без каких-либо усилий. Используйте виртуального помощника Microsoft Cortana на компьютере Mac.

Перейдите с PC на Mac

Теперь все ваши файлы, приложения, закладки браузера и другие данные можно очень удобно перенести с PC на Mac — просто следуйте инструкциям мастера настройки.

Надежная производительность

Parallels Desktop Pro Edition позволяет использовать более мощные виртуальные машины. Для каждой виртуальной машины доступно 64 Гб виртуального ОЗУ и 16 виртуальных процессоров, что позволяет вам работать даже в самых ресурсоемких приложениях.

Поддержка различных ОС

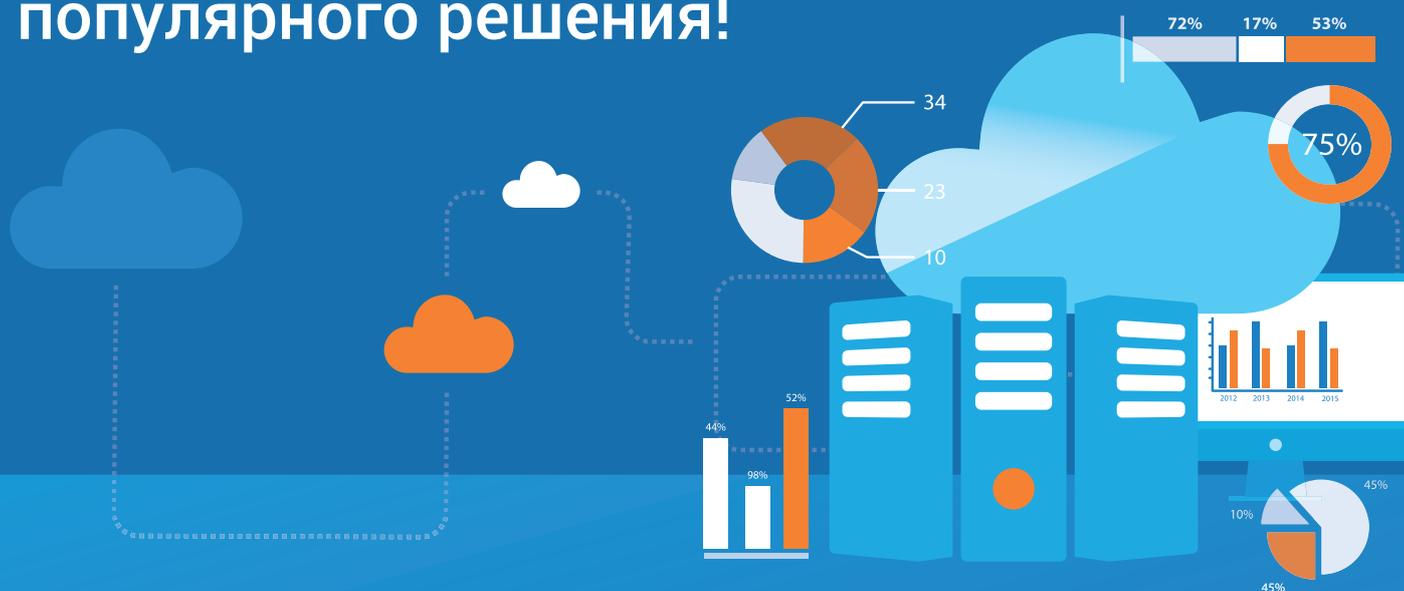
Используйте различные операционные системы, в том числе OS X, Windows 10, Windows 8.1 и Windows 7, Linux и Google Chrome. На компьютере Mac можно работать практически в любой операционной системе!

Работа с Boot Camp

Используйте уже установленную версию Boot Camp. Теперь конвертировать виртуальную машину из Boot Camp можно гораздо проще.



Microsoft SQL Server Enterprise в облаке - выгодный вариант использования популярного решения!



Вы получаете доступ к готовому сервису баз данных Microsoft SQL Server Enterprise от **950р. в месяц.**

В стоимость решения включены: лицензии, оборудование, отказоустойчивость с использованием технологии «Always On» и поддержка от ActiveCloud.

Используйте решение корпоративного уровня по доступной цене.

+7 (495) 988-22-62 доб. 6602
8 (800) 100-22-50

azure@activecloud.com
sql.activecloud.ru

Расписание курсов в Учебном центре Softline

Код курса	Город	Полное название курса	Даты
LL-101	Казань	Основы работы в операционной системе Linux	31 октября-3 ноября
20462	Казань	Администрирование баз данных Microsoft SQL Server 2014	31 октября-4 ноября
20696	Казань	Администрирование System Center Configuration Manager и Intune	31 октября-4 ноября
20461	Екатеринбург	Создание запросов к Microsoft SQL Server 2014	31 октября-3 ноября
LL-102	Екатеринбург	Системное администрирование Linux	31 октября-3 ноября
KL-002.10	Екатеринбург	Kaspersky Endpoint Security and Management. Базовый курс	31 октября-2 ноября
KL-302.10	Екатеринбург	Kaspersky Endpoint Security and Management. Масштабирование	31 октября-1 ноября
LL-103	Ростов-на-Дону	Сетевое администрирование Linux	31 октября-3 ноября
10961	Самара	Автоматизация администрирования с использованием Windows PowerShell	31 октября-4 ноября
ADVANCED-IPS	Самара	Углубленное изучение IPS	31 октября-1 ноября
10982	Новосибирск	Поддержка и устранение неисправностей Windows 10	31 октября-4 ноября
SWITCH v.2.0	Красноярск	IP-коммутиция на базе оборудования Cisco	31 октября-4 ноября
20341	Хабаровск	Базовые решения с использованием Microsoft Exchange Server 2013	31 октября-4 ноября
БПД	Владивосток	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	31 октября-5 ноября
CUWSS	Москва	Проведение обследования унифицированных беспроводных сетей Cisco	31 октября-3 ноября
LL-103	Ростов-на-Дону	Сетевое администрирование Linux	31 октября-3 ноября
10962	Москва	Автоматизация администрирования на PowerShell, расширенный курс	31 октября-2 ноября
20410	Москва	Установка и конфигурирование Windows Server 2012 R2	31 октября-3 ноября
CNS-220	Москва	Основы Citrix NetScaler и управление трафиком	31 октября-3 ноября
10964	Москва	Мониторинг Центров Обработки Данных с помощью System Center Operations Manager	31 октября-3 ноября
ITIL3_OSA	Санкт-Петербург	Операционная поддержка и анализ	31 октября-3 ноября
CUWSS	Москва	Проведение обследования унифицированных беспроводных сетей Cisco	31 октября-3 ноября
CNS-220	Москва	Основы Citrix NetScaler и управление трафиком	31 октября-3 ноября
10964	Москва	Мониторинг Центров Обработки Данных с помощью System Center Operations Manager	31 октября-3 ноября
10962	Москва	Автоматизация администрирования на PowerShell, расширенный курс	31 октября-2 ноября
VSFT5.5	Москва	VMware vSphere: Fast Track v.5.5 (Углубленное изучение vSphere)	31 октября-4 ноября
VCSRM58	Москва	VMware vCenter Site Recovery Manager: Установка, настройка, управление [V5.8]	31 октября-1 ноября
20410	Москва	Установка и конфигурирование Windows Server 2012 R2	31 октября-3 ноября
20488	Москва	Разработка основных решений Microsoft SharePoint Server 2013	31 октября-3 ноября
20697-2B	Москва	Развертывание и управление Windows 10 при помощи корпоративных служб	31 октября-3 ноября
DESGN v.3.0	Москва	Проектирование распределенных сетей Cisco (Designing for Cisco Internetwork Solutions)	31 октября-3 ноября
CIPT-2 v.8.0	Москва	Cisco Unified Communications Manager, Part 2	31 октября-3 ноября
20762	Москва	Разработка баз данных SQL	31 октября-3 ноября
20410	Санкт-Петербург	Установка и конфигурирование Windows Server 2012 R2	7-11 ноября
SLIT-292	Санкт-Петербург	TIL© v3. SOA: Управленческие инструменты организации отношений ИТ с бизнесом	7-9 ноября

Код курса	Город	Полное название курса	Даты
20694	Санкт-Петербург	Виртуализация корпоративных рабочих столов и приложений	7-11 ноября
20342	Санкт-Петербург	Продвинутое решение на базе Microsoft Exchange Server 2013	7-11 ноября
VNICM7	Санкт-Петербург	Horizon (совместно с View): Установка, настройка и управление v.7	7-11 ноября
QOS v.2.5	Ростов-на-Дону	Поддержка технологии QOS (Implementing Cisco Quality of Service)	7-11 ноября
LL-102	Нижний Новгород	Системное администрирование Linux	7-10 ноября
20761	Нижний Новгород	Создание запросов данных при помощи Transact-SQL	7-9 ноября
20765	Нижний Новгород	Обеспечение баз данных SQL	10-13 ноября
ITIL3_OSA	Самара	Операционная поддержка и анализ	7-10 ноября
CCNAX v.3	Самара	Создание сетей на базе оборудования Cisco: Ускоренный курс	7-11 ноября
20341	Екатеринбург	Базовые решения с использованием Microsoft Exchange Server 2013	7-11 ноября
TSHOOT v.2.0	Екатеринбург	Поиск и устранение неисправностей в IP-сетях на базе оборудования Cisco	7-11 ноября
US-1301	Екатеринбург	Microsoft Word 2013 – базовый курс	7 ноября
US-1302	Екатеринбург	Microsoft Word 2013 – расширенный курс	8 ноября
US-1303	Екатеринбург	Microsoft Excel 2013 – базовый курс	9 ноября
US-1304	Екатеринбург	Microsoft Excel 2013 – расширенная консультация	10-11 ноября
20332	Екатеринбург	Расширенные решения Microsoft SharePoint Server 2013	7-11 ноября
SLBT-004	Екатеринбург	ИТ-директор: о самом главном за 4 дня	7-10 ноября
20411	Омск	Администрирование Windows Server 2012 R2	7-11 ноября
20341	Омск	Базовые решения с использованием Microsoft Exchange Server 2013	7-11 ноября
SLBT-006	Новосибирск	Вдохновляющее и мотивационное лидерство	7-8 ноября
ITIL3_OSA	Красноярск	Операционная поддержка и анализ	7-9 ноября
20331	Красноярск	Базовые решения Microsoft SharePoint Server 2013	7-11 ноября
20410	Хабаровск	Установка и конфигурирование Windows Server 2012 R2	7-11 ноября
20342	Хабаровск	Продвинутое решение на базе Microsoft Exchange Server 2013	7-11 ноября
20341	Владивосток	Базовые решения с использованием Microsoft Exchange Server 2013	7-11 ноября
20347	Владивосток	Подключение и управление Office 365	7-11 ноября
VNICM7	Санкт-Петербург	Horizon (совместно с View): Установка, настройка и управление v.7	7-11 ноября
20341	Омск	Базовые решения с использованием Microsoft Exchange Server 2013	7-11 ноября
CCNAX v.3	Москва	Создание сетей на базе оборудования Cisco: Ускоренный курс	7-11 ноября
VSICM6	Москва	VMware vSphere: Установка, настройка, управление	7-11 ноября
10967	Москва	Основы инфраструктуры Windows Server	7-11 ноября
20411	Москва	Администрирование Windows Server 2012 R2	7-11 ноября
11gDBA1	Москва	Oracle Database 11g: Administration Workshop I	7-11 ноября
ITIL3_OSA	Красноярск	Операционная поддержка и анализ	7-11 ноября
20331	Красноярск	Базовые решения Microsoft SharePoint Server 2013	7-11 ноября
20347	Владивосток	Подключение и управление Office 365	7-11 ноября
DP0134	Москва	NetBackup 7.7 Administration	7-11 ноября
11gDBA1	Москва	Oracle Database 11g: Administration Workshop I	7-11 ноября
10967	Москва	Основы инфраструктуры Windows Server	7-11 ноября
VSICM6	Москва	VMware vSphere: Установка, настройка, управление	7-11 ноября
20764	Москва	Администрирование инфраструктуры баз данных SQL	7-11 ноября
20411	Москва	Администрирование Windows Server 2012 R2	7-11 ноября
20334	Москва	Базовые решения Microsoft Skype for Business 2015	7-11 ноября
20489	Москва	Разработка продвинутого решения на базе Microsoft SharePoint Server 2013	7-11 ноября
CCNAX v.3	Москва	Создание сетей на базе оборудования Cisco: Ускоренный курс	7-11 ноября
FIREWALL v.2.0	Москва	Внедрение межсетевых экранов Cisco ASA v.2.0	7-11 ноября

АВТОРИЗОВАННЫЕ КУРСЫ MICROSOFT

Ваши гарантированные инвестиции в развитие бизнеса и карьеры! Используются только авторизованные методики обучения. Для корпоративных клиентов доступны бесплатные курсы на основе программы Software Assurance.

Microsoft — мировой лидер в разработке программного обеспечения и интернет-технологий для персональных компьютеров и серверов. Плодотворное и долгосрочное сотрудничество Учебного центра Softline с корпорацией Microsoft является отличным доказательством того, что курсы по этому направлению соответствуют всем требованиям производителя ПО.

- Учебный центр Softline много лет обладает наивысшим статусом Microsoft Gold Learning Partner.
- Более 200 курсов по самым различным направлениям Microsoft, как для ИТ-специалистов, так и для ИТ-пользователей. Специализированные тренинги (технические и тренинги продаж) для партнеров Microsoft.

У вас есть возможность пройти курсы по новым продуктам Microsoft.

Курсы Microsoft SQL Server 2016

Код	Название курса	Дни	Ак. час	Очное обучение	Веб-класс
20761 A	Создание запросов данных при помощи Transact-SQL	3	24	21 000 руб.	18 900 руб.
20765 A	Обеспечение баз данных SQL	3	24	21 000 руб.	18 900 руб.
10985 A	Введение в базы данных SQL	3	24	21 000 руб.	18 900 руб.
10986 A	Обновление навыков до SQL Server 2016	3	24	21 000 руб.	18 900 руб.
10987 A	Настройка производительности и оптимизация баз данных SQL	4	32	27 000 руб.	24 300 руб.
10990 A	Анализ данных при помощи SQL Server Reporting Services	3	24	21 000 руб.	18 900 руб.
20762 A	Разработка баз данных SQL	4	32	27 000 руб.	24 300 руб.
20764 A	Администрирование инфраструктуры баз данных SQL	5	40	32 200 руб.	28 980 руб.
20767 A	Внедрение хранилищ данных SQL	4	32	27 000 руб.	24 300 руб.
10989 A	Анализ данных при помощи Power BI	2	16	14 900 руб.	13 410 руб.
20768 A	Разработка моделей данных SQL	3	24	21 000 руб.	18 900 руб.

Windows Server 2016

Код	Название курса	Дни	Ак. час	Очное обучение	Веб-класс
10983 A	Обновление навыков до Windows Server 2016	5	40	32 200 руб.	28 980 руб.

Exchange Server 2016

Код	Название курса	Дни	Ак. час	Очное обучение	Веб-класс
20345-1A	Администрирование 2016 Microsoft Exchange Server	5	40	32 000 руб.	28 800 руб.
20345-2A	Проектирование и развертывание Microsoft Exchange Server 2016	5	40	32 000 руб.	28 800 руб.



VEEAM. ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ, РАЗРАБОТАННЫЕ СПЕЦИАЛЬНО ДЛЯ ВИРТУАЛЬНОЙ СРЕДЫ И ОБЛАКА

Veeam предлагает эффективные, простые и доступные по цене решения, которые разработаны специально для виртуальной среды и облака. В Учебном центре доступен курс «Сертифицированный инженер Veeam (V.9)».

VMCE9: Сертифицированный инженер Veeam v9

Данный глубокий технический тренинг создан для обучения инженеров проектированию, внедрению и оптимизации программных решений Veeam. Курс будет одинаково полезен как техническим консультантам и системным администраторам, так и экспертам по Veeam, способным максимизировать выгоду для бизнеса. Курс объединяет в себе экспертные инструкции с интенсивными практическими упражнениями для предоставления максимального количества знаний всем категориям слушателей.

Расписание курса VMCE9 в Учебном центре Softline

Название курса	Формат	Место проведения	Дата	Стоимость
VMCE9				
Сертифицированный инженер Veeam (V.9)	очно	Казань	26–28 сентября 2016	49 000 руб.
	дист.	дист.	31 октября–2 ноября 2016	44 100 руб.
	очно	Москва	31 октября–2 ноября 2016	49 000 руб.



УЧЕБНЫЙ ЦЕНТР SOFTLINE ПОЛУЧИЛ СТАТУС АВТОРИЗОВАННОГО УЧЕБНОГО ЦЕНТРА ITIL

Теперь Учебный центр Softline имеет право читать в авторизованном формате курсы по двум направлениям: ITIL Foundation и ITIL OSA.

Курс ITIL Foundation посвящен основным понятиям и принципам, на которых строится управление современной службой ИТ, взаимоотношения с бизнесом и поставщиками, управление качеством предоставляемых ИТ-услуг.

Курс ITIL OSA (Операционная поддержка и анализ) ориентирован на получение глубоких знаний о том, как лучше организовать службу поддержки и оперативно реагировать на инциденты и запросы, а также управлять ожиданиями пользователей. Слушатели ознакомятся с методами управления инцидентами, проблемами, доступом и уровнем услуг.

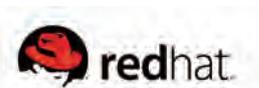
Ближайшие курсы ITIL в Учебном центре Softline:

Название курса	Дата	Город/Формат
ITIL Foundation	12 сентября 2016	Москва
ITIL OSA	15 сентября 2016	Москва
ITIL Foundation	19 сентября 2016	Дистанционно
ITIL Foundation	26 сентября 2016	Владивосток
ITIL Foundation	26 сентября 2016	Новосибирск
ITIL Foundation	3 октября 2016	Хабаровск
ITIL Foundation	10 октября 2016	Казань
ITIL OSA	10 октября 2016	Хабаровск
ITIL Foundation	24 октября 2016	Санкт-Петербург



Более полную информацию по курсам, направлениям и расписанию вы можете получить на нашем сайте: www.edu.softline.ru

Центры тестирования и сертификация ИТ-специалистов



На базе Учебного центра Softline действуют центры тестирования Prometric, Autodesk, Red Hat, «Лаборатории Касперского», Pearson VUE. Наши центры тестирования позволяют ИТ-специалистам пройти сертификацию и получить официальный статус сертифицированного специалиста по любым направлениям.

Вы можете воспользоваться системой предварительной оценки персонала на соответствие знаний и навыков в области ИТ – Alltests.

Внимание: цены на экзамены могут меняться, просьба уточнять актуальные цены у менеджеров!

Тестирование можно пройти в следующих городах РФ: Москва, Санкт-Петербург, Екатеринбург, Казань, Нижний Новгород, Новосибирск, Ростов-на-Дону, Самара, Уфа.

Тестирование проводится каждый день. Время проведения экзаменационного теста необходимо согласовывать с администратором Центра тестирования.



Подробная информация: <http://edu.softline.ru/certification>

Экзамены со скидкой!

Купите 10 экзаменов Microsoft — получите скидку 5%

Сроки проведения акции (реализации экзаменов) — 01.10.2016–31.03.2017 г.

Срок покупки экзаменов — до 1 декабря 2016 г., активации — до 31 марта 2017 г.

Приобретите 5 тестов «Лаборатории Касперского» со скидкой 5%

Сроки проведения акции, а также покупки

и активации экзаменов — 01.10.2016–31.12.2016 г.



Вкладывайтесь в знания

Мы живем в кризисное время. Но в любой кризис важно сохранять активную рыночную позицию. А повысить эффективность бизнеса можно только при помощи ИТ-технологий.

Не экономьте на ИТ!

Предложение Учебного центра Softline приходится как нельзя кстати.

УЦ Softline предлагает авторизованные курсы Check Point в Москве по цене от 40 000 рублей!

Качественное вендорское обучение по направлению Check Point в нашем Учебном центре Softline сейчас идет по небывало низким ценам.



Подробности вы найдете здесь: <http://edu.softline.ru/vendors/check-point>



Звоните: +7 (495) 228-47-07

Курсы Check Point

Обеспечивают теоретические знания и практические навыки, необходимые для настройки программных блейдов (Software Blades) версии R77.30, включая шлюз безопасности, управление политиками безопасности, систему регистрации и мониторинга, аутентификацию пользователей и систему построения VPN. Во время прохождения обучения слушатели будут учиться настраивать политику безопасности, строить защищенный канал передачи данных через интернет и настраивать работу с учетными записями пользователей.

Целевая аудитория

Курсы Check Point рекомендованы и будут полезны тем, кто занимается поддержкой, инсталляцией или администрированием систем безопасности на основе Check Point Software Blades – системным администраторам, системным инженерам, менеджерам по безопасности, сетевым инженерам, а также тем, кто собирается сдавать экзамены на сертификат CCSA и CCSE.

Курсы дают слушателям все необходимые навыки для достижения наибольшей отдачи от средств, вложенных в решения сетевой безопасности на базе продуктов Check Point.

Чтобы подготовиться с начального уровня до мастера по продуктам Check Point, рекомендуется прослушать три основных семинара.

- Управление безопасностью средствами Check Point 2013 (Check Point Security Administration 2013).
- Проектирование безопасности средствами Check Point 2013 (Check Point Security Engineering 2013).
- Мастер безопасности Check Point.

НОВЫЙ СТАТУС!

УЦ Softline получил статус «Авторизованный учебный центр АСКОН» по специализации «Система трехмерного моделирования КОМПАС-3D (машиностроительная конфигурация), универсальная система автоматизированного проектирования КОМПАС-График (машиностроительная конфигурация)».



Приобретены обновления по следующим курсам:

Код М2
Название курса
Трехмерное моделирование деталей и сборочных единиц в системе КОМПАС-3D
Дни
4
Ак. час
32
Стоимость очного обучения, руб.
14 665

Код М3
Название курса
Проектирование и разработка конструкторской документации в системе КОМПАС-График
Дни
4
Ак. час
32
Стоимость очного обучения, руб.
14 665



НОВЫЕ КУРСЫ CISCO ЛИНЕЙКИ CCNP WIRELESS

В Учебном центре Softline появились новые курсы по направлению CCNP Wireless:

- WIDEPLOY,
- WISECURE,
- WITSHOT.

Курс «Развертывание корпоративных беспроводных сетей Cisco» (WIDEPLOY) готовит сетевых специалистов при помощи информации о развертывании беспроводных сетей с использованием контроллеров Cisco, политик унифицированных архитектур коммутации и передового опыта, а также корректного применения мобильных стандартов и надлежащей настройки всех компонентов беспроводной сети. Лабораторные работы курса позволят слушателям получить полное понимание настройки новой Cisco 8.0, Prime Infrastructure 2.2 и возможностей Services Engine 8.0.

Продолжительность — 5 дней.

Стоимость — 125 500 руб.

Курс «Обеспечение безопасности корпоративных беспроводных сетей Cisco» (WISECURE) предоставляет слушателям инструкции по применению безопасной архитектуры Wi-Fi за счет комплексной настройки компонентов беспроводной сети Cisco. В курсе используются практические лабораторные работы для отработки полученных знаний. Материалы курса включают в себя Cisco AireOS 8.0, Prime Infrastructure версии 2.2 и возможности Identity Services Engine версии 1.3.

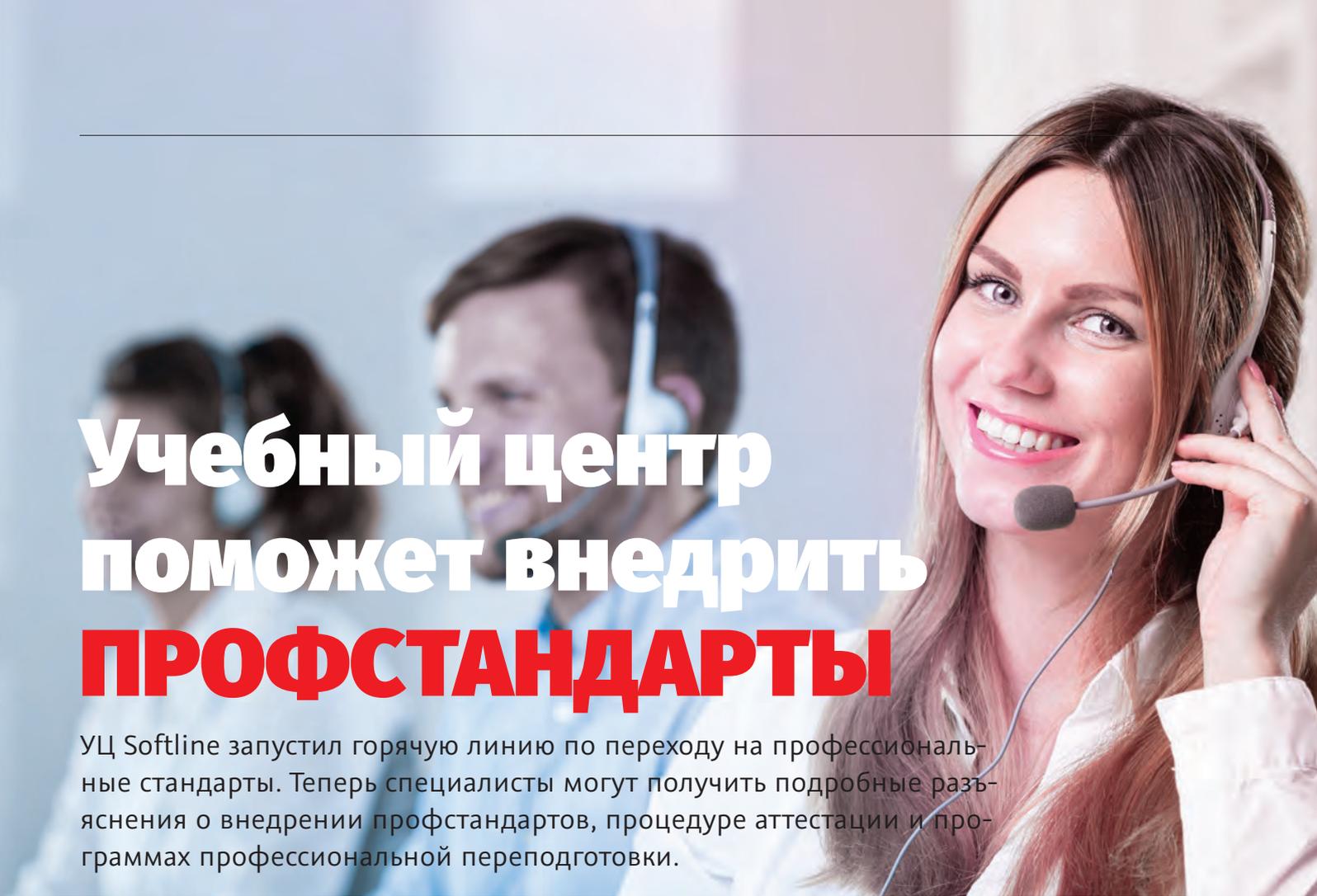
Продолжительность — 5 дней.

Стоимость — 125 500 руб.

Курс «Устранение неисправностей корпоративных беспроводных сетей Cisco» (WITSHOOT) предоставляет сетевым специалистам знания и навыки устранения неисправностей и оптимизации корпоративных беспроводных инфраструктур и связанных служб. Также в курсе рассматриваются инструменты и методологии, необходимые для определения и устранения ошибок клиентских подключений, производительности и RF.

Продолжительность — 3 дня.

Стоимость — 95 000 руб.



Учебный центр поможет внедрить ПРОФСТАНДАРТЫ

УЦ Softline запустил горячую линию по переходу на профессиональные стандарты. Теперь специалисты могут получить подробные разъяснения о внедрении профстандартов, процедуре аттестации и программах профессиональной переподготовки.



«Внедрение профессиональных стандартов — достаточно трудоемкий процесс. Мы обобщили накопленную экспертизу и запустили горячую линию, чтобы сделать переход к использованию профстандартов максимально комфортным для работодателей и работников, — предоставить им единую точку входа для разрешения возникающих вопросов. Мы уверены, что комплексный подход к консультированию, включающий работу колл-центра, помощь экспертов, предоставление рекомендаций по программам дополнительного образования, позволит компаниям формировать более эффективные стратегии управления и обучения кадров в соответствии с требованиями законодательства».

Ольга Белоусова
директор по продажам Учебного
центра Softline

Профессиональные стандарты — это документы, в которых описаны квалификации сотрудника, необходимые для осуществления какой-либо деятельности. С 1 июля 2016 года они стали обязательными к внедрению, в первую очередь, в госкорпорациях. Учебный центр Softline организовал горячую линию для оказания консультативной помощи по вопросам их применения, внедрения и аттестации специалистов. Также консультации будут проводиться и по профстандартам в области управления персоналом (Human Resources, HR).

Непрерывно и бесплатно

Техническую базу для организации и приема звонков обеспечила компания Tekmi, входящая в ГК Softline, предоставив выделенную телефонную линию на базе виртуальной АТС. Звонки поступают на бесплатный многоканальный номер 8-800-505-05-07, что гарантирует непрерывную обработку запросов. Горячая линия ведет прием звонков со всей России и работает в будние дни по московскому времени. Кроме того, специалисты компаний могут задать вопросы в круглосуточ-

ном режиме, заполнив специальную форму на сайте УЦ Softline.

Проконсультируем и направим

Работа горячей линии организована так, чтобы работники и работодатели могли получить максимально полную информацию о профстандартах в сфере ИТ и HR. Операторы колл-центра проводят первичную обработку звонков, предоставляют бесплатные методические материалы. Звонок может быть переадресован экспертам. Они, в свою очередь, проконсультируют по вопросам нормативных документов, рисков и санкций, процессу обучения сотрудников, проведению тестирования т.д. В состав экспертов входят инженеры и преподаватели УЦ Softline, которые принимали участие в разработке профессиональных стандартов.

Быстро!

Время отклика на входящий звонок — одна минута, максимальное время, в течение которого формируется ответ на запрос с привлечением экспертов и менеджеров — порядка шести минут.

ЭВОЛЮЦИЯ БЛЕЙД-СИСТЕМ И FLEX SYSTEM LENOVO



В настоящее время компания Lenovo разрабатывает и внедряет новые модули для созданной компанией IBM нового поколения блейд-систем под названием Flex System. Структура Flex System состоит из тех же компонентов, что и классическая блейд-система.

Пионером в блейд-технологиях стала созданная выходцами из Compaq Computers компания RLX Technologies, которая к 2000 году разработала соответствующую архитектуру и выпустила первую подобную систему, где 24 блейд-сервера помещались в шасси размером всего 3U.

Это был прорыв, и уже через пару лет блейд-системы выпускали как лидеры серверного рынка (Compaq, IBM, Dell, HP, Sun Microsystems, Fujitsu Siemens, SGI etc.), так и визионеры, сделавшие ставку именно на блейды (Egenera, Verari Systems и сама RLX). В дополнение к этому списку была еще блейд-продукция Supermicro для локальных сборщиков. Наибольшая (до 70%) доля на рынке на то время принадлежала компаниям IBM и HP. Но рынок ИТ растет бурно и постоянно меняется. Мелкие компании и стартапы обычно поглощаются крупными компаниями. Однако некоторые из них растут, развиваются и сами становятся законодателями мод или объединяются в консорциумы, в которых может произойти переход на другие технологии и/или сворачивание выпуска когда-то культовых продуктов. Иногда так происходят знаковые события (покупка RLX в 2005 году или переход Egenera под знамена Fujitsu Siemens). Но самой масштабной сделкой все равно остается покупка компанией Lenovo в 2014 году всего серверного бизнеса на платформе x86 у компании IBM. Под логотип Lenovo перешли инженерные центры разработок с самими инженерами, фабрики по производству и логистические центры вместе со всем персоналом. В результате этой операции Lenovo немедленно вышла в лидеры по производству и разработке блейд-систем.

Шасси

Классическое высотой 10U, вмещающее до 14 вычислительных узлов. В отличие от своих предшественников — серверов BladeCenter, — во Flex System была полностью переработана система охлаждения и питания, что позволило достигнуть отличных показателей в соотношении эффективности с уровнем шума.

Carrier-Grade шасси, высотой в 11U, спроектированное инженерами Lenovo. Предназначено оно для телекоммуникационной отрасли, где требования к оборудованию особо жесткие. Включает пылевые фильтры и блоки питания на 48В постоянного тока. Шасси протестировано для работы в условиях вибрации (в сейсмоактивных зонах) и может без ущерба для производительности продолжать работу до 96 часов кряду при температуре от -5°C до 55°C .

Вычислительные узлы или блейд-серверы

Их выбор широк: от двухsocketного сервера x240 M5 на процессорах Xeон по 18 ядер каждый и 24 слотами памяти (32ГБ*24=768ГБ) до первой в мире восьмисocketной блейд-системы, построенной по технологии X6. Портфолио X6 Flex System сейчас состоит из трех серверов Lenovo: двухsocketная система x280 X6, четырехsocketная x440X6 и восьмисocketная x880 X6. В них 24 слота памяти на процессор позволяют получить 1,5ТБ/6ТБ/12ТБ RAM на сервер в зависимости от модели. А это означает скоростную обработку повышенного числа виртуальных машин или полную загрузку в память объемных баз данных. Причем если ставить емкие модули LRDIMM TruDDR4 на 1.2V, то потреблять

они будут на 45% меньше, чем модули 1.5V DDR3. Также в серверах X6 Flex System впервые для блейдов были применены технологии eXFlashDIMMs. Если коротко, то это когда быстрые SSD-накопители подключены не к RAID-контроллеру, а к еще более быстрой шине памяти, и работают они с процессором напрямую. Объем такой eXFlash-памяти на сервер — до 9.6ТБ.

а также обеспечивает диагностику и мониторинг неисправностей на физическом уровне).

- Второй — это управление отдельно взятым сервером посредством его встроенного сервисного сопроцессора Integrated Management Module II (IMM2). Главное особенностью здесь является система предсказания сбоев, которая анализи-



Коммутаторы масштабируемые, то есть для увеличения числа доступных портов достаточно ввести код лицензии, получив до 46 портов в шасси. Основное отличие — сетевая инфраструктура образует плоскую сеть и является одним большим логическим коммутатором.

Шасси FlexSystem позволяет одновременно использовать два типа процессоров: Intel Xeon и IBM Power P7 для узлов на базе RISC-серверов p260. Это позволяет сохранить наработки заказчиков, сделанные на RISC-платформе IBM.

Модули расширения

Для увеличения возможностей вычислительных узлов на платформе x86 есть специальные модули расширения, позволяющие нарастить дисковое пространство или добавить PCI-устройства. Так, PCIe Expansion Node позволяет подключать стандартные PCI-адаптеры (до четырех на систему), а Storage Expansion Node расширяет дисковую подсистему до 12 дисков формата 2,5”.

Сетевая инфраструктура

Доступны все типы коммутаторов Ethernet (1Гб, 10Гб или 40Гб) уровня L2 и L3, конвергентные коммутаторы 10Гб, FC SAN (8Гб или 16Гб), FCoE, iSCSI. Также возможно использование патч-панели и коммутатора InfiniBand 56Гб/с. Посредством модуля B22 Fabric Extender можно подключиться к инфраструктуре на Cisco Nexus. Шасси спроектировано для высокой скорости обмена данными — до 100Гб/сек.

Модули управления

Есть три типа управления в FlexSystem.

- Первый (Chassis Management Module — CMM) представляет модуль управления самим шасси (его питанием, охлаждением, инициализацией и первичной настройкой вычислительных узлов и коммутаторов,

рует пять параметров и с большой вероятностью предупреждает, когда может выйти из строя что-либо в системе (диск, память и т.д.).

- Третий (самый масштабный) — посредством специальных модулей либо аппаратного обеспечения (Flex SystemManager — FSM), реализованного как специализированный блейд-сервер. Возможен также вариант с использованием виртуального модуля Lenovo XClarity.

Основные преимущества Flex-системы Lenovo над другими блейд-системами

Масштабирование мощности вычислений: от двух процессоров на 36 ядер до восьми процессоров, 144 ядер и 12 TB памяти в 192 слотах, причем максимальные показатели присущи серверам архитектуры X6 IBM.

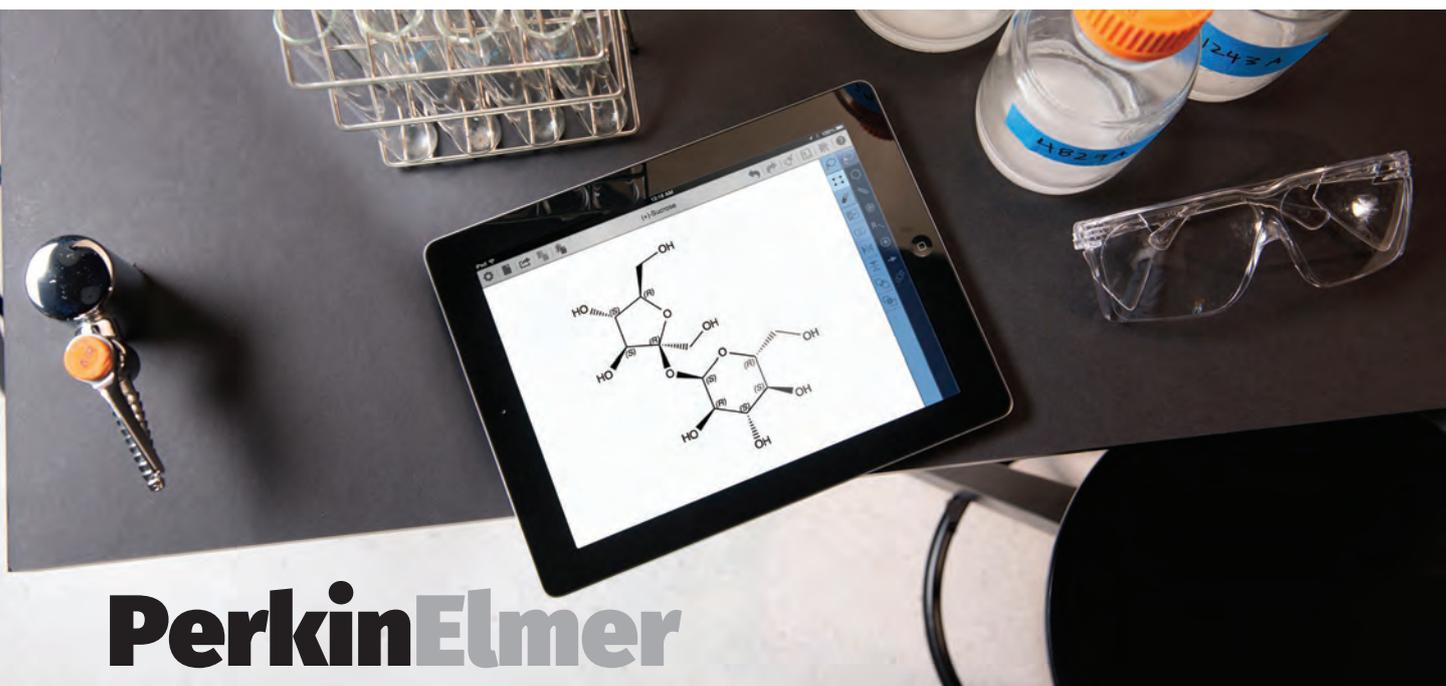
Применение передовых технологий для оперативной памяти, что позволяет потреблять на 45% меньше энергии при установке модулей памяти TruDDR4.

Возможность применять в одном шасси серверы на платформах x86 и RISC.

Гибкие возможности по установке флэш-накопителей: внутрь блейд-серверов вместо HDD и/или eXFlash DIMM вместо модулей памяти (это самые скоростные SSD); в блейд-модули расширения, соединенные с блейд-сервером по внутренней шине шасси.

Быстрота запуска новой блейд-системы с помощью набора шаблонов для автоматизированного разворачивания ПО или выхода в облако.

Эффективное управление через единую консоль — как всей блейд-инфраструктурой, так и обычными серверами, взаимодействующими с ней.



PerkinElmer

Решения для химии и биологии

С выходом 15 версии своего флагманского продукта ChemOffice (ранее выпускаемого компанией CambridgeSoft) специалисты PerkinElmer существенно изменили свою продуктовую линейку, предназначенную для автоматизации самых различных операций, с которыми исследователи-химики и биологи сталкиваются каждый день в процессе своей работы. В связи с этими изменениями специалисты компании Softline, являющейся партнером компании PerkinElmer на территории России и стран СНГ, подготовили обзор возможностей новых продуктов, чтобы помочь пользователям сориентироваться среди многочисленных возможностей различных программных продуктов.

Программное обеспечение компании PerkinElmer является лидером в своей области и используется более чем в 130 странах по всему миру. На сегодняшний день компания предлагает своим клиентам три основных продукта:

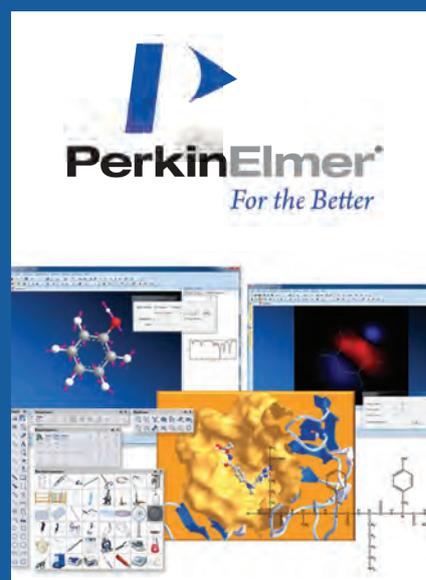
- **ChemDraw Prime** — многофункциональная, простая в освоении программа для визуализации атомов и молекул, которая позволяет быстро создавать высококачественные визуализации химических структур и реакций. ChemDraw Prime включает в себя калькулятор свойств, шаблоны для визуализации электрофореза, лабораторного оборудования и т.д.
- **ChemDraw Professional** — мощный инструмент для создания химических и биологических визуализаций, который позволяет осуществлять интеллектуаль-

ную обработку изображений, включая их использование для запросов в химических базах данных, например SciFinder®. ChemDraw Professional включает в себя все возможности ChemDraw Prime и дополняет их инструментами для работы с биополимерами, BioDraw, ChemDraw for Excel, ChemFinder Standard и ChemScript.

- **ChemOffice Professional** — интеллектуальная программная среда для сбора, хранения, анализа и обмена данными о химических реакциях, смесях, материалах и их свойствах. ChemOffice Professional включает в себя весь функционал ChemDraw Professional и Chem3D. Это позволяет ученым целенаправленно проводить исследования, анализировать результаты и сопоставлять биологические процессы с химическими реакциями и структурами.

Интеграция с SciFinder и доступ с iPad

С ChemDraw и ChemOffice пользователь получает возможность осуществлять поиск в базе SciFinder® по созданному им изображению. В готовой модели какой-либо реакции необходимо выбрать интересующий компонент и щелкнуть на иконку поиска. После подтверждения параметров поиска, результаты из базы SciFinder® появляются практически мгновенно. Больше нет необходимости переносить модели из одного приложения в другое. Поиск также поддерживает инструменты фильтрации и анализа полученной информации. Данная опция позволяет пользователям экономить время и не отвлекаться от своей основной работы. С помощью встроенного поиска стало возможным быстро находить аналоги веществ, структуры, в которые они входят, а также пути их синтеза. Пользователи получили возможность использовать мобильную версию ChemDraw for iPad, что позволяет создавать и обмениваться моделями химических структур и реакций с любого устройства при наличии доступа к интернету. Также предусмотрена интеграция с Dropbox для хранения и обмена файлами через облако.



ChemOffice Professional

Если говорить о функционале ChemOffice Professional более развернуто, то прежде всего следует выделить Chem3D — модуль, позволяющий создавать трехмерные модели молекул, соединений и рассчитывать их свойства, форму, а также максимизировать те или иные характеристики. Данный модуль также содержит интерфейс GAMESS и инструменты для связи с другими программными продуктами, включая Gaussian, MOPAC, CONFLEX® и AutoDock. Помимо этого, в состав продукта входит модуль CDSL для работы с созданными моделями через iPad, а также модуль ChemScript, который позволяет автоматизировать некоторые этапы работы с помощью написания скриптов. В новый ChemOffice входит функционал ChemDraw for Excel, который обеспечивает взаимодействие с MS Excel так, что исследователи могут использовать все доступные инструменты манипулирования и сортировки данных для выявления, например, зависимости активности вещества от структуры. ChemOffice широко используется в исследовательских лабораториях по всему миру, так как позволяет быстро и легко визуализировать молекулы, реакции и органические элементы. Их можно использовать в различных электронных документах, осуществлять поиск по встроенным химическим базам данных, включая SciFinder®, генерировать точные названия химических структур и предсказывать некоторые их свойства.

ChemOffice Professional обеспечивает тесную интеграцию между химическими и биологическими областями знаний, тем самым позволяя проводить междисциплинарные исследования, а различным научным коллективам легко

обмениваться документами и данными, повышая эффективность своей работы. Продукт также содержит специализированное меню для работы с биополимерами, включая D- и L-аминокислоты, бета-аминокислоты, ДНК и РНК. В системе предусмотрены механизмы автоматической корректировки ориентации диаграмм и расположения в них молекул и атомов. Среди свойств, которые пользователь может предсказывать с помощью встроенных инструментов, можно выделить кислотную диссоциацию, распределение и растворимость в воде.

ChemDraw Professional

ChemDraw Professional позволяет быстро создавать точные визуализации высокого качества, включая пептидные и нуклеотидные последовательности, импортировать данные из интернета или текстовых файлов, а также визуализировать клетки с помощью библиотеки биологических элементов. В систему встроены шаблоны для создания визуализаций в соответствии с требованиями ведущих научно-химических журналов. Трехмерные модели позволяют исследовать свойства и форму созданных структур, а также анализировать зависимость активности вещества от структуры, свойства кластеров и различные статистические данные с помощью гистограмм, логарифмических графиков, древовидных диаграмм и др. При анализе химических реакций автоматически осуществляется пересчет стехиометрических данных и других физических свойств. Экспорт созданных моделей возможен как в MS Word и MS PowerPoint, так и в классические графические форматы — TIFF, JPG, SVG, BMP и EPS.



Обращайтесь
к техническому
специалисту
Максиму Сахарову.



Maxim.Sakharov@
softlinegroup.com



+7 (495) 232-00-23
доб. 1632

Платформа MAPS от компании Scienomics

Современная масштабируемая система для молекулярного моделирования



Исследовательские компании выпускают все больше высокотехнологичных продуктов, вследствие чего возникает острая необходимость в глубоком понимании структурных свойств материалов, вовлеченных в процессы производства. Платформа MAPS (Material Process and Simulations) позволяет исследователям и инженерам строить, визуализировать и проводить анализ различных молекулярных структур.

Платформа предлагает пользователям полный набор возможностей и инструментов, которые могут понадобиться при проведении работ в области материаловедения. Спектр возможностей системы включает в себя функционал для трехмерной визуализации, эскизирования молекул, инструменты для построения кристаллов, поверхностей, полимеров, калькулятор для расчета основных характеристик, возможности экспорта в видеоформаты, создания анимации и написания скриптов на языке Python. Специалисты компании Scienomics специализируются в четырех основных областях материаловедения: нанотехнологии, химическая промышленность, композитные материалы и «зеленые» технологии.

Диффузия в упаковочных материалах

Полимеры часто используются для производства упаковочных материалов. В связи с этим они должны предотвращать диффузию небольших молекул, например, молекул воды внутрь или наружу. Для рас-

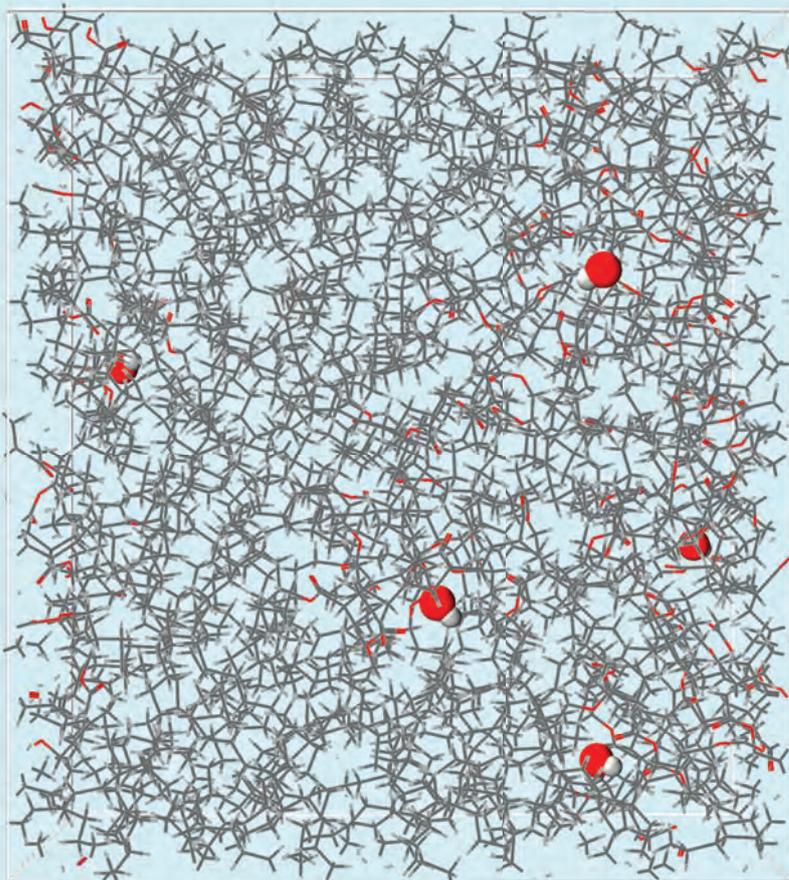
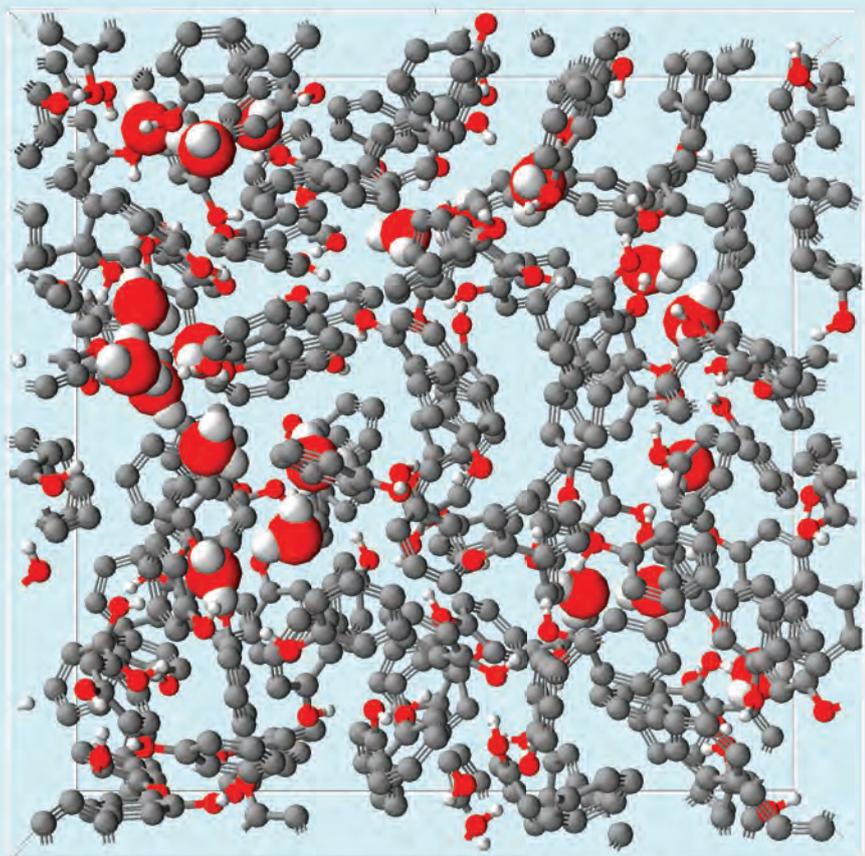


Рис 1. Результаты моделирования при $T = 298$ К пяти молекул воды в полимерной матрице (красные атомы кислорода).



чета коэффициента диффузии малых молекул через матрицу полимеров используют молекулярное моделирование.

В нашем случае рассматривается диффузия воды и метанола сквозь полимерную матрицу, состоящую из смеси полиэтилена и этилбутилакрилата. Диффузию малых молекул можно смоделировать с помощью анализа динамики молекул. Обычно движение молекул характеризуется коэффициентом диффузии, который отображает насколько далеко продвинется молекула за определенное время. Для изучения диффузии воды и метанола в матрице полимеров из 100 мономеров полиэтилена и блока из 20 мономеров этилбутилакрилата и 80 мономеров этилена, была построена модель с помощью платформы MAPS. Пять цепочек каждого полимера использовались для создания пробного объема.

В качестве первого шага моделирования матрица полимеров была оптимизирована и очищена от потенциальных контактов между молекулами, которые могли образоваться после генерации. Затем для

Рис 2. Смесь фенола и воды в жидком состоянии при температуре 420 К. Молекулы фенола обозначены серым цветом.

уравновешивания матрицы было проведено моделирование в течение 200 пс при нормальных условиях. После 75 пс система достигла своей средней плотности 0.8 г/см³, которая осталась постоянной. Затем с помощью платформы MAPS в матрицу были помещены 5 молекул воды или метанола. Далее моделирование при нормальных условиях давления и трех разных температурах (298 323 373 К) было проведено в течение 5 нс. Результаты моделирования были проанализированы исходя из расчета среднего квадратичного смещения молекул воды и метанола.

Так как атомы водорода в молекулах воды могут образовывать связи между собой, то эксперимент был проведен повторно для случая, когда в качестве начальных условий был построен кластер из водяных молекул вместо отдельных молекул. Кластер был вручную размещен в полости полимерной матрицы. Моделирование было так же проведено на протяжении 5 нс. Полученные усредненные коэффициенты диффузии практически совпали с экспериментальными. В то же время различные молекулы проделали различный путь, это связано с тем, что вокруг некоторых молекул цепочки полимеров были весьма разрежены, в то время как другие были заперты внутри так называемых «карманов» и по сути колебались вокруг положения равновесия.

Расчет термодинамических свойств смесей воды и фенола

В большинстве случаев в химической промышленности после проведения какой-либо реакции, итоговое вещество не обладает необходимой чистотой. Для достижения высокого качества продуктов важно использовать разделяющие методы. Традиционно используется дистилляция, извлечение, абсорбция, кристаллизация и т.д.

В частности, удаление фенола — очень важный этап при переработке

использованной воды. Фенол является одним из основных элементов в химической промышленности. Средняя концентрация фенола в поступаемом сырье варьируется от 3 до 10% в зависимости от температуры.

Численные методы, такие как Монте-Карло и термодинамические модели, могут помочь в расчете термодинамических свойств промышленных химикатов, таких как фенол и его смеси с водой. Моделирование методом Монте-Карло в избранных и изотермических системах позволяет напрямую осуществлять расчет свойств в зависимости от числа частиц, давления и температуры, таких как равновесие в системе «жидкость-пар».

Уравнения фазовых состояний часто используются для решения многих задач в химической промышленности. Их основное преимущество заключается в том, что по сравнению с молекулярным моделированием, они считаются быстрее и требуют меньше вычислительных ресурсов. Поэтому этот метод является предпочтительным, в случае, если необходим расчет для большого объема данных в широком диапазоне температур и давлений. В данном примере использовалась Statistical Associated Fluid Theory (SAFT) и ее модификация Perturbed Chain-SAFT (PC-SAFT). PC-SAFT может эффективно использоваться в сочетании с методом Монте-Карло так, что всего несколько параметров, полученных с помощью МК в сочетании с PC-SAFT, позволят покрыть все фазовое пространство и получить результаты с высокой точностью.

Оба метода реализованы в платформе MAPS, что облегчает их совместное использование. Комбинация этих методов позволила предсказать фазовое равновесие смеси воды и фенола и получить более точные результаты, по сравнению с использованием только

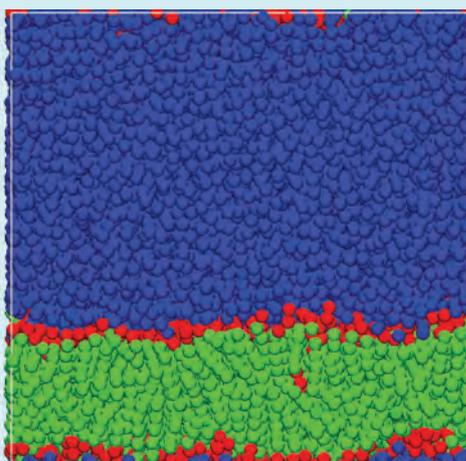


Рис.3. При уровне концентрации в водных растворах фосфолипидов, спонтанно образуются липидные бислои. На рисунке изображен бислой.

уравнений состояния. Данная информация важна для промышленного процесса переработки использованной воды и выделения фенола после химических реакций.

Высвобождение лекарственного средства через мицеллы

В последнее время мицеллы (лекарственные наночастицы) активно изучались как возможные переносчики для плохо растворимых активных лекарственных компонентов, в настоящее время открытыми остаются вопросы их стабильности и путей поглощения. Эти вопросы требуют дальнейшего изучения для создания мицелл нового поколения.

Почти одна треть новых лекарственных препаратов не растворяется в воде. Для доставки этих веществ по назначению используются мицеллы. Помимо повышения растворимости, препараты, переносимые на мицеллах, обладают еще рядом важных свойств – они препятствуют адгезии с другими смесями и замедляют вывод полезных веществ из организма.

Мицеллы легко смоделировать, так как они имеют необходимый наноскопический размер, а их способность переносить активные вещества, можно увеличить за счет комбинаций различных методов взаимодействия, таких как водородное и электростатическое связывание.

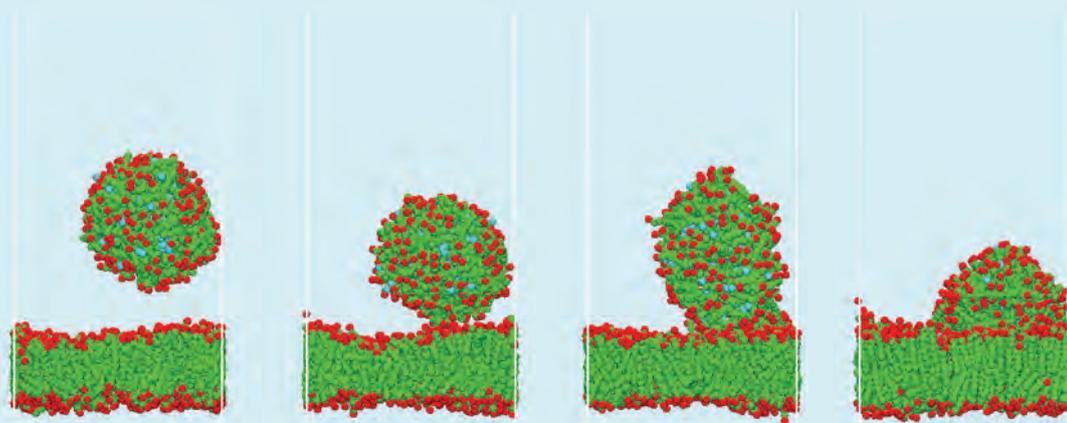


Рис 4. Фосфолипидная мицелла интегрируется в бислой и активный элемент высвобождается в гидрофобную внутреннюю среду бислоя

Также мало известно о взаимодействии мицелл с клетками, что представляет собой фундаментальные основы химиотерапии и поэтому исследования в этой области должны постоянно продолжаться для разработки более эффективных мицелл следующего поколения.

Еще одна интересная задача заключается в моделировании контакта мицеллы с липидным бислоем, так как данный тип контакта лежит в основе процесса высвобождения лекарственного препарата из мицеллы, но эта задача до сих пор плохо исследована. Что происходит, когда мицелла контактирует с оболочкой клетки? На рисунке 4 представлена серия снимков, моделирующих это событие. Видно, что фосфолипидная мицелла интегрируется в бислой и активный элемент высвобождается в гидрофобную внутреннюю среду бислоя.

Многие из мицелл, используемые для переноса лекарственного препарата, основаны на полимерах или искусственных фосфолипидах. Мицеллы используются в коммерческих целях для использования гидрофобного эффекта для загрузки плохо растворимых лекарственных препаратов и активных компонентов. Чтобы максимизировать нагрузочную способность мицелл, необходимо изучить способность к смешиванию между полимерами и активными компонентами, а также стабильность мицелл, и их взаимодействие с клеточными мембранами. Моделирование в мезомасштабе позволяет получить ответы на многие из поставленных вопросов и проводить эксперименты, результатом которых являются наиболее эффективные процессы высвобождения и выбор оптимальных материалов.



Нужны подробности?

Обращайтесь к техническому специалисту Максиму Сахарову.

@ **Maxim.Sakharov@softlinegroup.com**

☎ **+7 (495) 232-00-23 доб. 1632**

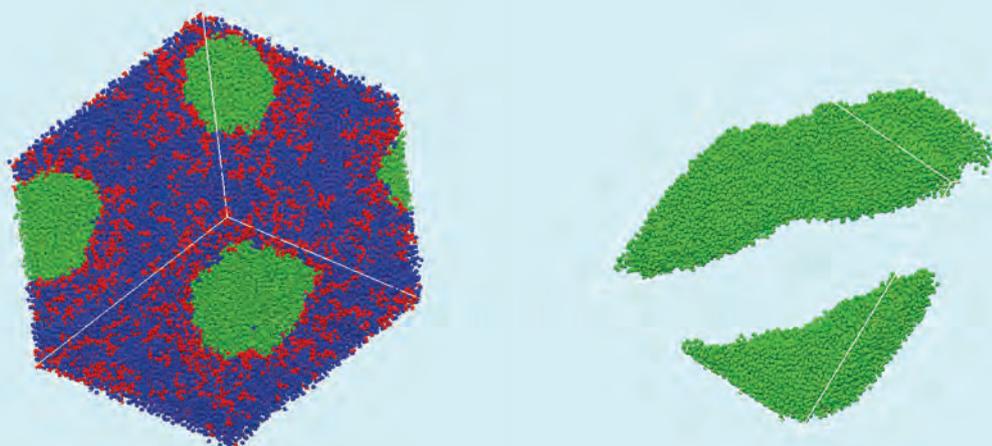


Рис 5. Плурионировый полимером с водоотталкивающими сегментами. Система состоит из 125 000 частиц, в кубическом объеме с ребром 23 нм. Моделирование проводилось в течение 3 мс.



Cisco WebEx

Сервисы для проведения веб-
и видеоконференций разного формата



Cisco WebEx

Простота в использовании, несколько сценариев подключения, все необходимые инструменты для совместной работы, а также высокое качество передачи аудио- и видеопотоков - это наиболее важные преимущества сервисов Cisco WebEx.

- Cisco WebEx Meeting Center - персональные встречи и совещания
- Cisco WebEx Event Center - большие конференции и вебинары
- Cisco WebEx Training Center - инструмент для дистанционного обучения
- Cisco WebEx Support Center - техническая и консультационная поддержка пользователей

WebEx Meeting Center

Персональные встречи и совещания

Решение Cisco WebEx Meeting Center помогает обмениваться документами, презентациями и приложениями в любое время и в любом месте.

СОВМЕСТНАЯ РАБОТА С ДОКУМЕНТАМИ, ПРИЛОЖЕНИЯМИ И РАБОЧИМ СТОЛОМ

Удаленные участники могут в режиме реального времени совместно просматривать контент. Возможна трансляция изображения рабочего стола с последующим комментированием.

РАБОТА С ИНТЕРАКТИВНЫМИ МУЛЬТИМЕДИЙНЫМИ МАТЕРИАЛАМИ

Для создания наглядных презентаций можно использовать файлы PowerPoint, флэш-анимацию, аудио- и видеозаписи.

ИНТЕГРИРОВАННОЕ ВИДЕО

Сервис предлагает возможность одновременного просмотра видеоизображения количеству участников до семи человек в формате высокой четкости с разрешением HD. Видеоизображение автоматически переключается на выступающего участника, что создает эффект присутствия. При необходимости можно зафиксировать видеоизображение на одном говорящем. Для максимально четкого просмотра можно выбрать полноэкранный режим, позволяющий видеть выступающего в формате высокой четкости с разрешением 720p.

ВСТРОЕННЫЕ АУДИОСРЕДСТВА

Расширить возможности интерактивного общения можно с помощью встроенных аудиосредств Cisco WebEx. Участники могут подключиться к аудио по интернету или с помощью телефона. Пользователям доступны номера по всему миру.

ПЛАВАЮЩИЕ ПАНЕЛИ

Транслируя участникам полноэкранные изображения, можно управлять ходом конференции «за кулисами».

ЗАПИСЬ, РЕДАКТИРОВАНИЕ И ВОСПРОИЗВЕДЕНИЕ КОНФЕРЕНЦИИ

Конференции и приложения можно записывать для последующего использования в качестве справочного, учебного или демонстрационного материала.

ПАКЕТ ДЛЯ ИНТЕГРАЦИИ С РАБОЧИМ СТОЛОМ

Конференции можно мгновенно запускать из Microsoft Office, Microsoft Outlook, Lotus Notes и ряда решений.

ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

Максимально расширить круг участников помогает поддержка WebEx во всех распространенных операционных системах и платформах. К ним относятся Windows, Mac, Linux, Solaris, а также мобильные устройства.

ДОСТУП К КОНФЕРЕНЦИИ ОДНИМ ЩЕЛЧКОМ МЫШИ

Запустив конференцию, можно быстро отправлять приглашения участникам с рабочего стола, панели задач или из избранных приложений.

ПРОСТОЙ МЕХАНИЗМ ПРИГЛАШЕНИЙ

Разослать приглашения и напоминания можно с помощью автоматических сообщений электронной почты, телефонных вызовов, SMS сообщений.

ИНТЕГРАЦИЯ В СЕТЬ ПРЕДПРИЯТИЯ

Для доступа к WebEx Meeting Center и другим корпоративным приложениям используется единый вход в систему. Интегрируется WebEx с активной директорией посредством SSO.

Collaboration Meeting Rooms

Ваша персональная комната с возможностью подключения с терминалов видеоконференц-связи. Расширьте способности WebEx Meeting Center!

- Персональные и доступные в любое время веб-комнаты с уникальным ID и URL-ссылкой для входа.
- Доступ в конференцию с любого видеотерминала (Cisco, Polycom, Lifesize и тд.) и любого другого программного клиента сторонних производителей (Skype for Business).
- Простое добавление опции CMR Cloud к уже используемому сервису WebEx Meeting Center.
- Поддержка до 25 видеотерминалов и до 500 видео- или аудиочек сервиса WebEx Meeting Center.
- Запись совещаний и предоставление совместного доступа к ним.



Cisco WebEx Event Center

Большие конференции и вебинары

ПЛАНИРОВАНИЕ И ПРОДВИЖЕНИЕ

Автоматизированное управление электронной почтой с помощью персонализированных шаблонов.

Автоматическая отправка приглашений и напоминаний, регистрация участников мероприятий, рассылка дополнительных сообщений. Настраиваемые шаблоны для сообщений электронной почты в HTML или текстовом формате.

Настраиваемая форма регистрации и оценки потенциальных заказчиков.

Сбор данных о зарегистрированных посетителях и автоматический отбор потенциальных заказчиков по заданным критериям.

Продвижение всеми доступными способами. Максимально эффективное использование любой возможности связаться с потенциальными заказчиками: предоставления доступа к рекламным материалам при регистрации, а также в сообщениях, которые рассылаются до и после мероприятия.

Управление регистрацией и контроль посещения. Система подтверждения регистрации и индивидуально настроенные фильтры.

ПРЕЗЕНТАЦИИ

Высокое качество видео с возможностью отображения активного участника. До пяти видеоизображений участников дискуссии или докладчиков в высоком качестве. Изображение активного докладчика автоматически выводится на главный экран. Кроме того, можно зафиксировать отображе-

ние того или иного участника дискуссии. Поддерживается до 3000 участников конференции без использования видеосвязи и до 500 участников с видео.

Отдельный зал для подготовки.

Возможно выделение отдельного виртуального зала для докладчиков в случае, если им необходимо подготовиться к выступлению до начала мероприятия.

Мультимедийный контент. Докладчики могут демонстрировать слушателям презентации, приложения и видеофайлы, снабжая их комментариями в режиме реального времени. Для участников, ожидающих начала мероприятия, можно включить воспроизведение предварительно загруженного контента и музыки.

Гибкие, интегрированные аудиоданные. Поддержка глобальных телеконференций, передачи данных VoIP и аудиотрансляции. При помощи интегрированной системы контроля аудио организатор может управлять трансляцией звука от участников мероприятия.

Последовательные вопросы и ответы, чат, опросы и мониторинг посещения.

Ответы на входящие вопросы и их отслеживание при помощи функции структурирования. Индивидуальные или общедоступные чаты с участниками дискуссии или посетителями во время мероприятия. Отслеживание заинтересованности при помощи опросов в режиме реального времени и индикатора внимания.

ПОСТРОЕНИЕ ВЗАИМООТНОШЕНИЙ

Целевые URL-адреса после посещения мероприятия. Перенаправление посетителей на URL-адреса маркетинговых сайтов или другие адреса для просмотра или загрузки дополнительной информации о продуктах или для обращения в отдел сбыта.

Опросы посетителей и рассылка сообщений электронной почты по завершении мероприятия. Автоматическая рассылка сообщений со ссылками на запись мероприятия и опросом для посетителей. С некоторыми результатами опроса можно ознакомиться на странице с высокой степенью защиты.

ОЦЕНКА И АНАЛИЗ

Индивидуальные и стандартные отчеты. Просмотр данных о регистрации и посещениях, продолжительности посещения и многом другом в стандартных или индивидуальных отчетах. Оценка потенциальных заказчиков. Выявление наиболее эффективных способов увеличения аудитории при помощи отслеживания источников потенциальных заказчиков.

Экспорт в системы CRM и автоматизация маркетинга. Ускоренное последующее обслуживание благодаря загрузке данных о мероприятии (например, результатов опроса и информации о регистрации) в систему CRM и автоматизации маркетинга, например, Salesforce.com, Oracle On-Demand CRM и Eloqua.



Cisco WebEx Training Center

Инструмент для дистанционного обучения

Cisco WebEx Training Center поможет преодолеть обычные сложности в сфере интерактивного образования: удержать внимание учащихся во время занятия и убедиться в том, что полученная информация ими усвоена.

ОБМЕН МУЛЬТИМЕДИЙНЫМИ ДАННЫМИ

Инструкторы могут передавать учащимся презентации PowerPoint, документы, видеоролики для потоковой передачи, демонстрационные версии ПО, материалы для демонстрации в классе и анимированные ролики в формате Flash. Помимо этого, есть возможность предоставлять учащимся права на обмен данными и добавление комментариев.

ВИДЕО ВЫСОКОЙ ЧЕТКОСТИ ТЕХНОЛОГИИ ОБРАБОТКИ АУДИОДАННЫХ С ПОДДЕРЖКОЙ VOIP-КОНФЕРЕНЦИЙ

WebEx Training Center помогает удержать внимание учащихся и заинтересовать их с помощью видеопрезентаций в формате HD и добавления в основной сеанс до шести видеоканалов в режиме реального времени. Система видеотрансляции поддерживает технологию отображения активного участника, которая автоматически переключается на видеоканал текущего участника дискуссии.

СТРУКТУРИРОВАННЫЕ ОТВЕТЫ НА ВОПРОСЫ

Инструкторы могут отслеживать вопросы и документировать ответы при помощи специальной системы структурирования. Можно распределить вопросы по приоритету, отобразить ответы на них для отдельных участников или для всей группы, а также назначить тот или иной вопрос своему коллеге.

ЧАТ

В частных и общедоступных чатах пользователи могут общаться с инструктором, другими учащимися или всеми участниками учебной группы.

ОПРОСЫ, ОТЗЫВЫ УЧАЩИХСЯ И ИНДИКАТОР ВНИМАНИЯ

Инструкторы могут собирать отзывы учащихся при помощи одного или нескольких опросов в течение сеанса и сразу же заносить результаты в таблицу для дальнейшей демонстрации. Учащиеся могут «поднимать руки»: система автоматически распределяет запросы таким образом, чтобы инструкторы могли ответить на них в порядке поступления.

CISCO WEBEX HANDS-ON LAB

Уникальная функция Hands-On Lab («Лабораторная работа») обеспечивает учащимся максимально безопасный доступ к удаленным ПК для практического изучения различных приложений. Сеансы лабораторных работ могут быть включены в сеансы интерактивного обучения или проводиться по требованию.

ИНТЕГРИРОВАННЫЙ МОДУЛЬ ТЕСТИРОВАНИЯ

Для оценки эффективности обучения инструкторы могут тестировать учащихся до, после и во время интерактивных сеансов. Поддерживаются различные типы тестовых вопросов: с несколькими вариантами ответов, с ответами «да/нет», с полем для ввода ответов и в

формате реферата. Эффективность процесса проверки знаний повышают функция автоматического выставления оценки, отчеты и соответствие стандарту SCORM.

ЗАПИСЬ И ВОСПРОИЗВЕДЕНИЕ

Инструкторы могут записывать уроки и сохранять эти записи для просмотра и повторного использования. Кроме того, у них есть возможность транслировать записи в режиме потоковой передачи в ходе интерактивного обучения, а также публиковать их, чтобы учащиеся могли ознакомиться в удобное время.

РЕГИСТРАЦИЯ И ОТЧЕТЫ

У инструкторов есть возможность упростить решение административных задач с помощью функций самостоятельного составления расписания, управления регистрацией и отчетов о посещаемости. Им доступны подробные отчеты о посещаемости, записи уроков, информация о степени заинтересованности учащихся, результаты тестов и многое другое.

АВТОМАТИЗИРОВАННАЯ ЭЛЕКТРОННАЯ КОММЕРЦИЯ

Инструкторы могут извлечь экономическую выгоду из интерактивных или записанных занятий при помощи системы самостоятельной регистрации и платежей, выставять цену за каждое занятие и создавать купоны. Cisco WebEx Training Center интегрируется с системой PayPal и поддерживает транзакции в США, Великобритании и Канаде.



Cisco WebEx Support Center

Техническая и консультационная
поддержка пользователей

Сервис позволяет заменить устаревший способ общения в чате на более продуктивные консультации с использованием средств аудио и видеосвязи, возможностями обмена документами и приложениями, а также с функционалом, позволяющим подключать к общению специалистов в предметной области в режиме реального времени.

МАРШРУТИЗАЦИЯ ВХОДЯЩИХ ЗАПРОСОВ

Управление маршрутизацией входящих запросов в соответствии с внутренней политикой, соглашением об уровне обслуживания или нормативами.

ВЫДЕЛЕННЫЕ URL-АДРЕСА ДЛЯ ОПЕРАТОРОВ СЛУЖБЫ ПОДДЕРЖКИ

Операторам службы поддержки предоставляются индивидуальные выделенные URL-адреса.

ОБРАТНЫЙ ВЫЗОВ И ВРЕМЯ ОЖИДАНИЯ

Возможность заказать обратный вызов. Расчетное время ожидания с возможностью оставить сообщение, если пороговое значение времени будет превышено.

СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ ВЕБ-СТРАНИЦ, РАБОЧИХ СТОЛОВ И ПРИЛОЖЕНИЙ

Представители службы поддержки могут запускать сеансы веб-конференций, предоставляя заказчику безопасный совместный доступ к веб-страницам, рабочим столам, приложениям и потоковому видео.

ВЫСОКОКАЧЕСТВЕННОЕ ВИДЕО И ИНТЕГРИРОВАННАЯ АУДИОСИСТЕМА

Персонализированное взаимодействие с заказчиком благодаря высококачественному (360p) двухканальному видео, телеконференциям и связи через VoIP.

УПРАВЛЕНИЕ НЕСКОЛЬКИМИ СЕАНСАМИ ЧАТА И БИБЛИОТЕКА СЦЕНАРИЕВ

- Операторы службы поддержки могут управлять несколькими сеансами чатов в одном окне с помощью вкладок.
- Возможно создание библиотеки часто используемых сценариев ведения беседы в чате. Эти сценарии операторы службы поддержки могут использовать в ходе беседы с заказчиком.

ЯЩИК ВХОДЯЩИХ СООБЩЕНИЙ ОПЕРАТОРА СЛУЖБЫ ПОДДЕРЖКИ

Операторы службы поддержки автоматически получают уведомление о добавлении в очередь нового заказчика, о предпочтительных клиентах и времени ожидания каждого из них.

ПРОСМОТР СТАТУСА ДРУГИХ ОПЕРАТОРОВ СЛУЖБЫ ПОДДЕРЖКИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Для перераспределения обращений или эскалации запросов операторы службы поддержки получают доступ к очередям и данным о доступности и загрузке других операторов.

ОПРОС ЗАКАЗЧИКОВ ДЛЯ ОПРЕДЕЛЕНИЯ УДОВЛЕТВОРЕННОСТИ

Автоматический опрос заказчиков по завершении сеанса для оперативного получения данных о том, довольны ли они обслуживанием.

ЗАПИСЬ СЕАНСОВ НА ОСНОВЕ СЕТИ И ОТЧЕТЫ ПО ЗАВЕРШЕНИИ СЕАНСОВ

- Запись и архивация сеансов вручную или автоматически; сохранение всех действий, выполненных в течение одного сеанса, в том числе чатов, звуковых сообщений, видеоданных и документов.
- Детализированные отчеты по отдельным сеансам и операторам; глобальные отчеты по очередям и пулам операторов службы поддержки.

IT-лизинг Softline

Больше возможностей, меньше издержек.

Мы поддержим ваш бизнес в кризис!



- **Получите** IT-продукт на более простых условиях, чем в кредит.
- **Минимальный** первоначальный взнос.
- **Выбирайте** удобный способ оплаты или схему платежей.
- **Финансирование** в разной валюте.
- **Индивидуальный** подход, учет пожеланий и возможностей заказчика.
- **Возвращайте** оборудование после использования, не заботясь об утилизации/реализации и вывозе.

Мы финансируем проекты совместно с ведущими партнерами в сфере лизинга в IT-области. Бухгалтерское сопровождение лизинговой сделки — на лизингодателе. Действуют специальные программы финансирования от производителей.

Active CLOUD

Начни зарабатывать на облаках!

до **40%**
от облака

Active CLOUD
Облачные сервисы
ваших клиентов

Предлагайте клиентам современные решения для бизнеса: облачные сервера, корпоративную почту, хостинг 1С, лицензионное ПО Microsoft (по программе SPLA) и многое другое.

Вы получите при этом до 40% от платежа клиента сразу после оплаты.

Партнерами ActiveCloud могут стать как юридические, так и физические лица. Каждому участнику программы предоставляется уникальный промокод, по которому его клиент получает скидку, а партнеру в личном кабинете начисляются вознаграждения.

Наша партнёрская сеть стремительно растет и насчитывает уже более 1500 партнеров!

Как это работает



Вы рекомендуете
наши услуги



Клиент с промокодом
оплачивает заказ



Вы получаете
вознаграждение

+7 (495) 988-22-62 доб.1346

partner@activecloud.ru

www.activecloud.ru/partner

ПАРТНЁРСКАЯ ПРОГРАММА – ЭТО ВЫГОДНЫЙ И РЕГУЛЯРНЫЙ ИСТОЧНИК ДОХОДОВ!