softline direct

КАТАЛОГ ИТ-РЕШЕНИЙ И СЕРВИСОВ ДЛЯ БИЗНЕСА

СПЕЦ
11·12
2018
ВЫПУСК

Оборудование как сервис. История о том, как сэкономить

Энергоэффективность ЦОД

Мультиполезность мультимедиа

Apple в корпоративной среде

«Бешеные принтеры»: компании теряют сотни тысяч в год на нецелевой печати

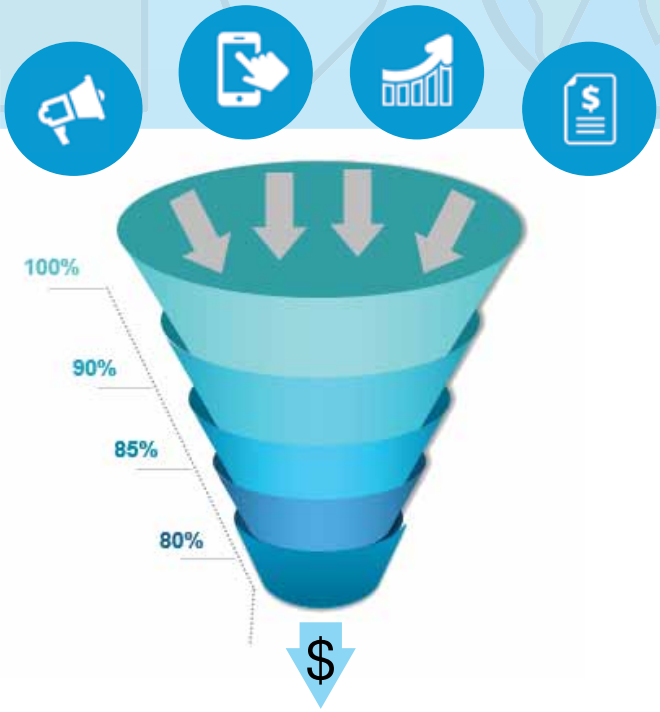
Новые курсы «Осведомленность ИБ»

ИТ-ИНФРАСТРУКТУРА

Digital Transformation and Cybersecurity Solution Service Provider | 8-800-232-00-23 | www.softline.ru

Allsoft Ecommerce

Увеличиваем ваши интернет-продажи с 2004 года



Обеспечим рост продаж минимум на **15%**

- **Адаптация под региональные особенности и требования рынка**
- **Продажа подписок (auto-renewable subscription)**
- **Маркетинговые инструменты**
- **A/B тесты и оптимизация**
- **Отчеты и аналитика**
- **Клиентский сервис**

Нам доверяют:

KASPERSKY lab, avast, Acronis, ABBYY, Parallels, Dr.WEB

и еще более 100 клиентов

Свяжитесь с нами: dev@allsoft.ru

Уважаемые коллеги, друзья!
ИТ-инфраструктура лежит в основе любых информационных систем.

Дата-центры и коммуникационные магистрали, серверы и сети, виртуальные среды и рабочие места, все это образует базу для инструментов, которыми мы пользуемся каждый день на работе, на учебе и когда отдыхаем.

Однако мы не продаем заказчикам инфраструктуру.

И мы, и наши клиенты рассматриваем информационные технологии как инструмент для решения задач бизнеса. И заказчики обращаются к нам именно за решением бизнес-задач: построить ЦОД определенной мощности, наладить биллинг с доступом через Интернет, создать резервную вычислительную площадку для отказоустойчивости.

Клиенты зачастую ставят перед нами задачи, на первый взгляд, далекие от технологий.

Как сделать продукты и услуги успешными?
Как расширить свою долю рынка, увеличить оборот и прибыль?
Как организовать принятие наилучших решений на основе имеющихся данных? Что сделать, чтобы заказчики захотели вернуться еще раз? Как повысить производительность труда?
Где можно снизить ненужные издержки?
Как достоверно просчитать все риски?

Цель нашей работы — решать подобные задачи на высоком технологическом уровне, с применением наиболее подходящих технических средств.

Спроектировать инженерную, аппаратную и сетевую составляющие, обоснованно выбрать средства виртуализации, обеспечить безопасность — и это далеко не все! Какие именно технологии будут задействованы — заказчику, по большому счету, не так важно.
Ведь люди покупают не серверы и облака, а именно решение бизнес-задач.
Совокупность отраслевой и технологической экспертизы делают Softline уникальной компанией, которая умеет поставить технологии на службу коммерческому успеху.

Приглашаем вас к сотрудничеству и желаю вам успеха!

Каталог
ИТ-решений
и сервисов
для бизнеса

Softline
direct
#11-12-2018

2018-11-12(189)–RU

Учредитель: АО
«СофтЛайн Трейд»

Издатель:
Игорь Боровиков

Главный редактор:
Максим Туйкин

Редакторы:
Яна Ламзина,
Вячеслав Гречушкин,
Антонина Субботина,
Лидия Добрачева

Дизайн
и верстка:
Алексей Воропанов,
Юлия Константинова

Над номером
работали:
Руслан Фазилов,
Антон Милёхин,
Денис Яркин,
Антон Карпов,
Петр Цирьков,
Сергей Монин,
Александр Захаров,
Геннадий Низовцев,
Сергей Фортунатов,
Максим Пуха,
Дмитрий Галкин,
Александр Петров,
Дмитрий Сорокин,
Виктория Костычева,
Дмитрий Шалеев,
Сергей Ненахов,
Михаил Апостолов,
Михаил Авсенев,
Анна Попова,
Игорь Кравченко,
Денис Чигин,
Яков Рутман,
Ксения Сазонова,
Светлана Распутина,
Екатерина Корбун,
Елена Катасонова,
Александр Макаров
и др.
Тираж: 60 000 экз.

Зарегистрировано
в Государственном
комитете РФ
по печати,
рег. ПИ № ФС77-71088
от 13 сентября 2017 г.

СОДЕРЖАНИЕ

Кибербезопасность

Эффективность бизнеса

СПЕЦИАЛЬНЫЙ ВЫПУСК: **ИТ-инфраструктура**

Softline в соцсетях

SoftlineCompany Softlinegroup SoftlineCompany softlinegroup

Зарегистрировано в Государственном комитете РФ по печати, рег. № ПИ ФС77-23773 Перепечатка материалов только по согласованию с редакцией © Softline-direct, 2017

ПОРТРЕТ КОМПАНИИ

Наша миссия

Мы осуществляем цифровую трансформацию бизнеса наших клиентов на основе передовых информационных технологий и средств кибербезопасности.

ПОЧЕМУ SOFTLINE?

1. Мы — глобальная сервисная компания, которая помогает бизнесу и государству осуществить цифровую трансформацию
2. Надежность, профессионализм и компетентность Softline признаны клиентами, вендорами и независимыми источниками
3. Единая точка решения всех ИТ-задач, мультивендорная поддержка и сопровождение
4. Softline всегда рядом и говорит с заказчиками на родном языке более, чем в 50+ странах и 95+ городах
5. Softline доверяют ведущие игроки рынка, государственные организации, средние и малые компании

Digital Transformation and Cybersecurity Solution Service Provider

Статусы Softline

Microsoft Partner

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

Kaspersky ENTERPRISE PARTNER

Oracle Platinum Partner

vmware PARTNER

Authorised Systems Integrator

IBM Gold Business Partner

intel Software Elite Reseller

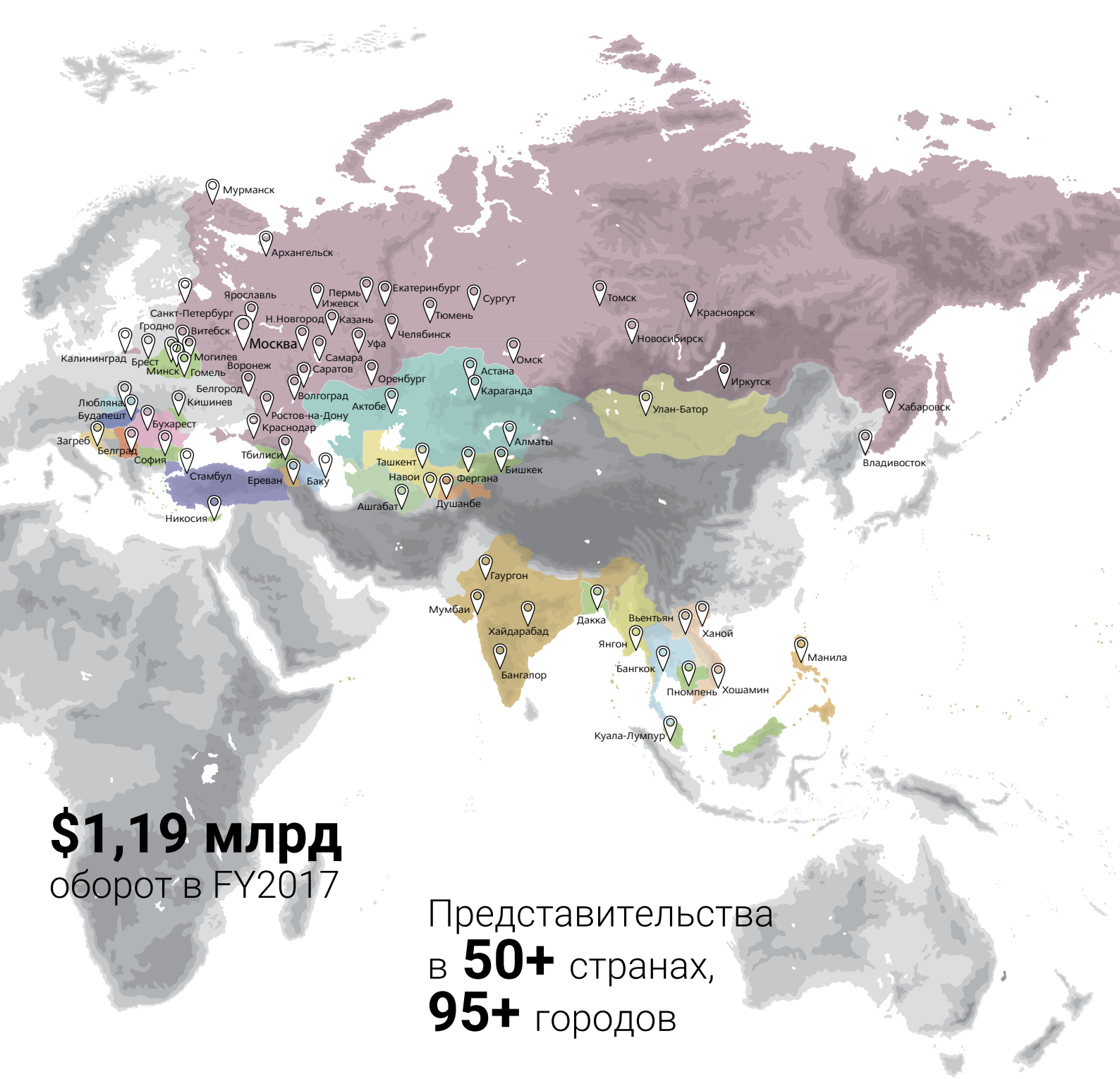
CITRIX PARTNER Platinum Solution Advisor

Acronis Gold Partner

VERITAS Partner Force Gold Partner

APC

eset Corporate Premier Partner



$1,19 млрд
оборот в FY2017

Представительства
в **50+** странах,
95+ городов

+30% рост в FY2017
по группе компаний

25 лет
на ИТ-рынке

НАШИ ЗАКАЗЧИКИ

от стартапов до транснациональных корпораций

ПРОИЗВОДСТВО И ЭНЕРГЕТИКА

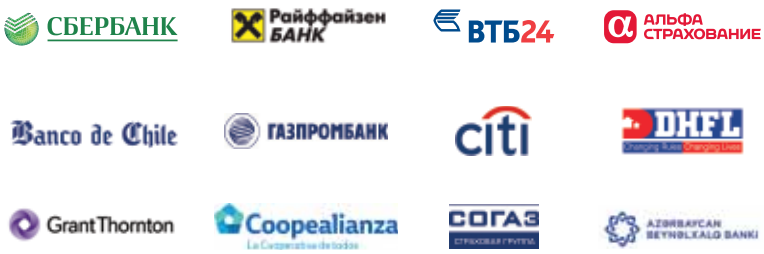
А также:
Объединенная компания РУСАЛ | Интер РАО ЕЭС | Акрихин | Трансмашхолдинг | Соллерс | Сибур | Chinfon Cement | Джи Эм-АВТОВАЗ | Toyota Tsusho | Caterpillar | Мосэнерго | Камчатскэнерго | ОГК-2 | Вимм-Билль-Данн | МРСК Северного Кавказа | STADA CIS | Hever Solar | Onninen | Металлимпресс | Damate | ОМК Востокцемент | Ashirvad Pipes |Северский трубный завод | Инженерный центр энергетики Урала | Полисан | Самараэнерго | УЗГА

3000+ поставщиков программного и аппаратного обеспечения

РИТЕЙЛ, УСЛУГИ

А также:
Ашан | Эльдорадо | Рольф | Виктория | Иль де Боте | Grupo Sura | Снежная королева | Славянка | Роспечать | ГК Форвард | MC Group | Юлмарт | CarPrice | Детский мир | Алтын | Яшма Золото | Grupo Phoenix | Bodytech | Ajegroup | РесурсТранс | Высшая лига | Миэль | Henderson | СТЛ Моторс | Interchape | Кораблик | Адамас | Fortrent

БАНКИ, ФИНАНСОВЫЕ ОРГАНИЗАЦИИ



А также:
ВТБ Страхование» | Барклайс банк Россия | BNP Paribas | Ренессанс Кредит | БИНБАНК | Khan Bank | Кредит Европа банк | Yoma Bank | АВТОВАЗ-БАНК | Эко Исламик Банк | Банк Согласие | Локо-банк | Банк Открытие | Банк Стандарт | Zurich | КИТ Финанс | Дельта Кредит | Альфа-банк | Уралсиб | Проирбанк | Банк Таата | Сентинел Кредит Менеджмент | CiV Life | Евразийский банк

softline®

25 Years in IT

60 000 + корпоративных заказчиков

ТЕЛЕКОММУНИКАЦИИ, СМИ, РАЗВЛЕЧЕНИЯ

МТС | МегаФон | Telefónica | TELE2 | Ucell | Supercanal | Aljazeera Türk | Ростелеком

А также:
Вымпелком | Yota | Российская телевизионная и радиовещательная сеть | ВГТРК | Condé Nast | НТВ | ТНТ-Телесеть | ГК ПрофМедиа | МГТС | Старт Телеком | MTT.DOM | Saima Telecom | Белтелерадиокомпания | ГК Искра | ITPS | Aggregion | OMD OM | RuTube

ГОСЗАКАЗЧИКИ

РЖД | Rosoboronexport | POS Malaysia | Росатом | Kyrgyzpatent | Роснано | ФИРВ | Ministerio de Educación Presidencia de la Nación | ВЦИОМ

А также:
Министерство связи и массовых коммуникаций РФ | Министерство образования и науки РФ | Управление делами Президента РФ | Инновационный центр Сколково | Администрации десятков городов и регионов России | Центральная базовая таможня | Департамент гражданской обороны города Москвы | Единый лесопожарный центр Архангельской области

600+ технических специалистов

1100 аккаунт-менеджеров

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

ЛУКОЙЛ | Газпром | Транснефть | TATNEFT | Роснефть | pluspetrol | SOCAR | Agip

А также:
Газпром ПХГ | Газпром Добыча Шельф | Газпром автоматизация | Нарьянмарнефтегаз | Мособлгаз | Уралтранснефтепродукт | Аки-Отыр | Газпром газораспределение Белгород | Зарубежнефть | Гипровостокнефть | КПК КРС | Волгограднефтепроект | Белоруснефть | PetroKazakhstan

Профилактика кибербезопасности

Как повысить осведомленность персонала в области информационной безопасности и почему за незнание приходится дорого платить, рассказал Руслан Фазилов, руководитель учебного центра Softline.

– К каким последствиям может привести недостаточная осведомленность об угрозах информационной безопасности?

– У своих клиентов мы всегда спрашиваем, знают ли они о тех угрозах, с которыми могут столкнуться. Практически все знакомы с вирусом Petya, похищением конфиденциальной информации, шпионажем, сливом базы конкурентам и т.д. Но при этом существуют исследования, которые подтверждают, что 46% российских компаний не имеют политики работы с осведомленностью по информационной безопасности. В связи с этим организации терпят огромные убытки, теряют ценные данные, несут масштабные репутационные потери. Кто виноват в этом? Как бы это ни было банально, но чаще всего причиной являются люди, которые не знакомы с культурой поведения в интернете. Это пользователи, которые кладут бумажку с паролем под ноутбук, подписывают ПИН-код на банковской карте, делают фото на рабочем месте и проявляют излишнее любопытство, путешествуя по сомнительным сайтам.

В одной из компаний сотрудник открыл пришедшее на почту письмо якобы от представителя банка. Моментально компьютер был заражен вирусом Petya, и все данные на нем в течение нескольких минут были зашифрованы. К большому счастью компьютер не был подключен к локальной сети. Так как же оценить последствия? Уволить специалиста? Данные это не вернет. Заплатить злоумышленнику? Можно быть уверенным, что нет смысла полагаться на его порядочность, ведь цель его деятельности – мошенничество и зарабатывание денег. На деле же компьютер описали, а провинившийся сотрудник два месяца оставался после работы, приходил на выходных и восстанавливал акты, ведомости, списки и т.д. Убытками можно считать сумму его зарплаты за два месяца, но это далеко не все. На протяжении долгого времени компания ждала, пока важные документы будут восстановлены, некоторые проекты были отложены, на других сотрудников упала дополнительная работа – при разных обстоятельствах оценивать все это можно уже миллионами. Это последствия действий всего лишь одного работника и всего лишь одного зараженного компьютера. Если сотрудники компании недостаточно осведомлены о правилах информационной безопасности, то руководство должно быть готово к подобным исходам.

Сотрудники – это первичный фильтр по защите от кибератак. По результатам исследований Google, если работник ведет себя корректно в интернете, то 80% угроз не представляют опасности для компьютера.

– Какие меры нужно предпринимать, чтобы предотвратить это? Расскажите о курсах учебного центра Softline, которые направлены на повышение ИБ-защиты?

– Даже обладая передовыми антивирусами и настроенными фаерволами можно оказаться жертвой вредоносных программ, лишиться данных и потерять деньги. В первую очередь сотрудники должны знать, с какими угрозами они могут столкнуться и как им себя при этом вести. Грамотный пользователь – это лучший фильтр от любых вредоносных воздействий. Тем более, что правила защиты элементарны. Однако процент их несоблюдения крайне велик, а последствия слишком печальны.

Для того, чтобы их избежать учебный центр Softline разработал курсы, посвященные повышению осведомленности сотрудников в области информационной безопасности. Мы также обучаем специалистов технической защите серверов, компьютеров, шифрованию данных. У нас есть отдельные курсы по киберзащите, основам законодательства в области безопасности персональных данных (152-ФЗ), критически значимых объектов инфраструктуры (187-ФЗ). В любой компании должны быть обученные, сертифицированные специалисты, которые умеют настраивать и сопровождать технические средства по защите данных и проводить консультации сотрудников по вопросам обеспечения информационной защиты.

Разработки учебного центра Softline согласованы во ФСТЭК и ФСБ, а обучающие программы соответствуют требованиям профессиональных стандартов. Мы также предоставляем и ряд вендорских курсов (Microsoft, «Лаборатория Касперского», VMware, Cisco, Citrix, Red Hat и другие).

Правила защиты элементарны, однако процент их несоблюдения крайне велик, а последствия слишком печальны. Для того, чтобы их избежать, учебный центр Softline разработал курсы, посвященные повышению осведомленности сотрудников в области информационной безопасности..

– Как повысить осведомленность персонала в сфере информационной безопасности?

– На курсах мы объясняем, как сгенерировать правильный пароль и как его запомнить, почему нельзя вставлять флешки в рабочий компьютер, какие сайты нельзя посещать, какие приложения не стоит устанавливать, как вести себя, получив сомнительное письмо и т.д. Вся эта информация чрезвычайно важна для поддержания бесперебойной работы, однако не все работодатели верят, что их сотрудники не знакомы с базовыми правилами. Многие ошибочно полагают, что эти знания даются по умолчанию, кто-то решает самостоятельно проводить разъяснения и инструктажи. Некоторые ИТ-директоры стремятся не оставить нерадивому сотруднику шансов сделать что-то не так: устанавливают антивирусы, настраивают фаерволы, заклеивают USB-порты, закрывают соцсети, частично отключают доступ к интернету. Как ни странно, несмотря на все это данные продолжают похищаться, поэтому первый блок работ, который мы предлагаем, это оценка – краткий аудит состояния ИБ компании.

Руслан Фазилов, руководитель учебного центра Softline.

– Как именно вы выявляете уровень киберграмотности сотрудников?

– Можно, к примеру, сымитировать фишинговую рассылку. Если мы имеем дело с женским коллективом, то отправляем стилизованные письма от имени какого-либо косметического бренда с акционным предложением. В сообщении просим пройти по ссылке, указать свои пароли, личные данные. Отследить количество человек, перешедших по ссылке, не составляет труда и, если их количество составило, к примеру, 120 человек из 300, то стоит серьезно озадачиться уровнем осведомленности своих сотрудников.

Не менее эффективным диагностическим мероприятием служит подбрасывание флэшек. Как показывает практика, мало кто проходит мимо новенькой блестящей флэш-карты, все сразу же стремятся вставить ее в свой рабочий компьютер, с целью выяснить, что же на ней может быть интересного. А там их ждет всплывающее окно с красочной надписью: «Поздравляем, вы подхватили вирус!». Такие приемы помогают выявить, что сотрудники компании часто пренебрегают правилами кибербезопасности в силу незнания или равнодушного отношения к судьбе корпоративных ресурсов.

После того как выявлены слабые звенья и доказано, что в компании все далеко не так благополучно, как казалось, нужно определиться с форматом обучения. Это могут быть электронные курсы, командные игры, тренинги, видео-квесты. У нас есть как общие программы обучения, так и адаптированные под индивидуальные потребности. Целое направление учебного центра Softline занимается разработкой электронных курсов применительно к нормативам компаний (например, атомной или военной промышленности), законодательству РФ. В конце обучения мы проводим итоговое тестирование, которое показывает, что сотрудники стали главными защитниками компании от киберугроз.

Все дело в разнице между инструктажем и обучением. В первом случае сотрудник знакомится с материалом, старается его запомнить, сдает стандартный тест, после чего может благополучно все забыть. Обучение подразумевает целенаправленную работу с целью убедиться, что сотрудник усвоил материал и применяет его на практике.

– В чем козыри учебного центра Softline?

– Как я уже говорил ранее, иногда компании проводят инструктажи по информационной безопасности собственными силами. Они тоже объясняют про пароли, флэшки, письма и т.д. Однако случаи нарушений происходят снова и снова. Все дело в разнице между инструктажем и обучением. В первом случае сотрудник знакомится с материалом, старается его запомнить, сдает стандартный тест, после чего может благополучно все забыть. Обучение подразумевает целенаправленную работу с целью убедиться, что сотрудник усвоил материал и применяет его на практике. Большую роль здесь играет опыт преподавателей учебного центра, то как они умеют подавать материал и заинтересовывать слушателей. Квалифицированные преподаватели применяют различные методики, используют специально разработанные флэш-ролики, у нас большая база тематического контента и дизайна (листовки, брошюры, раздаточные материалы). Все это регулярно обновляется и адаптируется к актуальным тенденциям. Хакеры не стоят на месте, и отставать от них не стоит, поэтому некоторые электронные курсы мы разрабатываем только на год, чтобы они не успевали терять свою актуальность. В учебном центре Softline доступны: разработка индивидуальных курсов, сертификационные экзамены, дневные и вечерние, очные и смешанные курсы, поддержка после окончания обучения и многое другое. Мы разрабатываем проекты под конкретную организацию, ее задачи, потребности и бюджет. Можно связаться с нами по телефону или прислать запрос на почту – не нужно ждать, пока незнание обойдется слишком дорого.

Контакты:

Актуальное расписание, программы курсов и цены на **edu.softline.ru**
E-mail: **edusales@softline.ru**
Тел.: **8-800-505-05-07**

Microsoft Azure для малого и среднего бизнеса

Эффективность бизнес-процессов напрямую влияет на прогресс компании. При успешном развитии дела неизбежно возникают новые задачи и потребности, которые требуют увеличения мощностей и применения новых сценариев использования облачных служб. Антон Милёхин, менеджер по развитию бизнеса Microsoft Azure в компании Softline, рассказал, как набор сервисов Microsoft Azure помогает решать проблемы создания, развертывания приложений и управления ими в глобальной сети.

Что такое Microsoft Azure?

Это глобальная платформа Microsoft, которая включает в себя более 200 различных сервисов. К ним относятся виртуальные машины и контейнеры, различные облачные СУБД (SQL, NoSQL), сервисы хранения данных, резервного копирования и георепликации, сетевые сервисы и сервисы анализа данных. Более 100 ЦОДов Microsoft располагаются в Европе, Азии, Северной и Южной Америке в 54 регионах. На территории России дата-центра нет, поэтому нашим заказчикам доступны европейские ЦОДы, или, если бизнес масштабируется на другие страны, то можно выбрать любую страну.

Из чего он состоит?

Инфраструктурные сервисы включают в себя **виртуальные машины**, обеспечивающие гибкость виртуализации для широкого ряда вычислительных решений, а также службу **контейнеров. Хранилища данных**: BLOP Storage, Azure Files, Premium Storage. **Сетевые службы**, созданные на базе одной из крупнейших оптоволоконных магистральных сетей, обеспечивают максимальное удобство и безопасность работы своих пользователей. Это ExpressRout – выделенный канал до ЦОДа Майкрософт, позволяющий добавлять подключение к частным сетям для доступа к облачным службам. Это VPN-шлюзы для безопасного доступа к виртуальным сетям Azure, application-шлюзы для оптимизации доставки из ферм серверов приложений, а также все, что связано с сетью и ее настройкой.

Платформенные сервисы включают в себя **центр интернета вещей, базы данных**, сервис **аналитики**. Они позволяют собирать информацию с датчиков, которые вы расположили в своей организации, хранить большие объемы данных и в дальнейшем строить предиктивные аналитические отчеты с целью предсказывать, к примеру, поведение покупателей. Набор инструментов для разработчиков Azure DevOps помогает повышать точность планирования, продуктивность сотрудничества и скорость поставки решений разработчиков.

Azure позволяет упрощать управление благодаря облачной платформе с высоким уровнем безопасности и пользоваться преимуществами самого широкого ассортимента функций гибридной среды. К ним относится многофакторная аутентификация, **Active directory** (доменные службы), **Key Vault** (хранилище ключей), магазин-приложение **Marketplace**, где можно приобрести необходимые облачные программные решения.

Каковы основные трудности, с которыми помогает справиться глобальное облако Microsoft? В первую очередь это высокие затраты на ИТ: стоимость владения текущей инфраструктурой и сложности соотношения затрат на конкретные ИТ-проекты. Второе – это низкая работоспособность: сбои в текущей инфраструктуре или отказ оборудования. И также к сложностям относится потребность в масштабировании. Если бизнес развивается, то открываются новые филиалы, офисы, магазины, возникает необходимость безопасного мобильного доступа к корпоративным ресурсам. Все эти проблемы помогают решить виртуальные машины Microsoft Azure.

Вычислительные мощности для приложений любого типа

Серия A. Самые экономичные виртуальные машины. Обладают характеристиками производительности процессора и памяти, лучше всего подходят для рабочих нагрузок начального уровня – для разработки и тестирования, веб-сервисов с низким уровнем трафика, баз данных малого и среднего размера.

Серия B. Виртуальные машины с накапливаемыми ресурсами позволяют избежать ненужных расходов и подходят для низкого и среднего уровня загрузки центрального процессора. Можно использовать для сервера разработки тестирования, экспериментальных решений и сборки каких-либо микрослужб.

Серия D. Машины общего назначения, которые оснащены более быстрыми процессорами. Они отличаются оптимальным соотношением производительности центрального процессора и памяти. На них можно размещать большинство приложений корпоративного уровня, различные базы данных.

Серия F. Виртуальная машина, оптимизированная для интенсивных вычислений. Может использоваться для пакетной обработки, аналитики и развертывания игр.

Серия G. Машины, с оптимизированной памятью для хранения крупных баз данных SQL, либо NoSQL, для размещения SAP или других ERP-систем.

Серия H. Специализированные для сложных, высокопроизводительных вычислений виртуальные машины. Это пакетная обработка, аналитика, молекулярное моделирование и т.д. Сервисы выделяются под конкретный запрос через службу Microsoft.

Серия N. Не используется на постоянной основе. Машины с графическими процессорами для операций, которые требуют мощных графических ресурсов.

Какие плюсы использования предлагает Microsoft?

Один из них – это возможность резервировать экземпляры виртуальных машин на 1 или 3 года. К тому же, если есть лицензии Microsoft с поддержкой Software assurance, их можно использовать на виртуальных машинах в облаке, что опять-таки снижает стоимость владения.
Не стоит забывать и о том, что Azure – это открытое облако. В нем есть практически все, чем можно пользоваться в локальной инфраструктуре: инструменты для разработчиков, инфраструктурные сервисы, базы данных, приложения, инструменты для управления и мн. др.

Обеспечение непрерывности бизнеса

Данное направление включает в себя **Azure Site recovery** – один из основных инструментов, с которым Microsoft был признан лидером в исследовании Gartner Magic Quadrant for Disaster Recovery as a Service за 2018 г. В ходе работы имеют место быть случаи, когда по каким-либо причинам сервер оказывается недоступен, пользователи сидят без работы, и от этого бизнес терпит убытки. Azure Site recovery позволяет переподключать пользователей на виртуальные машины. Их можно использовать до тех пор, пока все проблемы не будут устранены – сотрудники продолжат работать, ИТ-отдел не получит упреки в свой адрес и бизнес не пострадает. Данное средство аварийного восстановления поддерживает Hyper-V и VMware.
Еще один инструмент, который служит обеспечению непрерывности бизнес-процессов, это **Azure Backup.** С его помощью можно сократить время восстановления данных и повысить надежность защиты от программ-вымогателей. Служба предоставляется бесплатно, так как встроена в платформу Azure.
Решение **Azure Active Directory** работает с облачными каталогами и предоставляет инструменты многофакторной аутентификации. С их помощью можно избежать компрометации данных при подключении к тому или иному сервису. С помощью Azure AD можно публиковать локальные приложения без проблем с идентификацией. Это удобно, когда, к примеру, сотрудники на аутсорсинге подключаются к какому-либо приложению из разных сетей. Можно опубликовать это приложение для них и настроить либо единый вход, либо многофакторную аутентификацию.

Разработка и размещение приложений в Azure

DevOps – это методика, объединяющая специалистов, процессы и технологии, которые имеют отношение к разработке и ИТ. Благодаря данному инструменту специалисты по разработке, ИТ-операциям, проектированию качества и безопасности могут тесно сотрудничать, объединяя методики, которые раньше были изолированы. Таким образом, технология DevOps предоставляет инструменты командной работы и автоматизации, за счет чего создаются более совершенные продукты. Также увеличивается скорость их доставки, тем самым повышая уровень удовлетворенности клиентов. Возможность сбора телеметрии по производительности приложений позволяет принимать взвешенные решения и отслеживать потенциальные проблемы еще до их появления. Эффективное управление средами и возможность автоматического предоставления необходимых машин по модели pay-as-you-go позволяет оптимизировать ресурсы.

В облаке Microsoft Azure можно разрабатывать приложения как для облачной, так и для локальной инфраструктуры. Компания имеет все индустриальные стандарты в европейских странах и странах США. ▮

Microsoft развивается бурными темпами, каждый месяц выпускается большое количество обновлений для каждого сервиса. Среди его продуктов можно найти инструменты для решения практически любой ИТ-задачи

Антон Милёхин,
менеджер по развитию бизнеса
Microsoft Azure
в компании Softline

Перевод сервисов компании Macrokiosk (Малайзия) в облако Azure

О клиенте

Macrokiosk является ведущим в Азии поставщиком мобильных технологий и платежных услуг. Компания предлагает своим клиентам безопасные и масштабируемые решения, которые можно адаптировать к потребностям заказчика.

Бизнес-ситуация

Система Macrokiosk, отвечающая за доставку сообщений между офисом в Малайзии и инфраструктурой обслуживания клиентов на Тайване, размещена на локальных серверах. Она разрабатывалась собственными силами компании, работала медленно и не была оптимизирована. Также отсутствовала сопутствующая документация, с помощью которой можно было бы получить представление о самой системе и связях происходящих в ней процессов.

Основной целью проекта было повышение производительности системы, высвобождение дополнительных ресурсов.

Решение

Для достижения поставленных целей руководство Macrokiosk выбрало миграцию локально установленной системы в облако Microsoft Azure. Проект был поручен компании Softline, а все работы по нему оплатила корпорация Microsoft.

На первом этапе специалисты Softline проанализировали архитектуру заказчика и собрали сборочный комплект всех необходимых служб, чтобы затем превратить инфраструктуру наземных сервисов в прототипы облачных сервисов Azure.

На втором этапе проводились тесты с целью выявления узких мест и верификации скорости, с какой будут работать сервисы.

На третьем этапе специалисты Softline сформировали и передали исходные коды, внедрили пилотный проект, с помощью которого продемонстрировали особенности процесса миграции, объяснили все нюансы и обучили специалистов заказчика, которые в ближайшее время будут самостоятельно осуществлять процесс перевода системы в облако.

Результат

По завершении проекта заказчик получил полное и подробное руководство по переводу системы в облако Azure. Компания Softline обучила специалистов Macrokiosk и отработала вместе с ними процесс миграции на примере пилотного проекта.

Все необходимые программы были переведены в набор сервисов Azure. Каждому приложению определили свое место, нашли узкие места, описали структуру базы и ее синхронизацию с базами клиента. При разработке проекта систему оптимизировали за счет удаления избыточных компонентов и связей.

По проекту предоставлена исчерпывающая документация и осуществлены консалтинговые услуги, достаточные для дальнейшего перевода в облако всей системы силами одного штатного специалиста.

После миграции в Azure вопрос масштабирования системы будет решаться всего в два клика. За поддержку облачных сервисов теперь будет отвечать Microsoft, что в лучшую сторону скажется на стабильности всех служб. ▮

«Основная сложность подобных проектов – не сама миграция, а подготовка к ней. Проблема заключается в том, чтобы описать систему и корректно перевести все локально установленные службы и сервисы в облако. Почти всегда одновременно проводится оптимизация системы, устраняются узкие места. Эти процессы требуют участия высококвалифицированных специалистов. После проведения такой серьезной подготовки сама миграция легко осуществляется силами штатных ИТ-сотрудников», – отметил Денис Яркин.

Техника Apple в корпоративной среде

Обычно название Apple ассоциируется с дорогой техникой, которая используется в личных целях или в работе дизайнеров, специалистов по 3D-графике и прочих высокооплачиваемых профессионалов. На самом деле все не так очевидно. С помощью техники Apple можно создавать мобильные рабочие места продавцов-консультантов, автоматизировать склады и многое другое. О том, как это реализуется и каковы преимущества таких решений, нам рассказал Антон Карпов, Руководитель направления Apple в Softline.

– Почему именно техника Apple?

– Покупка личных устройств и корпоративных – это две в корне разные вещи. Личное устройство мы выбираем, исходя из собственных предпочтений и финансовых возможностей. С корпоративными гаджетами все не так очевидно.

Во-первых, корпоративные устройства нуждаются в установке и наладке приложений, а также настройке доступа к ресурсам. При большом количестве сотрудников это выливается в значительную потерю времени. Softline обеспечивает управление мобильными устройствами с помощью интегрированной системы управления. Эта система позволяет назначать правила работы устройств, в том числе на определенных локациях, например, можно отключать видео и фотокамеры в зоне разработки.

Во-вторых, ни для кого не секрет, что устройства компании Apple по праву считаются намного менее уязвимыми к вирусным и прочим атакам, чем любые другие. К примеру, во время эпидемий вирусов-шифровальщиков Petya и WannaCry не было затронуто ни одно устройство на MacOS и iOS, в то время как количество пострадавших устройств на Android исчислялось десятками тысяч.

В-третьих, отказоустойчивость устройств Apple ниже, а срок жизни – дольше, чем у смартфонов на Android. К тому же новые операционные системы Apple поддерживаются техникой на протяжении 3-4 лет. Для устройств на Android этот срок чаще всего не превышает 1 год, что напрямую влияет на стоимость владения гаджетом.

Следующим пунктом следует отметить адаптацию и разработку приложений. Для Android приходится содержать штат разработчиков, которые создают обновления на каждую новую ОС. Разработка приложений под Apple намного проще и не требует наличия большого количества специалистов.

Немаловажную роль играет также мотивирующий и имиджевый фактор. Наличие высококлассных корпоративных устройств в компании заинтересует молодых и перспективных сотрудников. Это может послужить решающим фактором. Кроме того, наличие девайсов Apple создает хороший имидж компании в глазах клиентов. Этот фактор многие недооценивают, но он играет большую роль.

Наконец, не следует забывать и о том, что дешевые телефоны имеют маленькую остаточную стоимость или не имеют ее вообще. Их почти невозможно продать. Для сравнения, iPhone, купленный за 50 тыс., через год можно продать за 20-25 тыс., что составляет 45-50%. Недорогое устройство на Android стоимостью до 20 тыс. рублей на вторичном рынке через год оценивается не дороже 2 тыс. рублей., что составляет всего 10% от стоимости.

– Насколько нам известно у компании Softline есть целый портфель услуг, связанных именно с техникой Apple. Можете рассказать нам об этих сервисах?

– В первую очередь хочу отметить Apple-as-a-Service. По сути дела, это аренда оборудования, не требующая больших единовременных капитальных затрат и позволяющая ощутимо сэкономить на налогах, поскольку оплата аренды относится к расходной части средств, за счет чего сокращается налог на прибыль. Также возможен вариант с техникой в «Трейд-Ин». Отдельной услугой является предоставление вместе с техникой девайсов, расширяющих возможности устройств: считыватели штрих-кодов, мобильные платежные терминалы и др. Есть еще такие востребованные услуги, как предоставление техники с подпиской на специализированное ПО и страхование устройств. Компания Softline предлагает также продукты, автоматизирующие рабочий процесс, такие как решение WorkFlowSoft, наша собственная разработка. Также мы можем создать новый программный продукт, если это будет необходимо для бизнес-задач заказчика.

– Как реализуется страхование устройств?

– Услуга страхования устройств по умолчанию предоставляется вместе с их арендой, но может быть приобретена и отдельно. Она покрывает все вероятные риски. Устройство может разбиться, потеряться, его могут украсть или залить водой, но все это покроет страховка. Расширенная страховка – это не только покрытие гарантийных случаев. В ней также заложены риски неаккуратного обращения с устройством и противоправные действия (кража). В отличие от обычных видов страхования, компенсация производится не деньгами, а новым идентичным устройством, ведь для работы нужно именно оно. Таким образом, сотрудник не остается надолго без рабочего инструмента, что бы ни случилось.

– Дополнительные девайсы, расширяющие возможности устройств Apple. О чем именно идет речь?

– Мы поставляем специальные чехлы для техники Dataphone, в которых есть, например, сканеры штрих-кодов и встроенные платежные терминалы. По сути, весь комплект позволяет создать мобильное рабочее место продавца или сотрудника склада.

Как это работает? К примеру, у каждого продавца-консультанта есть свое устройство, с помощью которого он найдет ответы практически на любые вопросы покупателя, связанные с товарами в магазине; сможет посмотреть, наличие товара на складе и возможности по его доставке; получит подсказку насчет того, что следует предложить в комплект с товаром (дополнительные продажи) и, конечно, сможет сразу же принять оплату за товар, что сильно повышает вероятность покупки. Благодаря такому мобильному рабочему месту сокращается и время на обучение сотрудников.

Со складами ситуация похожая. У нас уже есть подобные кейсы. С помощью поставленных устройств в комплекте со сканерами штрих-кодов возросла скорость работы склада. Приходит товар, его тут же сканируют, вся информация тут же отправляется в систему. Все происходит быстро и без накладок.

Антон Карпов, Руководитель направления Apple в Softline.

– Вы говорили, что можете создавать собственные программные продукты, если того требуют бизнес-задачи клиента? Можете привести пример, о чем идет речь?

– Например, сотрудник отдела продаж, который ходит по встречам. Компания заинтересована в том, чтобы контролировать ход переговоров. На телефоне сотрудника находится мобильная презентация, которая фиксирует, сколько времени он останавливался на каждом слайде, какая была конверсия и прочие показатели. Таким образом осуществляется контроль специалиста. После презентации все запросы клиента фиксируются в системе, после чего формируется коммерческое предложение, а все данные автоматически перемещаются в CRM-систему. Это удобно еще и тем, что сотруднику не надо запоминать все, о чем говорили на встрече с клиентом. Если что-то забудется – это можно будет посмотреть в системе. А для руководства это возможность контролировать действия сотрудника. ▮

Голодный ЦОД: как накормить и не разориться

Сколько стоит «содержать» дата-центр?
В мире на момент создания этого материала существует порядка пятисот тысяч ЦОД, и владелец каждого из них назовет свою цифру расходов. «Вилка» получится приличная.

Масштабы дата-центров растут, и их потребности тоже меняются, но лишь в единицах случаев операционные издержки удается тем или иным образом сдерживать. Эффективное и экономичное потребление электричества, энергосберегающие технологии могут в буквальном смысле стать залогом существования ЦОДа, ведь более половины всех затрат уходит именно на электроэнергию.

Дорогое удовольствие

У различного железа разный «аппетит» и теплоотдача; помещения, в которых сервера стоят, тоже имеют свои особенности, в том числе по охлаждению; а если мы посмотрим еще дальше, то заметим еще и экологический аспект в функционировании дата-центров. Они выбрасывают колоссальное количество углекислого газа. В России на этом пока не заостряют внимания, но в ряде стран данный факт волнует общественность. Снизить энергопотребление – значит уменьшить и парниковые выбросы (а также деньги сохранить).

Специалисты считают, что большинство дата-центров «съедает» гораздо больше, чем необходимо.

Кстати, о деньгах. Если раньше большая часть бюджета в проектах строительства ЦОД уходила на закупку, транспортировку и поддержку оборудования, мощность которого по сегодняшним меркам была совсем небольшой. Серверы потребляли немного, счета за энергию приходили мизерные. Все изменилось: оборудование значительно нарастило мощности, электричество ощутимо подорожало, масштабы проектов увеличились в десять раз.

Специалисты считают, что большинство дата-центров «съедает» гораздо больше, чем необходимо. Конечно, при строительстве новых ЦОДов уже применяются разнообразные меры по сокращению энергопотребления, тем более что зачастую в ту местность, где идет строительство, доставить нужные мощности сложно. А у вашей компании есть свой ЦОД? Планируется? Вы уже составили смету будущих затрат на электричество?

Электропотребление полезной нагрузки ЦОД колеблется (растет и уменьшается) в течение всего жизненного цикла ЦОД как площадки, зависит от развития технологий и конъюнктуры ИТ-рынка в целом, а также погоды и общего климата, от качества самой энергии и квалификации персонала, управляющего объектом. Колебание электропотребления сложно предугадать, но можно наблюдать постоянно: каждые сутки, неделю, месяц, год

Пара слов о PUE

Насколько значительны или малы потери мощности на обеспечение фукционирования активного железа, расскажет показатель PUE - Power Usage Effectiveness. Существует целый ряд методик его измерения. Самый простой рассчитывается в один клик: разделите общую мощность, съедаемую дата-центром, на ту, которую потребляет именно ненасытная серверная часть. Если потери на инженерную инфраструктуру составляют 0% - это идеальная ситуация, и PUE будет равен единице. Значение в пределах от 1 до 3 – норма для большинства ЦОД. Кроме того, у PUE важно определить пиковое значение, достигаемое в экстремальных условиях, например, в большой мороз.

В целом, это весьма относительная метрика, хоть и считается ключевой. PUE бывают годовыми, среднемесячными и моментальными и на расчет зачастую влияют дополнительные коэффициенты – например, затраты на центральные инженерные системы зданий, в котором стоят сервера, или на устройства для резервного копирования, которые тоже любят электричество.

Меры по рациональному использованию ресурсов лучше принимать как можно раньше (то есть еще на этапе проектирования дата-центра), но и модернизация существующих объектов вполне возможна.

Снижаем энергопотребление

Меры по рациональному использованию ресурсов лучше принимать как можно раньше (то есть еще на этапе проектирования дата-центра), но и модернизация существующих объектов вполне возможна. Вот общий список возможных шагов:

- Внедряйте технологии виртуализации и высокоплотные блейд-сервера, чтобы ЦОД производил только полезную работу. Загружайте оборудование по полной или отключите его!
- Активно управляйте приложениями, балансируйте нагрузку.

- Применяйте системы измерения, контроля, мониторинга расхода электроэнергии и PUE в ЦОДе, позволяющие моделировать изменения инженерной инфраструктуры с прогнозированием результатов.
- Совершенствуйте систему охлаждения. По возможно применяйте фрикулинг, уходите от общепериметрального охлаждению к более локальному модульному, зонируйте ЦОД по разным признакам, соразмерно нагрузкам и плотности мощности. Контролируйте системы кондиционирования динамически.
- Не стройте ЦОД там, где нет возможности подключиться к сетям высокого напряжения. Рассмотрите вариант строительства собственного объекта генерации (оправдано для масштабных ЦОДОв).
- Выбирайте источники бесперебойного питания от ведоров-флагманов, предлагающих продукты с широкими возможностями смены режимов.

Используйте только необходимое в конкретный момент оборудование во всех частях ЦОДа, моментально отключая или даже выводя его из эксплуатации, чтобы ничего не простаивало и не функционировало вхолостую. Все вышеперечисленные меры способствуют сокращению энергопотребления и тепловыделения в дата-центр на 15-30%.
Контролировать энергоэффективность своего ЦОДа компания может как самостоятельно, так и с помощью подрядчика-интегратора, предоставляющего услуги профессионального управления. Это может быть дороже, но в долгосрочной перспективе эффективнее и с предоставлением гарантии. Проведя аудит площадки, подрядчик предоставит отчет и заключение о возможных мерах по улучшению эффективности потребления ресурсов.

Петр Царьков,
менеджер по продажам
решений и развитию бизнеса
Департамента инфраструктурных
решений Softline
Petr.Tsarkov@softlinegroup.com

«Приведу небольшой пример повышения энергоэффективности. В одном из первых ЦОДов в РФ, построенном еще в начале двухтысячных, требовалось разместить дополнительно 10 серверных стоек с общим потреблением 100 кВт. Но электромощности залов были уже ограничены, как и площадь под размещение новой ячейки.
Для решения проблемы было произведено обследование инженерной инфраструктуры, которое выявило, что кондиционеры находятся в режиме ежесуточной ротации с низким порогом входа горячего воздуха; нагревательные пароувлажнители стоят в каждом кондиционере; блоки вентиляторов - без регулирования скорости от зависимости нагрузки; очень хорошие, эффективные и дорогие чиллеры работают на устаревший график холодоснабжения 7-12°С; коридоры не имеют герметизации; в половине серверных шкафов не заглушены неиспользуемые юниты и т.д.
Мы предложили компании меры модернизации с целью повышения энергоэффективности, и вот что сделали:

- установили регуляторы частоты вращения вентиляторов, неэффективную ротацию каждые 24 часа сменили на постоянную работу в совместном режиме с неполной нагрузкой;
- 50% изначально ненужных пароувлажнителей убрали, а взамен 50% других установили ультразвуковые;
- график холодоносителя установили на значение10-15°С;
- в стойках установили заглушки;
- сделали герметизацию коридоров, что повысило вход горячего воздуха на кондиционеры.

В целом одни только модернизации по климату принесли + 70 кВт электроэнергии.
Вторым шагом стала модернизация электросистем (ИБП, электроосвещения, распределение), которая также выделила дополнительные необходимые мощности.
Отмечу, что если бы компания изначально реализовала проект на более эффективном оборудовании, с продуманными схемами климата и предписаниями по дальнейшей эксплуатации, то залы имели бы на 20% больше запаса площади для размещения серверных шкафов.»

Работать с умом

Безопасность человека – одна из важнейших задач на производстве. Современное решение «умные каски» на базе технологий Интернета вещей помогает обеспечивать безопасные условия труда и избегать серьезных рисков для здоровья людей и бизнеса. Подробнее о нем расскажут эксперты в области решений по промышленному Интернету вещей группы компаний Softline, Сергей Монин и Александр Захаров.

– Какие проблемы и задачи помогает решать инфраструктура «умных касок»?

– Руководителям промышленных предприятий хорошо известно, что нарушение техники безопасности чревато крупными штрафами, лишением свободы, репутационными потерями и, что самое главное, угрозой для жизни их сотрудников. Именно поэтому в современных условиях чрезвычайно важно контролировать людей в их рабочем пространстве.

Программно-аппаратный комплект «Умная каска» предназначен для обеспечения безопасности на территории производственных, добывающих и других предприятий. Система позволяет оперативно собирать информацию о соблюдении сотрудниками правил техники безопасности, об отклонениях от нормативов и вовремя предпринимать меры по их устранению.

Оператор получает в режиме реального времени информацию о том, надета ли каска на голову сотрудника, не случилось ли сильного удара по ней или не зафиксировано ли падения с высоты. Возможность измерять температуру внутри каски позволяет принимать решения в сложных ситуациях. Например, в случае, если температура близка к критической для человека, нужно ускорить операции спасения. Наличие датчика удара позволяет использовать и обратную связь – например, сотрудник может ударить три раза по каске, и оператор сразу же среагирует на то, что сотрудник хочет связаться с ним.

Сергей Монин

Александр Захаров

Для предотвращения опасных инцидентов, которые наносят ущерб здоровью работников и приводят к серьезным убыткам для бизнеса, функционал предусматривает постоянный контроль за местонахождением сотрудника и регистрацию всех событий на предприятии. Отслеживается не только вход в «красные зоны» и отклонения в деятельности сотрудников, также выявляется соответствие конкретному заданию, соблюдение режима труда и отдыха, анализируются «исторические» данные для выявления нетипичных форм поведения работника.

Аналогично исследуются параметры окружающей среды: выявляются неблагоприятные факторы, «нетипичные» тенденции, аварийные ситуации, по которым предоставляется точная информация.

– Почему это актуально на сегодняшний день?

– По данным Росстата, в 2017 г. на производственных предприятиях России произошел 5 371 несчастный случай с тяжелыми последствиями. Из этого числа более 50% происшествий стали следствием плохой организации труда и несоблюдения техники безопасности, к ним же относятся нарушения в применении средств индивидуальной защиты (СИЗ).

В связи с этим в декабре 2017 г. Россия присоединилась к концепции «нулевого травматизма», продвигаемой Международной ассоциацией социального обеспечения (ISSA). Это качественно новый подход к организации профилактики безопасности, гигиены труда и благополучия работников на всех уровнях производства. В соответствии с передовыми принципами Минтруд России подготовил проект изменений в Трудовом кодексе РФ.

В соответствии со ст. 212 ТК РФ и ст. 14 № 181-ФЗ «Об основах охраны труда в Российской Федерации», обязанности по обеспечению безопасных условий и охраны труда в организации возлагаются на работодателя. Современному предприятию для выполнения норм ТК РФ необходимы новые и эффективные технологии, которые могут идентифицировать потенциальные угрозы и воздействовать на них, обеспечивать оповещение в режиме реального времени и глубокую аналитику, которая поможет предотвращать подобные инциденты.

Используя интеллектуальные СИЗ и носимые устройства, такие как «умная каска» от Softline на платформе промышленного Интернета вещей «Connected Workers», предприятия могут обеспечить наивысший уровень безопасности и производительности.

– Каким образом реализуется решение? Какие применяются технологии, устройства?

– Архитектура решения «Умная каска» позволяет довольно быстро и легко развернуть аппаратно-программный комплекс на предприятии заказчика. Он состоит из защитных касок с электронными модулями Softline, которые отправляют сигналы на базовую станцию Lora IoT. Она передает полученные данные в обычную сеть по Ethernet-кабелю или через оператора сотовой связи по протоколу LoRaWAN. Данный протокол минимизирует затраты энергии батарей и обеспечивает очень хорошее распространение сигнала – до 10 км на открытой местности или до 2 км в городе.

Сбор данных от «Умных касок», хранение их в базе данных, оперативную аналитику событий и визуализацию обеспечивает программное обеспечение «Аналитический сервер». Развернуть его можно как в облаке Softline Cloud, так и в облаке Microsoft – MS Azure. Предоставление Softline доступа к программному обеспечению для управления программно-аппаратным комплексом позволяет заказчику не заботиться о серверах, базах данных, лицензиях и других проблемах.

Существуют также и другие варианты развертывания: On-premise – управление программно-аппаратным комплексом на сервере или виртуальной машине в ЦОДе заказчика – и геопозицирование. Оно может производиться на открытой местности – трекер (модуль) GPS/Glonass и в закрытом помещении – система локального позиционирования UWB.

– Какие возможности предоставляют «умные каски»?

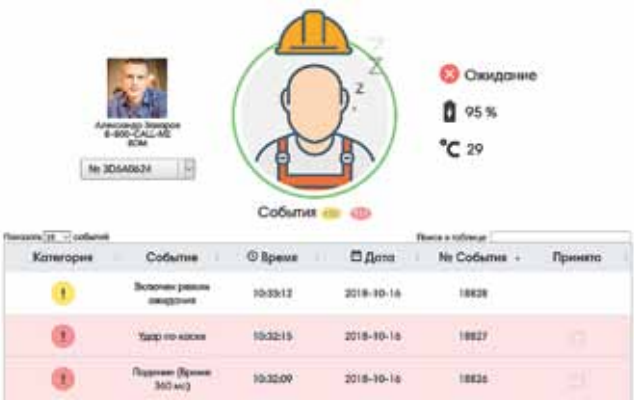
– Если суммировать, то функционал решения широк и многообразен. В режиме реального времени контролируется:

- факт наличия каски на голове сотрудника,
- информация о серьезных ударах по каске,
- наличие фазы свободного падения сотрудника с высоты от 1.0 метра,
- ориентация каски в случае длительной неподвижности (на боку, вверх дном...),
- температура, заряд батареи.

– Расскажите об успешно реализованных проектах. Почему заказчики выбрали именно это решение?

– Мы провели ряд пилотных запусков решения «Умные каски» на крупных предприятиях различных секторов промышленности в России и СНГ. Согласно программе и методике испытаний, были получены положительные заключения – подписаны акты о том, что АПК «Умные каски» полностью соответствует «техническим заданиям» и может быть внедрен на предприятиях. Успешно запущены тендерные процедуры

Заказчики выбирают «умные каски», так как решение полностью отвечает необходимым требованиям и четко решает задачи по охране труда и промышленной безопасности. Оно оптимально по цене и срокам реализации, а платформа «Connected Workers» постоянно развивается и может быть настроена под индивидуальные и интегрирована с другими «умными» СИЗ (очки, наушники и т.д.), а также внутренними системами контроля.



Решение позволяет производить:

- самодиагностику,
- вызов оператора – «мне нужна помощь»,
- интеграцию с модулем оперативного оповещения руководства (SMS/Whatsup/Viber/E-mail...),
- определение местонахождения работника и регистрацию событий на территории предприятия с помощью модулей GPS/Glonass,
- интеграцию с системами позиционирования реального времени UWB.

В процессе реализации и развития платформы «Connected Workers» возможны:

- интеграция и дополнительная функциональность с другими носимыми СИЗ (очки, наушники и т. д.),
- выпуск варианта NBIoT вместо модуля Lora,
- возможность кастомизации интерфейса и отчетности под каждого заказчика.

Инфраструктура «умных касок», созданная инженерами группы компаний Softline, способна сократить издержки, обеспечить непрерывность производственного процесса, а также поддерживать высокий уровень безопасности. Это решение отвечает одному из главных требований крупнейших российских предприятий – вести свою деятельность без аварий и жертв, а работать безопасно – значит, работать с умом.

Мультиполезность мультимедиа

Под мультимедийным комплексом в самом общем смысле обычно понимают программно-аппаратное решение для проведения в конкретном помещении заседаний, совещаний, презентаций, обучения и прочих мероприятий, в том числе в режиме видеоконференцсвязи. Получается, что это целая совокупность «железных» и софтверных составляющих. Благодаря огромному разнообразию компонентов, мультимедиа систему можно разработать под любые задачи; областей применения можно назвать массу, они зависят от назначения/сферы деятельности предприятия.

Например, мультимедиа технологии применяются в ситуационных центрах оперативного реагирования МЧС, МВД, РЧЦ для взаимодействия со смежными органами. Диспетчерским службам мониторинга компаний, работающим в энергетической сфере, мультимедийные комплексы позволяют осуществлять мониторинг состояния систем отопления, газотранспортной системы и т.д.

Мультимедиа комплекс можно разделить на следующие подсистемы:

- отображения;
- конференцсвязи;
- синхронного перевода и голосования;
- обработки звука, аудиокоммутации и звукоусиления;
- технологического телевидения;
- протоколирования записи и трансляции;
- коммутации видеосигналов;
- управления;
- бесперебойного электропитания.

Ситуационные центры

Проекты по созданию ситуационных центров — это проекты государственного уровня, инициированные приказом Президента, распространяющимся на губернаторов всех регионов РФ. Залы ситуационных центров оснащаются оборудованием с функциями ведения записи, протоколирования, а также софтверной частью межведомственного взаимодействия с аналитическими модулями для работы правительственных органов. Ситуационные центры аттестуются по требованиям безопасности Гостайны.

В МЧС, МВД, ведомственных структурах — свои ситуационные центры. Сеть камер видеонаблюдения в городе, ведущих обзор с разных ракурсов, в оперативном режиме помогает службам коммуницировать между собой и принимать быстрые обоснованные решения.

Конференции и другие мероприятия

Во всех российских регионах строятся залы для правительственных мероприятий, которые оборудуются системами конференц- и видеосвязи. Залы Законодательного собрания, а также залы заседаний депутатского состава обязательно должны быть оснащены системами синхронной видеозаписи и протоколирования, а желательно — и системой голосования (программная часть таких систем отличается сложными алгоритмами и интегрируется с другими конференцсистемами, поэтому обычно создается под каждый зал индивидуально и по регламенту конкретного законодательного органа). В процессе обсуждения того или иного вопроса на мероприятии, люди обычно изучают сопровождающие документы, которые могут отображаться не только на большом проекторе, дублирующих мониторах на рабочих местах, но и на персональных мобильных устройствах. Это очень удобно — подключившись к серверу, иметь доступ к обсуждаемому документу прямо на своем планшете или ПК и просматривать материалы в комфортном для себя режиме. Мы рекомендуем использовать планшеты с защищенным доступом.

Для образовательной сферы

Мультимедиа технологии ситуационных центров работают и в сфере образования: по всей России организованы центры обработки экзаменов для сдачи школьниками ЕГЭ. Видеокамеры в зале осуществляют наблюдение за сдающими экзамен детьми; на видеостену выводятся те или иные данные. Камеры могут зафиксировать факт списывания. Видеоролики хранятся в архиве и могут применяться для апелляций.

Softline выполняет любые работы в рамках комплексных мультимедиа проектов— начиная от прокладки кабеля в здании и заканчивая разработкой специализированного ПО и поставки любого мультимедиа-оборудования. ▮

Свежие проекты

Оборудование зала заседаний правительства Ханты-Мансийска

В результате проекта в зале заседаний правительства Ханты-Мансийска специалистами Softline были модернизированы следующие системы:

- технологического телевидения (интегрирована с существующей системой ВКС);
- отображения;
- обработки и микширования звука;
- коммутации видео;
- протоколирования заседаний;
- управления.

Кроме того, появилась возможность подключения пресс-служб к мероприятиям.

Модернизация зала заседаний Законодательного собрания Ямало-Ненецкого автономного округа

Инженеры Softline модернизировали зал в части мультимедиа-систем, автоматизировали процессы проведения заседаний депутатов, а также провели реконструкцию помещения.

По всем вопросам обращайтесь к **Геннадию Низовцеву,**
руководителю направления продаж мультимедийных систем компании Softline.
Gennadiy.Nizovtsev@softline.com

Переключи канал!

Как построить долгосрочные отношения с клиентом? - Отлично его обслуживать. Залог получения радующих вас бизнес-результатов — забота о тех, кто к вам обращается, особенно если вы знаете, как монетизировать обращения. Объединить все каналы общения вокруг клиента — то есть работать по принципу омниканальности — сегодня не тенденция, а необходимость, продиктованная условиями суровой конкуренции за потребителя.

Сергей Фортунатов, Руководитель направления «Телефония, контакт-центр, ВКС» Softline

Омниканальный подход подразумевает кропотливое «изучение» истории каждого клиента, сбор этакого досье. Что бы ни сделал клиент (совершил покупку у вас на сайте, заполнил анкету, выбрал товар, но не оплатил и т.д.), о чем бы ни сообщил или заявил, с какими бы проблемами ни приходил в течение последних лет – вся информация будет у оператора контакт-центра. По любым каналом обращения омниканальное решение автоматически собирает, сохраняет и передает данные обо всех действиях операторам.

Как выглядит плохой контакт-центр

Не удивляйтесь, но многоканальный контакт-центр – значит устаревший, и значит плохой. Почему? Многоканальность вовсе не подразумевает, что многочисленные способы взаимодействия будут работать как единая система. К сожалению, они остаются разрозненными, отделенными друг от друга. Как это выглядит на деле, вы наверняка испытывали «на собственной шкуре»: у вас есть вопрос, и вы задаете его через мессенджер. В ответ получаете следующее: «Перезвоните по номеру 8-800.. и получите развернутую инструкцию». Вы вынуждены самостоятельно звонить (хотя возможно у вас в данную минуту нет такой возможности!) и снова рассказывать о своей проблеме. Бывает, что клиентам приходится сменить три канала обращения, прежде чем удается «достучаться». На уровень их удовлетворенности это вряд ли влияет позитивно... Итог – бизнес-результатов нет.

Как это исправить

Омниканальность, в отличие от многоканальности, основана на понимании, что дополнительные способы взаимодействия сами по себе большого толчка бизнесу не придадут. Важен не канал коммуникации, а то, как вы собираетесь клиенту помочь. Сосредоточиться стоит на двух вещах: в чем суть обращения клиента; как решить вопрос.

Система омниканального контакт-центра в идеале интегрируется с CRM и решением для бизнес-аналитики – для того, чтобы собирать в единую картину все активности с клиентом, все, что делал он и все, что сделано для него. Так компания будет следить за решением задач, поступающих от заказчиков, по всем своим системам. Кроме того, станет понятно, какой канал

коммуникации каждый клиент использует чаще всего. То, что применяется чаще других, обычно является самым удобным для конкретного человека. Это может быть, например, переписка по электронной почте или услуга обратного звонка. Зная такие детали, операторы экономят собственное время, быстрее и правильнее реагируют, и таким образом компания выигрывает – и клиент, разумеется, тоже.

Что еще дает омниканальность

Основа программного продукта – платформа, которая обрабатывает и звонки, и почту, и чаты, и смс, и видео. Речь и текст анализируются особыми интеллектуальными модулями, которые способны, как в автоматическом режиме найти и предоставить ответ клиенту на запрос, так и перенаправить обращения к определенным специалистам. А системы статистики загрузки операторов (WFM – workforce management) позволят регулировать работу контакт-центра в реальном времени и в пиковые часы обеспечивать присутствие на рабочих местах наибольшего количества сотрудников. Команда операторов может быть территориально-распределенной, работающей удаленно и в различных часовых поясах.

О решениях

Систему можно построить, используя целый ряд продуктов от разных производителей, или же предпочесть единое решение. В первом случае интеграция, настройка и поддержка могут быть несколько затруднены, зато компания выиграет в стоимости владения. Иногда ввиду определенных обстоятельств компания вынуждена собирать воедино набор разрозненного ПО, зато, победив раздробленность, получит чудеса эффективности. Другая альтернатива – коробочное решение корпоративного уровня с готовыми пресетами настроек и разнообразными функциональными возможностями.

Осуществляйте работу с клиентами компании по всем каналам, будь то входящие и исходящие звонки, электронная почта, чаты, SMS, ко-браузинг, социальные сети, общение через мобильные приложения. Сотрудникам контакт-центра будет видна вся история общения с заказчиками. Работу операторов будет отслеживать подсистема анализа, контролирующая продуктивность процессов для последующих отчетов руководителям, а также скорость ответов, продолжительность ожидания, особенности трафика и т.д. Ориентируясь на данные о предыдущих обращения клиента, IVR-система сможет сортировать опции голосового меню в зависимости от того, что человека интересует.

Набор разных систем от различных вендоров или «все в одном» - что лучше, подскажут консультанты Softline.

Доступность

Нужны ли высококлассные омниканальные системы небольшим компаниям? Это зависит от особенностей бизнеса, количества обращений и предпочтений клиентов. Интернет-магазинам, финансовым организациям, образовательным и сервисным учреждениям – безусловно, да. Стоимость решений сегодня вполне адекватна и доступна не только крупным организациям, но и тем, кто планирует модернизировать свой контакт-центр, даже если там всего 5-15 операторов.

В чем преимущество омниканального подхода?

1. Подход к клиенту становится более персонализированным; компания – ближе к своим заказчикам. Растет лояльность и доверие аудитории.
2. Клиентский сервис интегрируется в каналы продаж – физические и онлайновые. Продажи растут.
3. Компания трансформируется и выходит на стратегически новый уровень цифровизации. ▮

На ваши вопросы ответит **Сергей Фортунатов**,
Руководитель направления «Телефония, контакт-центр, ВКС» Softline
Звоните: **+7 (495) 232-00-23 доб. 1571**
Пишите: **Sergey.Fortunatov@softline.com**

Виртуализация сегодня

Максим Пуха, руководитель отдела виртуализации и резервного копирования, и **Дмитрий Галкин**, руководитель группы технической экспертизы департамента инфраструктурных решений Softline, рассказали SLD о выгодах виртуализации и о том, на что нужно обращать внимание при внедрении решений.

– Какие решения предлагает Softline в области виртуализации? Что наиболее востребовано сегодня?

– Мы называем свое направление программно-определяемые дата-центры и пользовательская мобильность. Современный подход к созданию передовых ЦОДов подразумевает использование технологий виртуализации вычислительных мощностей, СХД, сетей, систем автоматизации и т.д. К корпоративной мобильности относится виртуализация рабочих столов пользователей и дополнительный класс решений EMM (Enterprise mobility management), которые отвечают за управление мобильными устройствами.

Направление пользовательской мобильности сегодня особенно востребовано. Удаленные сотрудники всегда на связи, могут выполнять свою работу практически в любых условиях, будь то командировка или другое вынужденное отсутствие в офисе. К тому же это на 100% соответствует тенденции цифровой трансформации бизнеса. Подключения пользователей всегда защищены и позволяют оставлять данные внутри компании, а это хорошо еще и с точки зрения безопасности. Таким образом, пользовательская мобильность – это сейчас тренд номер один.

Виртуализация – это одно из самых сильных направлений компании Softline с профессиональной командой технических специалистов. Мы обладаем богатым опытом, так как работаем с данными технологиями практически с начала их существования. В наших интересах предлагать проверенные, надежные решения и реализовывать проекты с минимальными сроками и рисками.

Виртуализация серверов пользуется спросом для решения задач организации катастрофоустойчивости инфраструктур. Раньше стоимость каналов связи между дата-центрами была высокой, и это довольно сильно тормозило развитие направления, но сейчас она значительно снизилась, и благодаря этому появился довольно высокий спрос. Можно сравнительно за небольшие деньги обезопасить свой бизнес даже в случае чрезвычайных обстоятельств. Поэтому виртуализация серверов – это тренд номер два.

Гиперконвергенция или централизованное управление СХД, сетевым оборудованием и средствами виртуализации – достаточно свежая технология. Первыми на нее обратили внимание крупные компании, такие как Google, Facebook, «Вконтакте». У них очень большой прирост данных, высокая нагрузка и особая требовательность к производительности дисковых систем. Тем не менее гиперконвергентные решения сейчас стали гораздо дешевле, и ими активно начинают интересоваться заказчики из среднего сегмента бизнеса.

– Каковы основные преимущества для клиентов, использующих виртуализацию?

– Технология виртуализации реализуется за счет программных продуктов, и это уже само по себе выгодно, так как ПО не подвержено амортизации в отличие от физического оборудования. К примеру, серверы и СХД служат 5-7 лет, а затем нужно приобретать новые. Сетевые устройства служат дольше, но при этом скорее устаревают морально – технологии сейчас развиваются с фантастической скоростью. Зачастую для устаревших устройств уже нет новых прошивок, поэтому даже если устраивает производительность, то какого-то функционала может начать не хватать, и для того, чтобы его расширить, необходимо полностью менять железо.

С виртуализацией не существует таких проблем, потому что она опирается на классическую архитектуру x86, которая универсальна и поддерживает любые обновления ПО, а они всегда приходят вовремя и сохраняют должный уровень инфраструктуры.

Преимущества виртуализации для заказчика – это всегда самые новые прошивки, прогрессивные технологии, широкие функциональные возможности. Поддержка, простое масштабирование, своевременная замена оборудования, централизованное управление, программная автоматизация – всё это позволяет значительно повысить качество администрирования, а также гибко управлять своими информационными ресурсами и сокращать расходы.

– Почему руководители часто не могут решиться на реализацию полномасштабного виртуализационного проекта?

– Очень часто в крупных компаниях сотрудники ИТ-отдела относятся к существующей ИТ-инфраструктуре очень консервативно, полагая, что внедрение новых технологий может отрицательно сказаться на их работе. Например, администраторы СХД могут опасаться, что гиперконвергенция сделает их менее востребованными специалистами, или «не взлетит» по причинам низкой производительности или недостаточному уровню отказоустойчивости. Однако это не так, и специалисты должны понимать, что чем больше они имеют компетенций, тем более ценными кадрами они являются.

Или, например, некоторые компании не хотят реализовывать проекты по модернизации сетей из-за разросшейся за много лет сетевой инфраструктуры. Сеть – это кровеносная система центра обработки данных, и там очень важна постоянная доступность. Виртуализация же огромного количества физического оборудования представляется очень большим и сложным проектом, где очень легко допустить ошибки, которые приведут к простоям, отключению ряда сервисов или полной недоступности. Конечно, всё это нужно учитывать и быть достаточно квалифицированным для решения данных вопросов.

Максим Пуха

– На что стоит обратить внимание при принятии решении о внедрении?

– Главное, что мы бы советовали, – это доверить внедрение профессионалам. Иногда заказчики сами пытаются реализовывать тяжелые решения, в результате допускают ошибки и получают неэффективно работающую ИТ-систему, либо тратят на ее внедрение в несколько раз больше времени, чем опытные специалисты. У профессионалов за плечами далеко не один десяток разнообразных проектов, за это время уже даже на интуитивном уровне появляется понимание того, где могут возникать проблемы и как их избежать.

Дмитрий Галкин

К примеру, проекты по физическому переезду оборудования достаточно сложны. Им предшествует очень серьезная подготовка, разработка запасных планов, резервное копирование, страхование устройств, организация подменного фонда оборудования на случай форс-мажоров. Также тщательно необходимо составить план-график работ, чтобы не допустить простоев в рабочее время. Цена ошибки здесь очень высока, поэтому продуманное планирование и опыт реализации аналогичных проектов играют ключевую роль.

Что касается производителей ПО, то во многом они идентичны, но отличаются разными подходами. Softline – мультивендорная компания, поэтому мы можем помочь подобрать оптимальное решение, исходя из индивидуальных предпочтений. Чаще всего имеют значение условия технической поддержки, уровень технологического развития, интеграция с уже внедренными в инфраструктуру решениями.

Виртуализация – это одно из самых сильных направлений компании Softline с профессиональной командой технических специалистов. Мы обладаем богатым опытом, так как работаем с данными технологиями практически с начала их существования. В наших интересах предлагать проверенные, надежные решения и реализовывать проекты с минимальными сроками и рисками. ▮

Преимущества виртуализации для заказчика – это всегда самые новые прошивки, прогрессивные технологии, широкие функциональные возможности.

Примеры реализованных проектов

СЕНТИНЕЛ КРЕДИТ МЕНЕДЖМЕНТ

Модернизация IT-инфраструктуры регионального офиса «Сентинел Кредит Менеджмент»

MTS

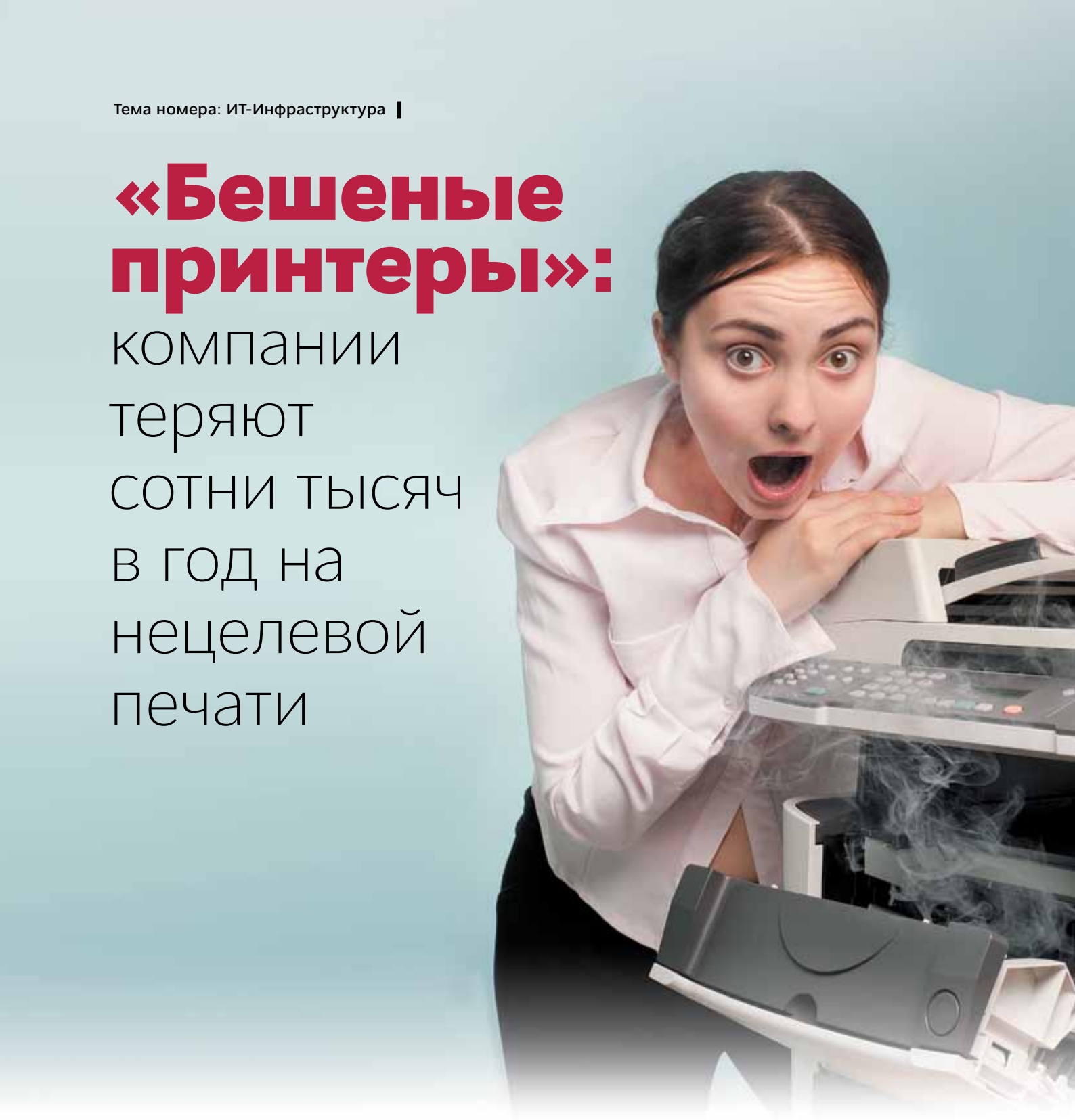
Построение инфраструктуры доступа к приложениям на базе терминальных технологий Citrix для МТС

РОССИЯ

Softline оптимизировала работу с бизнес-приложениями сотрудников авиакомпании «Россия»

Виртуализация инфраструктуры ОАО «Дальневосточная генерирующая компания» на базе решений Microsoft System Center

«Бешеные принтеры»: компании теряют сотни тысяч в год на нецелевой печати



Даже небольшие предприятия могут понести миллионные убытки по причине недостаточного контроля за работой офисных принтеров – к такому выводу пришли эксперты Softline, опросив потенциальных заказчиков в регионах и проанализировав использование оборудования для печати. Пятая часть документов, распечатываемых на офисных принтерах, не относятся к рабочему процессу. Порядка 15% отпечатков не востребованы — они так и остаются лежать в лотке принтера, или немедленно отправляются в корзину. Нецелевые отпечатки и невостребованные документы в пересчете на каждого сотрудника несут работодателю более 12 тыс. руб. убытка в год.

Полмиллиона в шредере

Александр Петров, руководитель направления сервисов печати Softline

Согласно предварительному аудиту инфраструктуры печати, который Softline проводит среди своих действующих и вероятных заказчиков, в месяц на каждого сотрудника коммерческих предприятий и государственных организаций, имеющего доступ к принтеру со своего рабочего места, приходится порядка 1 тыс. отпечатков. При этом рабочей необходимостью обусловлено появление лишь 65% от общего числа оттисков. В остальные 35% входят отпечатки, не имеющие отношения к рабочим задачам сотрудников (это примерно 20% от 1 тыс. среднестатистических отпечатков в месяц), а также невостребованные документы, которые напечатаны, но остаются лежать в приемном лотке принтера или сразу же отправляются в корзину для бумаг (еще 15%). Стоимость одного оттиска, состоящая из затрат на оборудование, его ремонт и обслуживание, расходные материалы и прочее – минимум 3 рубля. А значит, потери компании от нецелевого использования печатного оборудования на каждого сотрудника в месяц составляют более 1 тыс. рублей, или более 12 тыс. рублей в год.

Таким образом, даже небольшая компания, число сотрудников в которой условно составляет 100 человек, а принтером активно пользуется четверть из них, в год теряет сотни тысяч рублей. Чем значительнее численность коллектива и чем больше документооборот, тем выше потери.

Немалые издержки работодатель несет, когда офисные сотрудники самостоятельно занимаются исправлением мелких неполадок – устранением заторов бумаги, пополнением запасов расходных материалов в устройстве, перезагрузкой устройств из-за сбоев. Один такой эпизод занимает в среднем три минуты, при этом, проблемным оказывается в среднем каждый десятый эпизод печати, таким образом, если за месяц сотрудники отправляли документы в печать тысячу раз, то число подобных эпизодов дойдет до ста, и потери работодателя при средней цене часа работы сотрудников в 200 рублей (с учетом налогов) составят 1 тыс. рублей в месяц, или 12 тыс. рублей в год. Опять же – чем больше у вас сотрудников, и чем чаще они пользуются принтером, тем выше будет цена инцидентов.

Взять под контроль издержки на печать можно двумя способами. Первый – организовать контроль печати, например, авторизацию работы с принтером или многофункциональным устройством. Второй способ – закупать услугу печати как управляемый сервис у специализированного поставщика. В этом случае заказчик платит только за конкретный отпечаток.

«В условиях, когда каждый сэкономленный рубль ценится так же высоко, как заработанный, заказчики стали гораздо внимательнее относиться к издержкам и искать способы их снижения. «Бешеные принтеры» можно обуздать, внедрив с помощью ИТ-консультанта системы управления печатью, либо вообще начав закупать сервис печати у поставщика такой услуги. Предприятия финансового сектора охотнее других принимают новую модель потребления услуг печати. За ними идут госструктуры и телекоммуникационные компании», - говорит Александр Петров, руководитель направления сервисов печати группы компаний Softline.

Как укротить принтер

Взять под контроль издержки на печать можно двумя способами. Первый – организовать контроль печати, например, авторизацию работы с принтером или многофункциональным устройством. Для этих целей подойдут карты, которые используются для доступа в офис. «Печать по карточкам» позволяют контролировать активность использования печатного оборудования конкретным сотрудником. В том случае, если его работа не предполагает постоянного обращения к бумажным документам, это может стать поводом выяснить причину аномальных объемов пользования принтером. «Мы всегда рекомендуем компаниям информировать коллектив о внедрении таких решений: зная о том, что информация о количестве и содержимом документов будет открыта для

Рабочей необходимостью обусловлено появление лишь 65% от общего числа оттисков. В остальные 35% входят отпечатки, не имеющие отношения к рабочим задачам сотрудников.

непосредственных руководителей и доступна службе безопасности, сотрудник каждый раз будет взвешивать необходимость создания бумажной копии документа или использования техники для печати личных документов», - говорит Александр Петров. Сейчас решения для управления печатью пользуются наибольшей популярностью у крупного бизнеса, для которого потери от неэффективного использования средств печати могут нести десятки миллионов в год – по оценкам эксперта, они занимают порядка 65% в общей структуре продаж.

Второй способ – закупать услугу печати как управляемый сервис у специализированного поставщика. В этом случае заказчик платит только за конкретный отпечаток. Все остальные процессы и задачи – подбор оборудования, подключение и конфигурирование принтеров, пополнение запасов расходных материалов в самом устройстве, устранение неполадок, подмена оборудования в случае неисправности, описание процессов, связанных с печатью и т.д. – берет на себя поставщик услуги. Также поставщик разрабатывает новые политики печати для компании заказчика, распределяет нагрузку на принтеры, внедряет системы контроля печати, чтобы сократить число нецелевых и невостребованных оттисков. По опыту Softline, в рамках оказания сервиса печати под ключ один отпечаток обходится клиенту примерно в 2 рубля – на 1,5 рубля меньше, чем в случае самостоятельного содержания инфраструктуры и об их обслуживании при аналогичном уровне оказания услуг внутренним заказчикам.

Несколько лет назад решение о передаче управления копировальной техникой на аутсорс приняло руководство Альфа-Банка. Совместный проект с компанией Xerox помог финансовой организации снизить расходы на печать на 47% и установить более прозрачную систему управления расходами на печать. Оптимизация проводилась в центральных и дополнительных офисах, а также операционных кассах банка, что в целом составляет порядка 90 помещений, в которых работают более 6 тыс. человек.

Бонус для ИБ

Помимо очевидной экономии на количестве бумажных документов, управление печатью может снизить вероятность утечки информации. Согласно ряду независимых исследований вендоров, разрабатывающих и внедряющих программные решения по управлению инфраструктурой печати, до 40% инсайдерской информации выносится за пределы компании именно на бумажных носителях. Решения по управлению печатью позволяют сохранить копию любого документа, отправленного на печать или сканирование, отправить копию в архив, к которому имеет доступ служба безопасности. Инструменты, позволяющие контролировать содержимое документов и сохранять информацию о них, есть и в случае использования услуг аутсорсинга печати.

«В моей практике были живые примеры, когда использование решения для управления печатью помогло избавить компанию от утечек информации. Одна крупная торговая компания, акции которой размещались на бирже, обратила внимание на необоснованные скачки курса собственных ценных бумаг (до 12% за день), появилось подозрение об утечке информации. Компания внедрила решение MyQ с функциональностью так называемой «теневой копии» - копия каждого документа, отправленного в печать, сохранялась в системе в виде pdf с указанием имени пользователя и хранилась на сервере. Таким образом компании удалось выявить группу инсайдеров и снизить потери на колебаниях курса», - приводит пример Александр Петров.

Александр Петров ответит на ваши вопросы лично
Пишите: **Al.Petrov@softline.com**

От импортозависимости к импортозамещению. Безопасно и планомерно

Управление доступом на внутренний рынок – это не российская «инновация», а инструмент, широко используемый в мире для стимулирования развития внутренних производителей и снижения зависимости от импортируемых товаров и технологий. Весь прошлый век данным инструментом активно пользовались Соединенные Штаты Америки, Китай, Великобритания, Бразилия и многие другие страны. Если мы говорим о текущей активности нашего государства в области импортозамещения информационно-коммуникационных технологий (ИКТ) в России, то это, по сути, необходимость на пути строительства цифровой экономики.

Дмитрий Сорокин, руководитель отдела развития продаж отечественного ПО, рассказал, как компания Softline помогает заказчикам снизить риски от введения ограничительных мер со стороны правообладателей зарубежного ПО и поэтапно перейти на использование отечественных программных продуктов.

Что такое импортозависимость ИТ в РФ?

Исторически в России сложилась ситуация, в которой мы в основном используем программные продукты лидеров-разработчиков ПО (Microsoft, IBM, Oracle), которые в настоящее время доминируют на глобальном рынке. Их лидирующее положение возникло не за один год, и является результатом эффективного использования тех условий, которые были для них доступны на первом этапе развития на внутренних рынках и экспансии на нашем рынке ИТ. Но несмотря на их глобальное присутствие, они все же находятся под юрисдикциями конкретных стран, а точнее, в большинстве случаев, конкретной страны, создавшей все необходимые условия для активного роста.

Вместе с благоприятными условиями для роста правообладатели ПО получили прямую зависимость от юрисдикции стран, в которых они находятся. Опосредованно мы, пользующиеся на территории РФ иностранными продуктами, зависим от регуляторов другой страны, которая может путем воздействия на правообладателей добиться определенных негативных последствий для нас.

Зависимость – явление негативное потому, что быть зависимым – значит быть управляемым. Есть примеры, когда импортозависимость в явном виде была использована в прошлом, и есть предпосылки прогнозировать, что будет использоваться против нас в будущем, причем в еще более жестких формах. Через наше зависимое положение оказывается прямое внешнее воздействие на политические и экономические интересы нашей страны.

Нужно обратить внимание, что это воздействие в первую очередь производится даже не на государственные учреждения, а на энергетические, нефтегазовые, оборонные предприятия и даже банки.

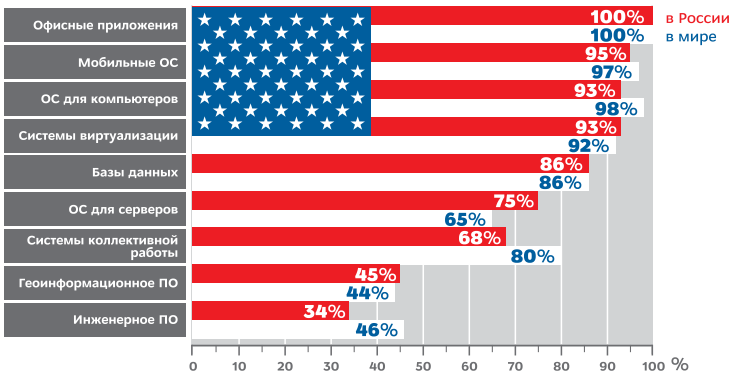


Диаграмма из презентации Министра Минкомсвязи Никифорова Н.А., 2016

Весь тренд импортозамещения направлен на то, чтобы не оказаться в изолированной и парализованной стране. Цифровая экономика – это не просто модный тренд, а, как говорят регуляторы, основной шанс нашей страны прорваться в лидеры среди других мировых держав.

Как государство стимулирует развитие разработок отечественных продуктов?

Разрабатываются новые нормативные документы, появляются специализированные реестры и методические рекомендации, работают программы господдержки для того, чтобы помочь промышленности и критически важным отраслям, уже попавшим под зависимость, во-первых, выйти из-под нее, а, во-вторых, в рамках программы по цифровой экономике, сделать тот самый прорыв. Ведь мы имеем хорошую интеллектуальную базу.

Импортозамещение – не только санкции с внешней стороны и ответные запретительные меры со стороны нашего государства, но и различные программы поддержки, финансирования, кредитования на льготных условиях, направленные на развитие внутреннего потенциала.

Уже давно существуют программные разработки наших специалистов, которые пользуются большим спросом по всему миру. Например, антивирусное ПО Касперского или коммуникационная платформа CommuniGate Pro. Для федеральных и региональных государственных организаций Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации уже разработало и приложило конкретные методические рекомендации, которые позволяют уйти от резких шагов и при помощи поэтапных действий планомерно перейти на использование отечественных программных продуктов и решений, созданных на их основе. Насколько известно, в планах у данного Министерства создать подобные методические рекомендации и для коммерческих организаций с государственным участием.

Ключевой момент – стать государством, где точки нашего потенциального роста будут выявлены, переведены в цифровой формат, будут развиваться и контролироваться, без воздействия иностранных регуляторов.

Что предлагает Softline заказчикам на пути к независимости в сфере ИКТ?

Softline предлагает стать доверенной компанией-партнером, готовой помочь на уровне перехода к независимости от внешних рисков. В компании работает специальный отдел «Отраслевые решения», который помогает подготовить и построить отраслевые специфические решения, которые еще не существуют в готовом виде, но в рамках цифровой экономики их можно и нужно создать, чтобы обеспечить точки контролируемого роста и достигнуть необходимых результатов.

Softline наработал большой практический опыт и приобрел высокую компетенцию в области внедрения отечественного программного обеспечения и оказания всесторонней помощи заказчикам. В настоящее время мы предлагаем не просто софт, а различные сервисы, интеграцию, проведение исследований. Если посмотреть на все программные продукты, которые есть в нашем портфеле, ценность представляет не то, что мы просто говорим о нем, а то, что вокруг каждого ПО мы выстраиваем целые «экосистемы» сопроводительных услуг. Они позволяют заказчику купить российское ПО в Softline без рисков, связанных с непониманием или незнанием особенностей того или иного программного продукта. Softline обеспечивает заказчику прямой доступ к необходимой персонифицированной помощи желаемого формата: будь то обучение, внедрение, аутсорсинг или помощь при тестировании.

Дмитрий Сорокин, руководитель отдела развития продаж отечественного ПО

Существует ли потенциал у отечественных ИТ-разработок выйти на новый глобальный уровень?

Во время подъема мировых информационных технологий в России был сложный период времени, и создатели ПО были вынуждены продавать свои разработки продавать за рубеж. Приведу пример. Компания CommuniGate на рынке уже 25 лет, и ее продукты используются, например, компаниями NASA, SITA и многими другими. Ее самый покупаемый и широко известный в мире продукт – коммуникационная платформа CommuniGate Pro, объединяющая в себе готовые к использованию почтовую систему, сервис мгновенных сообщений, IP-телефонию и продвинутый API. У нас были и есть российские разработки, и наши продукты используются по всему миру. Но в тот момент, когда сфера ИКТ начала активно развиваться, наиболее перспективным рынком был зарубежный. Мы пришли к этому позднее. И сейчас после применения нашими регуляторами действий по импортозамещению в ИКТ, российский производитель CommuniGate активно продает и на российском рынке.

Атомные и военные технологии, прикладные ПО – эти отрасли всегда использовали отечественное программные продукты. Но эти разработки заточены в первую очередь на результат и безопасность, а не на удобный пользовательский интерфейс. Такой софт способен делать «удивительные»

вещи, но он не рассчитан на массового потребителя. Кроме того, чтобы массовая аудитория приняла это, требуются очень большие финансовые затраты.
Почему США в определенный момент времени стали лидером в сфере ИТ? Это не стечение обстоятельств или исключительная гениальность. У них был поддержка со стороны государства и необходимое время.
Сейчас в нашей страны благодаря программам поддержки становления цифровой экономики и промышленности идет активное содействие конкретным отраслям. При этом эти программы поощряют использование отечественного ПО, обеспечивающего нам тот самый «ИТ-суверенитет», льготами и субсидиями.

Верно ли утверждение, что события 2014 года, связанные с санкциями, стали основным драйвером импортозамещения ИТ в РФ?

До 2014 года задача по импортозамещению была, скорее, факультативной. То есть было понимание о необходимости, но вопрос не стоял остро. И из факультативной задачи, это вдруг стало одной из важных задач, переросло в конкретную текущую потребность – обеспечение безопасности и ИТ-суверенитета страны.
Все эти программы по становлению цифровой экономики готовились давно, но это не стояло на основной повестке дня. Но на самом деле одним из самых больших драйверов импортозамещения стали реальные санкции иностранных государств.

Ключевой момент – мы те, кто побуждает обратить внимание на тему импортозамещения, и применить её, постепенно делая шаги в «цифровую экономику». Наша цель – стать вашим доверенным партнером в непростой для вас период.

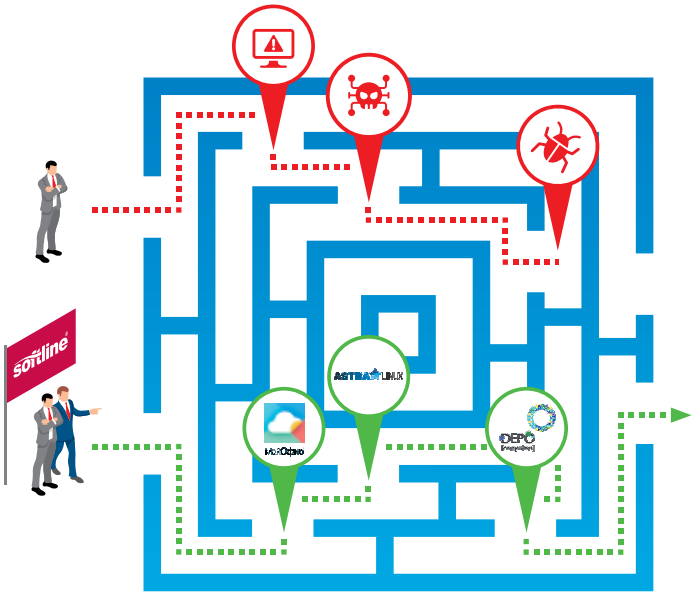
Если сократить использование иностранных разработок в пользу отечественных, возможно ли решить проблему введения правообладателем зарубежного ПО запретительных мер?

Softline помогает заказчикам не «бросить все» построенное и сразу перейти на отечественное ПО, мы предлагаем составить «дорожную карту» перехода на использование отечественного ПО и подсказываем, как сделать это правильно, безопасно и планомерно. Когда делается шаг в сторону импортозамещения, мы должны помнить, что происходит там, где не происходит замена иностранных продуктов отечественными. Мы не говорим заказчикам «Вперед, за нами, в светлое отечественное будущее!». Мы шагаем вместе с ними и в ногу со временем.
При комплексных поставках мы можем предоставить заказчику дополнительные преференции и льготы, которые возможно получить у вендора. В случае проектирования каких-то готовых решений на базе отечественного ПО мы можем проконсультировать заказчика по вопросам существующих программ господдержки или кредитования на льготных условиях.

Может ли свободное программное обеспечение служить хорошей заменой проприетарному, особенно если дело касается вопросов безопасности для ИТ-компании?

У СПО всегда есть соответствующий правообладатель. И он попадает под зону действия регулятора территории, на которой зарегистрирован. Это может быть не организация, а мировое сообщество. Но! Есть центр принятия решений, и он может выполнять определенные действия, в том числе связанные с ограничениями лицензионного соглашения или передачей прав.
Есть примеры, когда у правообладателей СПО покупали права на их продукты, а также, когда СПО при выпуске новых версий или новых редакций переставало быть свободно распространяемым. Использовать СПО нужно с пониманием того, каким образом ты сможешь его эксплуатировать и при этом получать ответственную поддержку.

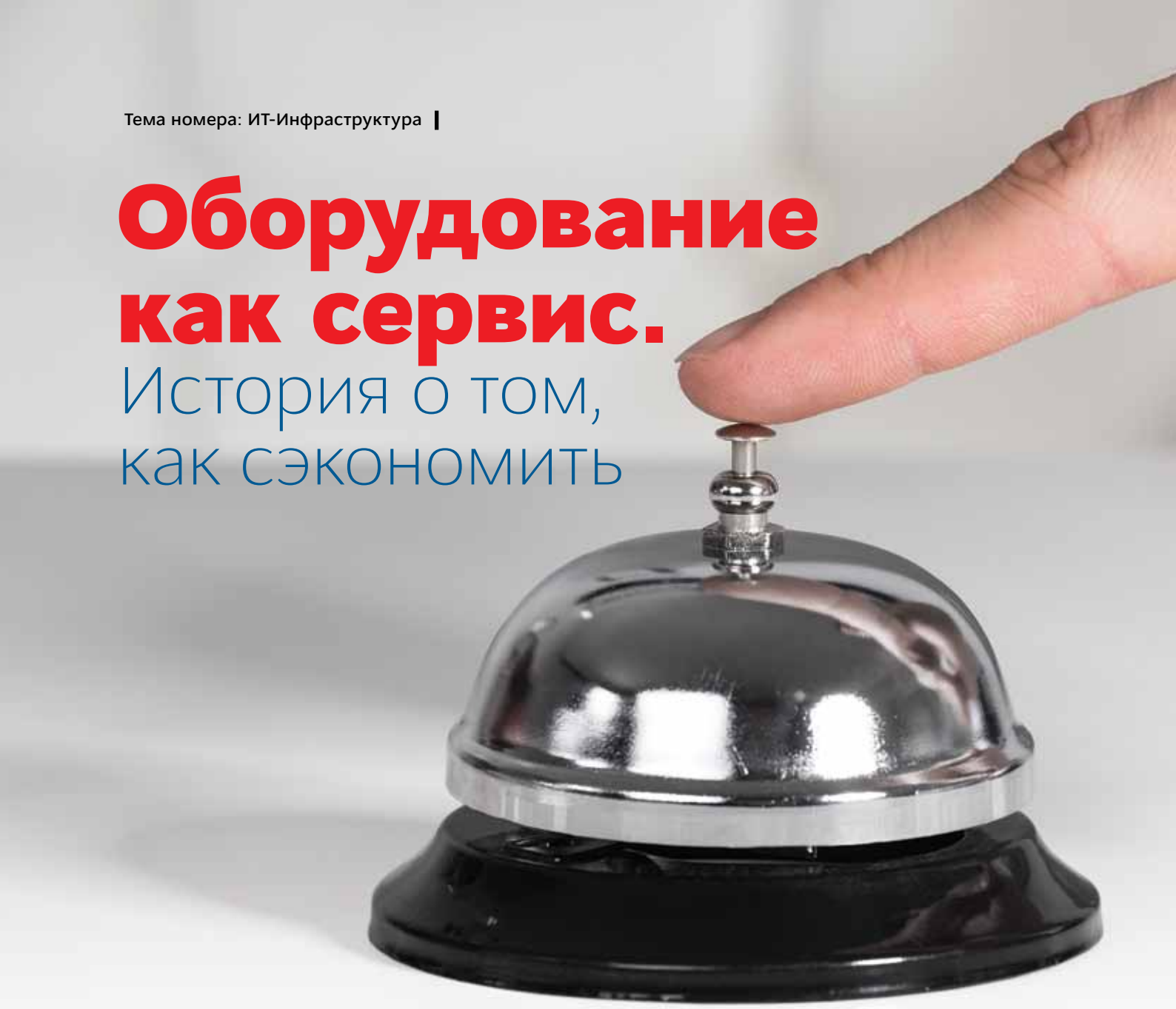
Softline – ваш проводник в лабиринте импортонезависимых решений



По всем вопросам обращайтесь к **Дмитрию Сорокину,** руководителю отдела развития продаж отечественного ПО
Dmitriy.Sorokin@softline.com

Оборудование как сервис.

История о том, как сэкономить



Современная и мощная ИТ-инфраструктура – это основа жизнедеятельности любой компании. Бизнесу неизбежно требуется ИТ-оборудование, также он нуждается в его бесперебойной работе, доступности ключевых приложений и безопасности данных. Услуга «Оборудование как сервис» (HaaS – Hardware-as-a-service) – это современный подход к использованию ИТ-инфраструктуры. Оптимальный способ решения проблем, связанных с ИТ-оборудованием, который позволяет переводить капитальные затраты в операционные. Рассмотрим на примере, как услуга помогает экономить.

Владелец небольшой логистической компании планирует закупку ИТ-оборудования.
Ему кажется выгодным и разумным решением самостоятельное управление серверной инфраструктурой — купить все один раз и не переплачивать за аренду.

Бизнесмен, успешно развивающий стартап по созданию сети медицинских центров, планирует аренду оборудования.

Закупка VS аренда

Самостоятельное управление ИТ-инфраструктурой

Капитальные затраты при построении ИТ-инфраструктуры.

Роль сервера	Закупочная стоимость
Почтовый сервер	280 000 руб.
Сервер приложений	600 000 руб.
Сервер баз данных	580 000 руб.
Веб-сервер	250 000 руб.
Итого:	**1 710 000 руб.**

Серверное оборудование

Роль сервера	Закупочная стоимость
Коммутатор	100 000 руб.
Межсетевой экран/VPN	50 000 руб.
Итого:	**150 000 руб.**

Итого, потребуется около **1 860 000 рублей** единовременных вложений плюс операционные затраты на обеспечение работоспособности собственной ИТ-инфраструктуры.

Операционные затраты на эксплуатацию собственной инфраструктуры.

Статья расходов	Стоимость
Аренда серверного помещения	13 000 руб./мес.
Плата за электроэнергию (потребление 3,5 кВт/ч по тарифу 4,7 руб.)	12 000 руб./мес.
Обслуживание (ФОТ администратора)	35 000 руб./мес.
Итого:	**60 000 руб./мес.**

Аренда оборудования у сервис-провайдера

Аренда серверного оборудования

Роль сервера	Закупочная стоимость
Почтовый сервер	15 900 руб./мес.
Сервер приложений	29 700 руб./мес.
Сервер баз данных	28 000 руб./мес.
Веб-сервер	13 000 руб./мес.
Итого:	**86 600 руб./мес.**

Сопоставление затрат на покупку и аренду. Горизонт – 3 года

Затраты	Закупка	Аренда
1 год	2 430 000 руб.	1 039 200 руб.
2 год	720 000 руб.	1 039 200 руб.
3 год	720 000 руб.	1 039 200 руб.
Итого:	**3 870 000 руб.**	**3 117 600 руб.**

За счёт реинвестирования освободившихся в результате перехода на OPEX средств очевидно, что схема аренды экономит **752 400 рублей** или около **20%** от всех затрат только за первые 3 года.

Сколько стоят деньги?

При сравнении стоимости покупки и аренды оборудования, в особенности долгосрочной, очень часто возникает ощущение того, что единовременная закупка выгоднее.

Сопоставление затрат на покупку и аренду. Горизонт – 6 лет.

Затраты	Закупка	Аренда
1 год	2 430 000 руб.	1 039 200 руб.
2 год	720 000 руб.	1 039 200 руб.
3 год	720 000 руб.	1 039 200 руб.
4 год	720 000 руб.	1 039 200 руб.
5 год	720 000 руб.	1 039 200 руб.
6 год	720 000 руб.	1 039 200 руб.
Итого:	**6 030 000 руб.**	**6 235 200 руб.**

Однако в этих расчетах не учтен тот факт, что покупательская способность денег со временем снижается. В качестве основы для расчёта ставки дисконтирования возьмём индекс ММВБ «Корпоративные облигации совокупный доход» и прибавим 5 процентных пунктов. Так как эффективность компании должна быть выше гарантированного дохода на фондовом рынке, в противном случае выгоднее перевести активы на фондовый рынок и получать гарантированный доход. Для расчёта стоимости аренды используем ставку – 18,69% для ситуации с покупкой – 13,69%. Данный подход обоснован тем, что снижение стоимости денег во времени ведёт за собой повышение тарифов на обслуживание и индексацию ФОТ сотрудников, однако на заключённый договор долгосрочной аренды данные факторы не влияют. Стоимость аренды, по данным договорам, фиксируется на весь её срок.

Сопоставление затрат на покупку и аренду. Горизонт – 6 лет. Приведённый денежный поток.

Дисконтированные затраты	Закупка	Аренда
1 год	2 430 000 руб.*	954 644 руб.
2 год	676 497 руб.	790 738 руб.
3 год	589 481 руб.	654 974 руб.
4 год	513 656 руб.	542 520 руб.
5 год	447 585 руб.	449 373 руб.
6 год	390 013 руб.	372 219 руб.
Итого:	**5 047 232 руб.**	**3 764 468 руб.**

** - единовременный платёж. Дисконтирование не применяется.*

Ситуация в данном случае меняется кардинально. Фактическая экономия при аренде оборудования на длительный период составит более 25%.

В итоге

Владелец логистической компании получил полный контроль над своей ИТ-инфраструктурой, но вместе с ним и огромные затраты на покупку и лицензирование, необходимость поддерживать оборудование в обновленном состоянии и нанимать дополнительных специалистов. Как было видно из расчетов, ожидаемых финансовых преимуществ получено не было.

Тем временем бизнес медицинских центров процветает. Владельцу удалось оптимизировать свои затраты и направить все силы и средства на цифровую трансформацию и развитие своего дела. Заказчик убедился, что аренда экономически эффективна, безопасна и полностью регламентирована существующим законодательством.

Таким образом, уже многими заказчиками доказано, что не существует никаких объективных ограничений или аргументов, препятствующих переходу на сервисную модель построения инфраструктуры.

Инвазивное обследование: кто такие пентестеры

Любая информационная система может содержать уязвимости. Особенно это касается крупных систем, в создании и доработке которых участвовало множество команд. Все ли части системы правильно и до конца настроены? Не осталось ли незакрытых рабочих учетных записей. Не было ли технологического упущения еще на этапе проектирования? На все эти вопросы поможет найти ответы пентест (от англ. Penetration test, pentest – тест на проникновение)!

Цифры говорят сами за себя*

~50%
веб-приложений содержат уязвимости

~129 дней
уходит на исправление критической уязвимости

56%
доля систем с тривиальной сложностью преодоления сетевого периметра

36%
доля успешных атак с получением доступа к конфиденциальным данным

** по данным Application Security Stetistics Report 2017 и Positive Technologies за 2016-2018 гг.*

Как работает пентестер

Пентестер, используя стандартные и нестандартные инструменты, проверяет системы, которые будут в первую очередь подвергаться атакам, находит уязвимости и смотрит, какие возможности они открывают перед злоумышленниками. Эта работа похожа на действия хакеров, однако пентестеры не доводят дело до деструктивного воздействия. Вместо этого они обращают внимание заказчика на потенциальные «дыры» и помогают их закрыть. Компании и организации, которые всерьез опасаются потери данных или иного ущерба, понимают, что такая проверка поможет им лучше защитить свои системы. Пентестеров было бы неправильно называть легальными или «белыми» хакерами, скорее они талантливые программисты и инженеры, профессионалы, которые отлично знают свои инструменты, с помощью которых проверяют системы на прочность.

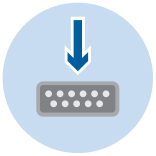
В компаниях Softline и Infosecurity накоплена обширная экспертиза по пен-тестированию. Нам хорошо знакомы как стандартные инструменты и регламенты проверки на уязвимость, так и собственные приемы наработки, своеобразные ноу-хау.

Какие виды угроз часто находят пентестеры

Несвоевременное обновление ПО

Уязвимые веб-приложения, например, для SQL-инъекций

Незакрытые рабочие логины



Порты в открытом доступе

Только в 5% случаев пентестер не находит ни одной уязвимости

Сценарии тестирования

Black Box

Пентестер воспроизводит действия внешнего злоумышленника, имеющего общее представление об атакуемом объекте из открытых источников

Grey Box

Пентестер имитирует действия злоумышленника, обладающего знаниями об атакуемом объекте. Уровень и глубина знаний определяются заказчиком.

White Box

Пентестер обладает правами доступа администратора и имеет полное представление об инфраструктуре

Виды тестирования

Разные предметные области охватывают разные виды тестирования. Прежде всего, следует сказать о методах белого, серого и черного ящиков.

Чаще всего заказчики просят протестировать их именно методом черного ящика, так как он наиболее приближен к реальной ситуации.

Зачем заказчику пентест?

Часто мотивом, чтобы обратиться за тестированием на проникновение, становятся для заказчика требования регуляторов. Для организаций, которым требуется независимое подтверждение защищенности, пентест становится доказательством благонадежности перед проверяющими органами. Второй мотив – инциденты ИБ в прошлом. Третий – необходимость защищенного удаленного доступа сотрудников для удаленной работы.

А в отраслях, где от безопасности зависит жизнеспособность бизнеса, регулярное тестирование перед аудитом становится стандартом качества ИБ, своеобразным требованием «цифровой гигиены».

Области проведения пентеста

Внешний пентест и тестирование веб-приложений (Black, Gray box)

Это самый распространенный вид пентестов. Мы обследуем пул IP- или веб-адресов, используемых серверами компании, сканируем их и испытываем на прочность, исходя из знаний технологий атак.

- Поиск в интернете сайтов заказчика и поддоменов
- Сканирование портов и определение служб, использующих их
- Идентификация используемого ПО и технологий
- Поиск и анализ уязвимостей приложения, входящих в классификацию OWASP
- Проведение атак, направленных на эксплуатацию уязвимостей (по согласованию с заказчиком)
- Анализ результатов и подготовка рекомендаций

Внутренний пентест информационных систем (Black, Gray box)

Второй по распространенности вид пентестирования. Пытаемся воспроизвести атаку во внутреннем контуре заказчика.

- Подключение к пользовательскому сегменту сети
- Анализ трафика протоколов канального и сетевого уровней
- Физическое внедрение и инструментальное сканирование ресурсов внутренней сети
- Поиск уязвимостей на обнаруженных ресурсах
- Проведение сетевых атак и атак, эксплуатирующих уязвимости
- Получение локальных и доменных учетных записей
- Анализ результатов и подготовка рекомендаций

Пентест точек доступа Wi-Fi (Black box)

Осуществляем внешнюю атаку через Wi-Fi

- Изучение характеристики и особенностей сетей Wi-Fi на объекте
- Проведение атак на аутентификацию и авторизацию в беспроводных сетях
- Получение ключей шифрования между клиентом и точкой доступа
- Проведение атак на аппаратное обеспечение сетей Wi-Fi
- Установка поддельной точки доступа Wi-Fi, проведение атак на клиентов сетей
- Обработка результатов и подготовка рекомендаций

Социотехнический пентест (Black, Gray box)

Симулируем внешнюю атаку с использованием техник социальной инженерии

- Сбор данных об объекте и пользователях
- Подготовка провоцирующих данных
- Рассылка сообщений по электронной почте, через мессенджеры
- Личные звонки (телефон, Skype)
- Общение через социальные сети
- Распространение носителей информации с провоцирующими данными
- Анализ результатов и проведение обучения
- Взлом паролей на сервисах личного использования и их подбор на корпоративных ресурсах

Аудит сети (White box)

- Инвентаризация сети
- Проверка актуальности версий ПО, ошибок конфигурации хостов и межсетевых экранов
- Поиск и анализ уязвимостей сетевых служб
- Проверка соответствия межсетевых экранов стандартам ИБ (PCI DSS, NIST, NERC и др.)
- Определение модели атакующего, размещение его в интересующем сегменте сети
- Проведение сетевых атак (Spoofing, MiTM)
- Построение векторов атак и подготовка плана для минимизации рисков ИБ

Наши специалисты

Специалисты Инфосекьюрити и Softline постоянно повышают свою квалификацию. В Инфосекьюрити работает 4 сотрудника с редким профессиональным сертификатом OSCP.
OSCP – курс, разработанный компанией Offensive Security, один из немногих общепризнанных профессиональных сертификатов по проведению тестов на проникновение. Это редкий и сложный сертификат, который проходят немногие специалисты. Экзамен длится сутки, дается 6 стендовых машин, к 5 из которых надо получить полный доступ. Вторые сутки даются претенденту на написание отчета. Специалистов по пентестингу со статусом OSCP в России совсем немного, а в Инфосекьюрити уже 4 человека сдали этот экзамен.

Отчетность

Результатом пентеста становится отчет с рекомендациями по модернизации приложений, сетей, настроек серверов для закрытия существующих «дыр» в безопасности.

Пример реализации

КОМПАНИЯ «А»: 5000 сотрудников, 6 филиалов, 160 B2B-клиентов (крупных и средних интернет-магазинов).
РЕЗУЛЬТАТЫ: Выявлено 12 уязвимостей с низким уровнем риска, 5 – со средним, 2 – с высоким. Самая критичная уязвимость – SQL-инъекция на веб-портале, которая позволяет злоумышленнику получить контроль над сервером баз данных. Даны рекомендации, как повысить защищенность системы с учетом всех выявленных уязвимостей.
МЕРОПРИЯТИЯ: Внешний пентест, включая тестирование веб-приложений методом «черного ящика»
СРОКИ: 25 рабочих дней

НАШИ ПРЕИМУЩЕСТВА

- Сертифицированные сотрудники (Pentestit, OSCP)
- Гибкий подход: от обследования отдельных компонентов (Wi-Fi, сайт и т.д.) до комплексного обследования
- Опыт работы с разными компаниями: финансовыми, государственными, промышленными
- Использование собственных ноу-хау, высокотехнологичного аппаратного обеспечения и методологий

Антифрод: что это такое и с чем его… едят?

О системах автоматизированного выявления мошеннических действий и интересных фактах, связанных с их использованием или отсутствием, рассказали Михаил Апостолов, руководитель продуктового направления SOC Softline, и Михаил Авсенев, руководитель департамента сопровождения инфраструктуры входящей в ГК Softline компании «Инфосекьюрити».

SL: Расскажите какую-нибудь интересную историю об антифроде, о защите от мошенничества. Есть мнение, что антифрод нужен только банкам...

Михаил Авсенев: Мнение есть. Но я расскажу историю про, внимание, сеть автозаправок! На первый взгляд, какая может быть связь? Но в большинстве таких предприятий действует программа лояльности или так называемый кэшбэк. В крупной сети автозаправок, название которой я, по понятным причинам, не упоминаю, на одной из бензоколонок оператор проводила все платежи через свою личную карту с кэшбэком. То есть физически брала у клиентов деньги и прогоняла через свой счет, получая кэшбэк. Схему вычислили таким способом: за день посмотрели все операции и получилось, что на эту одну карточку заправили практически целую цистерну бензина. Вот в таких ситуациях и нужен антифрод, который покажет или даже заморозит подобные транзакции.

Или, вот еще пример, схемы мошенничества на различных игровых серверах. Например, как было с компанией CCP, разработчиком космической многопользовательской стратегии EVE Online. Игрок добыл какой-то не очень дорогой ресурс, артефакт, назовем его «веточка», потом вышел торговать на игровую биржу, где искусственно поднял на него цены, получил космическую прибыль в прямом и переносном смысле и обрушил всю игровую экономику. В итоге сервис был практически на грани закрытия.

Михаил Апостолов: Антифрод нужен не только банкам, но даже автозаправкам и разработчикам онлайн игр. Он актуален в любом месте, где возникают онлайновые товарообменные отношения и происходят транзакции по переводу денег.

Михаил Авсенев: Кстати, о банках! Мошенники в финансовой сфере придумывают очень интересные схемы. Например, выпускают так называемый «белый пластик». Это когда на легальные карты создаются клоны, которые начинают быстро отовариваться в онлайн-магазинах, как правило, созданных теми же самыми мошенниками. Часто ли вы смотрите смс-сообщения от банка с информацией по операциям и счету? А у многих смс-информирование даже не подключено. В таких случаях клиент не сможет заблокировать карту вовремя и очень быстро лишится всех денег.

Мы живем в век информационных технологий, поэтому сведения о том, что у кого-то что-то получилось распространяются очень быстро. Какая-нибудь слабая группировка создает схему мошенничества, потом продает эту схему более сильной группировке, у которой больше ресурсов. Поэтому риски могут быть от 1000 руб. до нескольких миллионов, которые можно потерять буквально в течение нескольких часов.

Михаил Апостолов: В таких случаях убытки неизменно составляют большие суммы, не сопоставимые со стоимостью антифрода, такого как Fraud Detection System компании «Инфосекьюрити».

SL: Расскажите, от каких актуальных угроз может спасти услуга Fraud Detection System?

Михаил Авсенев: В прошлом году наиболее популярными были целенаправленные атаки. Не какие-нибудь типичные вирусы, а заранее подготовленное проникновение в сеть. При таких атаках злоумышленники в течение нескольких месяцев выясняют инфраструктурные моменты, протоколы обмена информацией, а дальше приступают к нападению. Еще при таких видах проникновения мошенники находится в сети долгое время, поэтому могут подготовить средства автоматизации и быстро вывести деньги. Наш антифрод позволяет выявлять эти угрозы очень быстро и в автоматическом режиме. Человек-оператор может пропустить что-то, не обратить внимание на подозрительные транзакции, не успеть вовремя среагировать.

Благодаря встроенным механизмам профилирования Fraud Detection System позволяет автоматически выявлять подобные атаки, выводы денег, нетипичное поведение пользователей. Например, человек производил транзакции в основном из Москвы и тут внезапно оказался во Владивостоке, а потом опять в Москве. Выявление таких аномалий позволит оператору увидеть подозрительные транзакции и предотвратить вывод денег. Атака, может быть и состоится, но деньги не будут потеряны.

Свои атаки мошенники направляют также на платежные шлюзы. Формируются специально подготовленные документы, которые передаются в платежную систему. Наш антифрод позволяет контролировать легитимность платежа.

SL: Какие узлы внутри банка являются излюбленными целями для мошенников? Что чаще всего выбирают хакеры?

Михаил Авсенев: Хакеры в основном заинтересованы в тех узлах сети, где содержится информация о платежах, клиентах или непосредственно в доступе к самим платежным шлюзам.

В первую очередь это АРМ КБР. Дальше идут платежные системы Cyberplay, Cyberpay с RAPIDA и другие платежные системы АБС, информация о клиентах и их счетах, все, что может представлять ценность. Также это персональные и паспортные данные, информация о контрактах, материалы, которые можно использовать для конкурентной разведки.

Михаил Апостолов: Я хотел бы отметить, что среди услуг компании «Инфосекьюрити» есть мониторинг информационного пространства, который помогает выявлять возможные потенциальные или уже осуществленные «сливы» подобной информации.

SL: Теперь хотелось бы поговорить о борьбе с мошенничеством в ритейле и страховании. Как именно будет полезен антифрод в этой сфере?

Михаил Авсенев: В ритейле наша система Fraud Detection System пригодится для выявления злоупотреблений в программах лояльности. В самом начале этого интервью я уже рассказывал о мошенничестве в сети бензоколонок, но какие-нибудь дополнительные баллы за покупку товаров также могут быть предметом интереса неблагонадежных лиц.

Страхование – еще одна интересная тема, так как в нем очень много схем мошенничества. Например, страховой агент берет несколько полисов и не регистрирует их в системе учета. Далее он говорит клиенту о суперскидке и продает полис дешевле. Если у клиента произойдет какой-то страховой случай, он сначала сообщит об этом страховому агенту. Тот зарегистрирует соответствующий полис задним числом, а остальные такие же – нет, в итоге у него получится огромная реальная выгода.

Михаил Апостолов: Если подытожить этот блок, там, где присутствуют какие-либо транзакции, потенциально есть и угроза мошенничества, поэтому организациям, которые дорожат своим именем и отказоустойчивостью системы, нужен антифрод.

SL: Расскажите, пожалуйста, как работает Fraud Detection System?

#как работает FDS

Транзакция поступает в систему


Проверяется по “белым” и “черным” спискам


Проходит через систему правил выявления пошенничества


Если операция признается сомнительной, оператор антифрода обрабатывает ее вручную

Михаил Авсенев: Базовым элементом антифрода является транзакция, которая поступает в систему обработки. Эта система включает несколько фильтров.

Первый фильтр – черный и белый списки. В белых списках содержится информация по транзакциям, которые система безотказно принимает. В черных –информация о мошенниках, их счетах, а также признаки, которые позволяют выявить мошенничество в транзакциях.

После того, как черные и белые списки отработали, транзакция попадает в систему правил, которая выявляет нехарактерные параметры. Приведу пример: человек всегда оплачивал определенную сумму за коммунальные услуги, и внезапно платеж увеличился в десятки раз. Наша система выявит это благодаря встроенному механизму правил. Другой пример нехарактерного поведения – человек начинает очень резко снимать деньги. Если его обычный лимит был, допустим, 70 тыс. рублей в месяц, а в один прекрасный момент он обналичивает полтора миллиона – это повод связаться с ним и выяснить, точно ли он снимает деньги со своего счета.

Еще пример, когда с одного счета уходят платежи сразу в несколько мест с одинаковой суммой. Признаком мошенничества может являться и перечисление мелких сумм денег на множество различных счетов. Такие операции вызывают подозрения у системы антифрода. Они фиксируются, обогащаются и передаются оператору, который получает данные о том, кто проводит транзакции, на какие счета и каково назначение платежа. Это помогает в принятии решения.

Если транзакция прошла через белые и черные списки, а также механизм правил, и при этом система не смогла принять решение, что транзакция легитимна, то такой спорный вопрос переадресуется оператору. Оператор начинает выяснять, действительно ли транзакция легитимна, можно ли ее пропустить.

SL: А кто пишет правила, на которые вы ссылаетесь? Откуда они берутся?

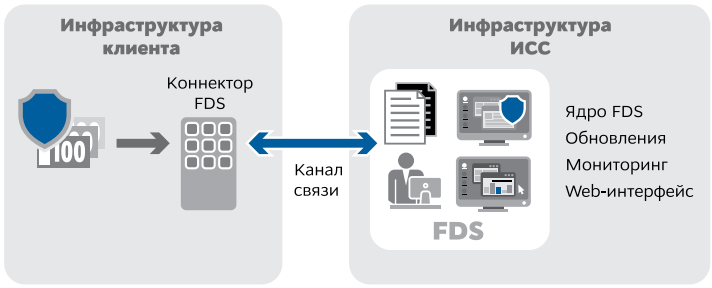
Михаил Авсенев: Обучение решения идет на основе исторических данных. Мы подгружаем в систему информацию о транзакциях, которые были проведены за год или полгода, и начинаем обучать ее выявлению мошеннических действий. Это позволяет разгрузить оператора и обеспечить наименьшее количество рассмотрений транзакций в ручном режиме (около 1%).

Fraud Detection System интегрируется практически с любыми системами баз данных, в том числе и noSQL (без SQL).

SL: Fraud Detection System – это облачное решение или его нужно устанавливать локально?

Михаил Авсенев: Есть и тот, и другой вариант. Если клиент хочет использовать облачную архитектуру, то мы размещаем у заказчика только коннектор к антифроду, который будет подключен к его внутренней структуре и будет передавать данные для расследования. Вся работа, правила и вычислительные мощности, которые нужны для антифрода, будут располагаться у нас на площадке. Для клиента это означает уменьшение затрат на выявление мошенничества. Но если клиент желает, мы можем разместить всю инфраструктуру у него. В тех случаях, например, когда заказчик не хочет отправлять нам свои данные, мы можем реализовать всю необходимую инфраструктуру на его площадке. Конечно же, отправка информации в наше облако осуществляется по защищенному каналу: SSL-шифрование по VPN. Клиент может быть уверен, что данные не утекут никуда.

#в “облаке”



SL: При желании заказчика разместить все у себя, как будет работать антифрод?

Михаил Авсенев: Если заказчик размещает решение у себя, он получает ядро антифрода вместе с правилами, черными и белыми списками, веб-интерфейсом для операторов, которые будут подтверждать или опровергать транзакции и каналом связи, по которому мы будем мониторить нашу систему и отправлять обновления.

#on-premise

SL: Заканчивая беседу, давайте подытожим, какие ключевые особенности можно выделить в работе Fraud Detection System? Чем оно отличается от других антифрод-решений?

Михаил Авсенев: Во-первых, два режима работы. Мы можем работать в разрыв, при котором сама система антифрода автоматически блокирует транзакции, либо в параллельном режиме. В последнем случае антифрод выявляет подозрительные транзакции и информирует об этом оператора, но транзакция все равно производится с возможностью отозвать ее после, что не нарушит функционирование бизнеса.

Вторая наша особенность – это большое количество источников, с которых мы собираем данные. Это и Microsoft SQL Server, Postgres SQL, MySQL, Oracle, DB2, MQ, REST API.

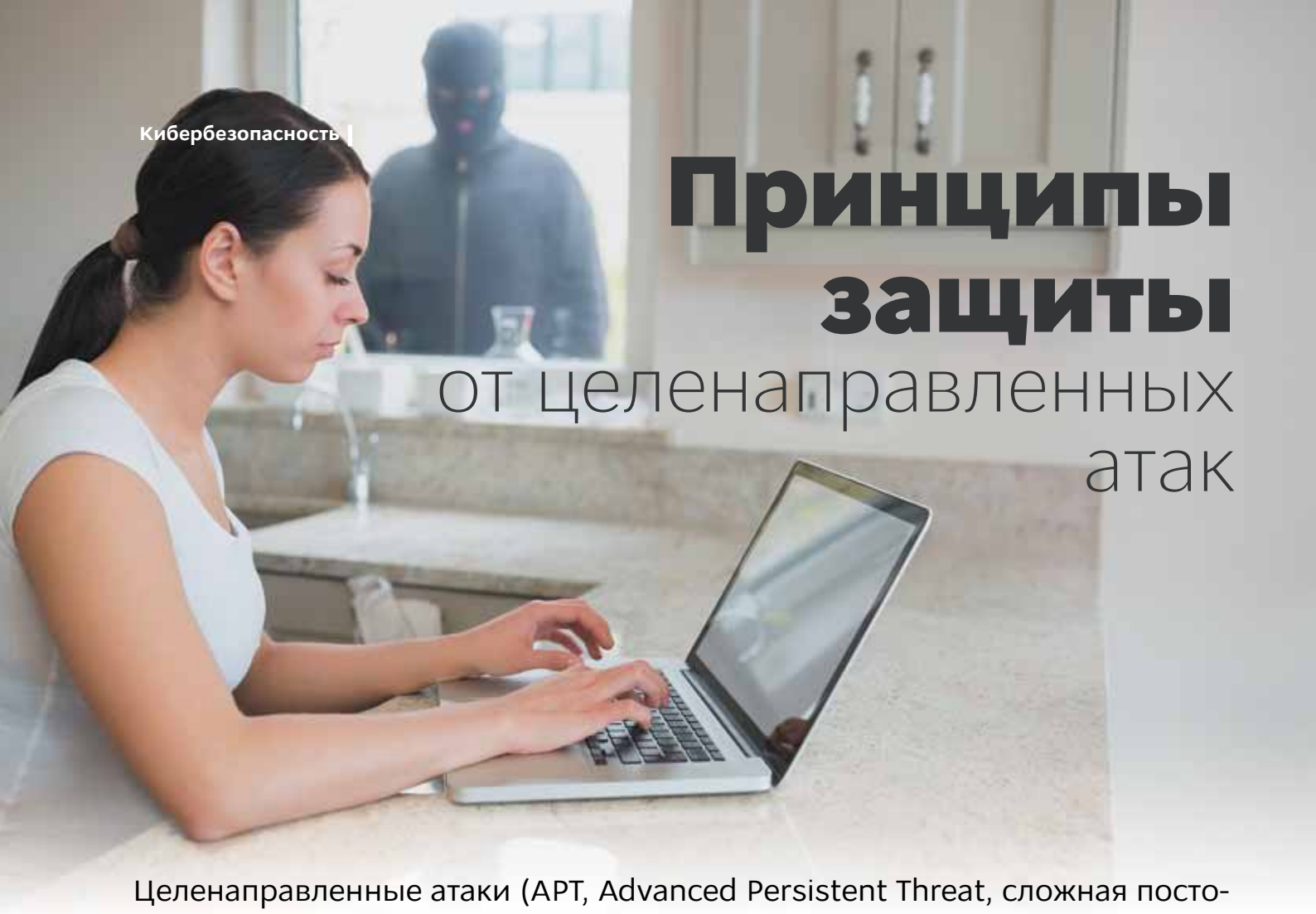
Помимо этого, у нас есть, назовем его так, «джентльменский набор» правил. Клиент получает этот набор по умолчанию при установке решения. Дальше мы адаптируем систему под нюансы конкретного заказчика. Правила подлежат гибкой настройке, что позволяет уменьшить количество ложных срабатываний. В итоге снижается нагрузка на операторов, и они могут обращать больше внимания на действительно важные вещи.

Следует также отметить возможность обучения для уменьшения количества ложных срабатываний. Благодаря этому наши клиенты получают систему, которая разбирает в автоматическом режиме более 98% транзакций. На ручную обработку остается лишь чуть более 1%.

Михаил Апостолов: Компания «Инфосекьюрити» существует на рынке уже достаточное количество времени. Антифрод Fraud Detection System используется в ИТ-системах очень крупных клиентов. Мы можем с уверенностью утверждать, что главной и ключевой особенностью решения является быстрая обработка большого количества транзакций.

SL: А как сейчас развивается решение?

Михаил Авсенев: Развитие продукта идет в сторону нереляционных баз данных (noSQL), так как мы используем такие базы данных не только в антифрод-решении, но и в нашем SOC. Это позволяет выполнять множество транзакций в параллель, дополнительно увеличивает скорость работы антифрода и его отказоустойчивость. Распределенная база данных – это гораздо более надежное решение, чем решение на одном сервере. ▮



Принципы защиты от целенаправленных атак

Целенаправленные атаки (APT, Advanced Persistent Threat, сложная постоянная угроза) – это «долгоиграющие» мероприятия злоумышленников, имеющие четкий план. Они рассчитаны не на внезапный удар по ИТ-системам, а на продолжительный захват. Вы можете в течение долгого времени не знать о том, что у вас в инфраструктуре действуют хакеры. И готовятся подобные атаки не один месяц. Им предшествует подготовительная работа и предварительная разведка. Злоумышленники продумывают атаку до мелочей – от способа первичного проникновения в инфраструктуру до того, каким образом впоследствии они заметут следы.

Зачем и для кого

Какие мотивы приводят компанию к решению установить защиту от целевых атак? Движущим фактором часто становится какой-то инцидент в недалеком прошлом – реальная атака и похищение данные. Впрочем, чужой опыт тоже поучителен. Прошлый год был богат на хакерские атаки, например, небезызвестные Petya, WannaCry, Bad Rabbit. Люди стали испытывать недоверие к антивирусам и файрволам и искать новые решения.

Наибольший интерес к защите от целевых атак проявляют, конечно, компании, связанные с денежными потоками, например, банки. Они являются лакомым кусочком для киберпреступников. Промышленные предприятия, для которых успешная атака может означать остановку производства, выход из строя оборудования, тоже заинтересованы в решениях такого класса. Государственные организации, обрабатывающие важные данные, также смотрят в сторону анти-ATP решений. Нередко поступают запросы и от небольших компаний.

Что бывает до ATP?

До того, как компания приходит к решениям ATP (Advanced Threat Prevention), в ее инфраструктуре, как правило, уже заложен некий фундамент кибербезопасности, чаще всего антивирус, межсетевой экран, возможно, прокси. Может быть комбинированный набор TMG, в котором есть и файрвол, и прокси. Такой набор соответствует ландшафту угроз 5-летней давности, но время идет, и злоумышленники не стоят на месте.

В маркетинге принято делить файрволы на next-gen и простые. Next-gen файрволы уже в своем составе имеют средства для борьбы с ATP, старые – не имеют такой возможности во многом потому, что на момент создания не стояло такой задачи.
Справедливо, что появился такой класс решений, как решения анти-ATP. Только существуют такие средства защиты в разном виде и внедряются по разной стоимости исходя их потребностей заказчика.

Каналы проникновения

Безусловно, почта – самый популярный канал проникновения вредоносного ПО внутрь предприятий. По некоторым данным, доля такого способа внедрения от числа всех каналов атак доходит до 95%. Есть два варианта проникновения. Первый, когда файл напрямую посылается на почту адресату, второй – в почтовом сообщении содержится ссылка, клик по которой приведет к скачиванию вредоносного файла. Также для проникновения используются подставные сайты. В любом случае основной канал, который следует защищать – это почта. На втором месте – интернет-трафик, на третьем – съемные носители.

Реальные кейсы. Как обычно выглядит ущерб?

Хищение данных, вывод из строя серверов, оборудования, кража денежных средств. В конце 2017 года была совершена первая в России атака на платежную система SWIFT. Им удалось вывести несколько десятков миллионов рублей у одного из наших российских банков. Также вывод из строя промышленных объектов. На Украине относительно недавно совершена атака, в результате которой была выведена из строя энергетическая система.
Надо понимать, что не всегда целью злоумышленников является ваша организация. Это может быть контрагент, с которым вы работаете. И через доверенную организацию туда попасть проще. Так или иначе ломают вас, но цель – не вы. И такой пример тоже есть, например, компания RSA, которая занималась разработкой средств защиты информации. И целью атаки являлась не она сама, а их контрагент, занимающийся авиастроением. То, что авиастроительная компания понесла крупные убытки – факт, а RSA понесла репутационный ущерб, который сложно перевести в деньги.

Роль ATP в системах защиты

Проверка на вредоносность не должна идти первым в линии защиты. Сначала это могут быть межсетевое экранирование, анти-спам, анти-фишинг, которые внедрены в почтовую систему, прокси-сервера, обнаружение вторжения на сетевом уровне, и только после прохождения файлом этих барьеров идет песочница – крайняя мера защиты. На этом этапе необходимо понимать, что оперативность проверки файла требует больших ресурсов, большой потом таких файлов повлечет за собой дополнительные затраты. Чтобы их сократить, необходимо сперва максимально эффективно использовать существующие средства защиты.

Песочница

Что касается технической части: файлы, получаемые через почту или веб-браузер, проходят через периметр и появляются на конечной рабочей станции. Если файл не опознан, он помещается в песочницу. Это сервер или комплект серверов в виртуальной среде, где работают настоящие ОС (зачастую Windows), которые используются на конечных рабочих станциях. На таких ОС стоит офисный набор ПО, ПО для просмотра PDF-файлов, деловой переписки, и там же происходит реальный запуск на реальных машинах файла, который может представлять угрозу.

Облачная проверка и искусственный интеллект

Насколько эти средства защиты от целевых атак могут существовать в облаке, интегрироваться с EAM, SOC? Такая интеграция существует. И она помогает при расследовании инцидентов. Это один из акцентов, на чем сосредоточен производитель такого оборудования и решений. Облачная проверка файлов – не новое решение с самой низкой стоимость. Вариант проверки на месте у заказчика обходится гораздо дороже.
В связи с такими системами часто упоминают ИИ, машинное обучение. Роль этих технологий - сбор и обработка статистических данных, поведенческой модели вредоносных файлов. Этот вопрос остается на стороне вендора. Многие из них заявляют, что такие системы у них внедрены для того, чтобы оперативно принимать решения о том, вредоносен этот файл или нет. Это вопрос облачного анализа этих файлов. ▮

Системы защиты от утечек данных: как они внедряются

Использование систем предотвращения утечек данных становится всё более общепринятой практикой не только среди крупных компаний и организаций, но и в среднем бизнесе. О системах DLP и существующих практиках их внедрения рассказывает Анна Попова, руководитель блока DLP компании Инфосекьюрити.

Более 90% наших заказчиков – это крупные компании, ведущие игроки в своих отраслях. Для таких клиентов актуальны все виды рисков – репутационные, финансовые, юридические. Например, утечка базы клиентов коммерческого банка влечет:

- нарушение закона о банковской деятельности;
- нарушение закона о персональных данных;
- риск оттока клиентов к конкурентам, которые будут их переманивать;
- ущерб имиджу банка.

И этот пример вполне жизненный. Среди наших клиентов был банк, переживший отток сотен и тысяч клиентов. После «слива» клиентской базы конкуренты обзвонили вкладчиков, у которых заканчивался срок депозита и пригласили их переходить к себе на выгодные условия. Ситуация абсолютно реальная и вполне объяснимая – любая компания заинтересована в новых клиентах, и воспользоваться для этого чужой клиентской базой – простой и удобный способ укрепить свое положение на рынке.

Еще одной причиной внедрять и использовать DLP становится соответствие требованиям регуляторов, которые касаются банковских, кредитных, финансовых организаций и многих других отраслей. Защищать данные от утечек предписывают многие законодательные акты, в том числе закон о банковской деятельности, закон о коммерческой тайне, закон о защите критической информационной инфраструктуры. В этих законах четко прописано, какие данные подлежат защите и как они должны храниться и передаваться. Хотя аббревиатура DLP не упоминается в тексте законов прямо, требования по защите вполне однозначно трактуются как предотвращение утечек данных.

Первое необходимое условие для внедрения системы защиты от утечек – наличие в компании пакета документации – актуального перечня данных, которые подлежат защите: здесь должны быть перечислены конкретные активы и объекты. Документация может называться «Перечень сведений, составляющих коммерческую тайну» или как-то иначе, и в ней должно быть подробно описано, кто имеет право доступа к тем или иным данным, на основании каких документов, как этот доступ выдается и отзывается, что именно можно делать с данными и что нельзя, по каким каналам связи их можно передавать и т.д. Именно эта документация лежит в основе системы защиты от утечек.

Кому поможет DLP-система

1 Собственники бизнеса, ТОП-менеджмент

Предотвращение ущерба/возврат потерь, исполнение требований законов, формирование доказательной базы, обнаружение уязвимостей в бизнес-процессах.

2 Служба безопасности

Контроль взаимодействия с партнерами, поиск инсайдеров, контроль неформальных связей в организации и нетипичных контактов, защита наиболее критичных процессов и ценных кадров

3 Служба информационной безопасности

Предотвращение утечек КИ, контроль движения КИ, дополнительные сведения по инцидентам

4 Функциональные руководители, HR

Эффективность сотрудников, обстановка в коллективе, уязвимость и лояльность сотрудников

Кроме персональных данных и клиентских баз к критической информации, которая не должна покидать корпоративную сеть, может относиться широкий круг данных, например договора, финансовая отчетность, конструкторская документация и т.п. В каждой компании может оказаться уникальный набор данных, которые требует защиты от утечек.

Казалось бы, самый простой и эффективный способ – перекрыть вообще все каналы, по которым теоретически возможен слив данных. Однако такой подход невозможен с точки зрения бизнеса, так как любые бизнес-процессы требуют передачи данных по каналам связи. В реальной жизни требуется найти баланс открытости и защищенности и, конечно, контролировать в строгом соответствии с политиками каналы передачи данных: почту, мессенджеры, службу печати, и все остальное. Именно это и делают системы класса DLP.

Анна Попова, руководитель блока DLP компании Инфосекьюрити.

Prevention в аббревиатуре DLP означает предотвращение. Однако на практике DLP-системы российского производства могут действовать в двух режимах: наблюдения и блокировки. Первый режим позволяет выявлять инциденты утечки, а второй – блокировать их.

Итак, мы внедряем систему DLP в компании, например, с 50 тыс пользователей. Первое, о чем надо задуматься – какое количество потенциально опасных событий будет регистрировать такая система. Если у нас нет возможности анализировать тысячи событий в день – систему надо настроить так, чтобы событий были не тысячи, а сотни – для этого уменьшаем количество триггеров, смягчаем условия генерации оповещений об опасных событиях.

Еще один полезный механизм для предотвращения перегрузки событиями – профилирование сотрудников и их распределение по группам риска. Пользователь, совершающий подозрительные действия, попадает в особую группу, и за ним устанавливается более пристальное наблюдение, вплоть до обследования вручную снимков экрана, логов клавиатуры, чтение

переписки и т.д. Наш опыт показывает, что на 10-15 тыс пользователей примерно 200 человек попадает в такую подозрительную группу. Конечно состав этой группы должен динамически обновляться.

Вообще, чем больше «сырых» событий собирает система, тем больше аналитического ресурса требуется на обработку этой информации. Приведу долгосрочный пример: около 8 лет мы обслуживали DLP в компании с 20 тыс сотрудников. Обработкой событий занимались 15 аналитиков, причем уровень аналитики был очень глубокий. Кстати, дело упростила длительность проекта – за первый год аналитики разобрались, какие сотрудники и с какой информацией работают, и впоследствии наблюдение шло в более спокойном режиме.

Приходится сталкиваться и с неудачными примерами. Если в компании численностью 100 тыс сотрудников аналитикой DLP занимается 1-2 человека, они должны будут работать круглосуточно, и все равно не справятся. К сожалению, такие неэффективные внедрения бывают, и дорогая система DLP не дает того результата, которого от нее ждут.

Гарантированно получить ожидаемый результат поможет подход «DLP как сервис». Речь идет о команде аналитиков и инженеров, которые полностью берут на себя сопровождение DLP системы и аналитическую обработку информации, которую она генерирует. Эта команда работает в тесном взаимодействии со службой безопасности и руководством заказчика, отчитывается перед ними и может выполнять е конкретные поручения, связанные с расследованием инцидентов. Таким образом мы помогаем заказчикам получить ожидаемую отдачу от внедрения DLP и освобождаем их от необходимости содержать собственных аналитиков.

Функционально DLP как сервис по всем признакам очень напоминает SOC, отличие состоит в том, что центром такого центра реагирования является не SIEM а DLP-система. Его даже иногда называют SOC DLP.

Существующие системы DLP принципиально различаются подходом – наблюдение или блокировка. Кроме того системы могут быть по-разному реализованы. Одни вендоры разрабатывают DLP в формате web-приложения, другие – выглядят как толстый клиент, третьи – как тонкий. Еще один важный фактор – полнота покрытия каналов передачи данных. Например, один вендор объявляет о поддержке своим продуктом мессенджера telegram, и остальные оказываются по telegram в положении догоняющих. Вообще производители различных систем DLP смотрят, развивая свои продукты, не только друг на друга, но и на реальные потребности своих клиентов и многое дорабатывают по их запросу.

На российском рынке присутствует уже множество систем отечественного производства –4-5 игроков могут похвастаться большими инсталляциями на десятки тысяч человек.

У Softline и Инфосекьюрити нет любимой системы DLP. Мы хорошо знаем разные системы и можем предложить выбор, причем по любому продукту наша экспертиза соответствует экспертизе вендоров. Также мы готовы в интересах клиента работать с любой системой, которая у него уже есть.

Возможность регистрировать любые действия пользователей позволяют применять DLP-системы не только для предотвращения утечек, но и для решения ряда других задач. Такие побочные эффекты очень интересны нашим заказчикам. Мониторинг производительности труда, отношений в коллективе, поведенческий анализ позволяют руководству и службам безопасности объективно оценивать эффективность работы сотрудников, выявлять людей, склонных к противоправной деятельности, вести оперативно-разыскную работу.

Среди наших заказчиков множество крупных компаний, лидеров в своих отраслях. Это Банк Точка, инвестиционная компания Sova Capital, производственный Кама-Холдинг и десятки других организаций, которых мы не можем упоминать..

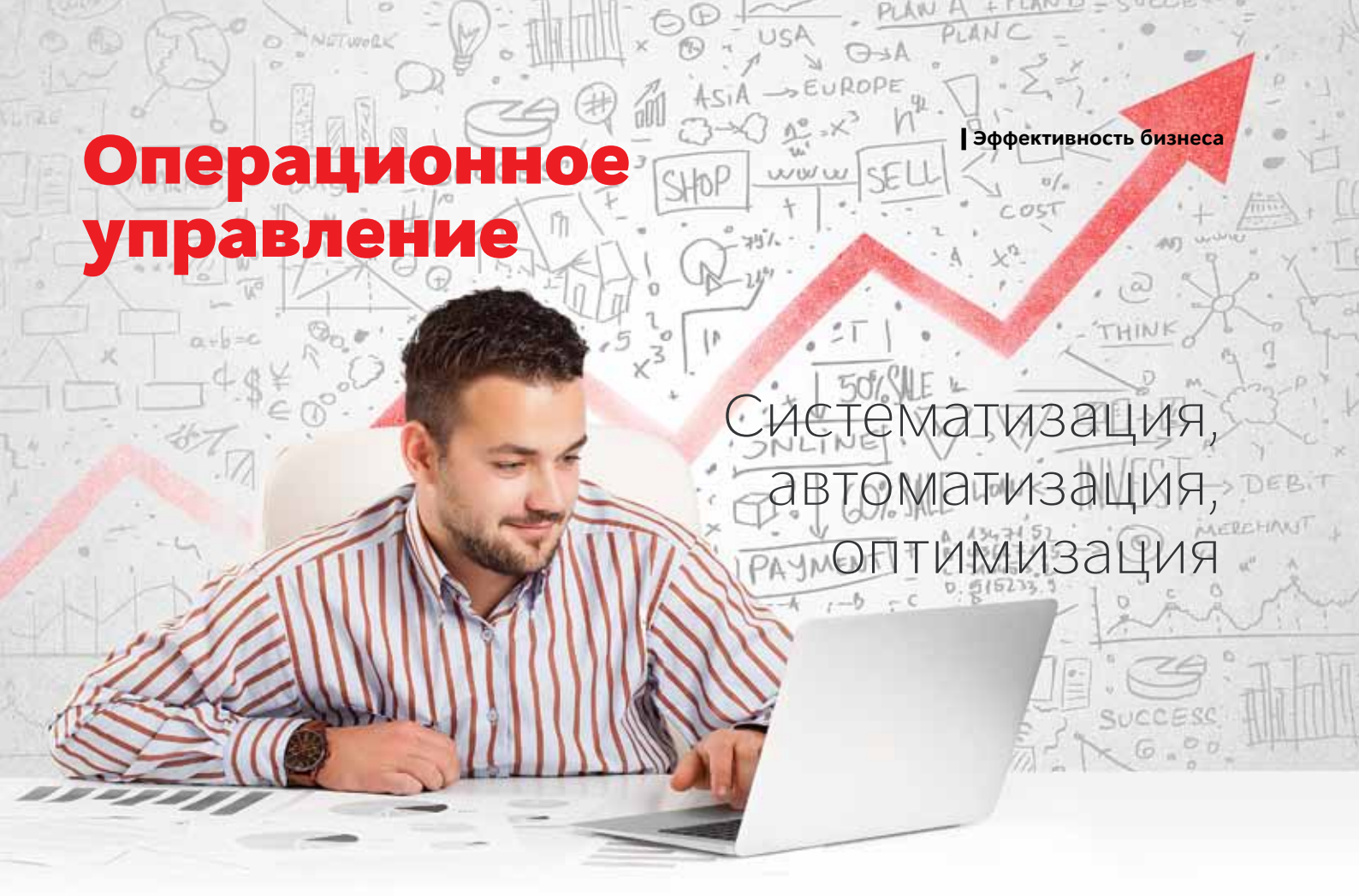
Наши решения

INFOWATCH SEARCHINFORM ГАРДА ТЕХНОЛОГИИ Solar Dozor falcongaze

STAFFCOP ZECURION DeviceLock DLP

Стахановец Symantec FORCEPOINT McAfee

Операционное управление



Систематизация, автоматизация, оптимизация

Яков Рутман, руководитель направления продажи и развития решений ITSM компании Softline, рассказал о создании систем операционного управления как о первом шаге на пути к цифровой трансформации, о главных принципах автоматизации и особенностях реализации данных проектов.

– Яков, расскажите, пожалуйста, что включает в себя операционное управление?

– В любой компании существует определённая структура рабочих процессов. Бухгалтерия отвечает за расчет зарплат, справки 2-НДФЛ, обработку актов сверки и т.д. Административно-хозяйственный отдел снабжает офис мебелью, канцелярией; HR-департамент занимается поиском и наймом сотрудников и очень богат различными операциями. Для того чтобы нанять сотрудника, руководитель должен создать заявку, рекрутер должен найти кандидата, а потом выполнить целый комплекс мероприятий по его оформлению, адаптации, подготовке рабочего места. Все эти процессы должны быть упорядочены и централизованы, чтобы к моменту, когда человек выйдет на работу, у него были все условия для того, чтобы сразу влиться в рабочий процесс. В других сферах мы можем говорить про техническое обслуживание оборудования, аудит, ремонт, взаимоотношения с подрядчиками и контрагентами – организация всего этого и есть операционное управление.

Любая рабочая деятельность подчинена единому алгоритму, правилам, условиям, которые уже давно выработаны в сфере ИТ. Они говорят нам о том, как должен быть выстроен процесс, чтобы он был непрерывным и приводил к ожидаемому результату. Задачи должны выполняться быстро, а ответственность распределяться четко, чтобы избежать эффекта пинг-понга. Главный принцип управления услугами – это регламентированность рутинных операций. Каждый процесс представляет собой набор функций, за каждую из которых отвечают компетентные сотрудники. Они принимают заявку, обрабатывают ее по инструкции, в оговоренные сроки достигают результата и выдают его бизнесу. Таким образом создается система операционного управления, где заказчики имеют возможность прийти за сервисом в бухгалтерию, в административно-хозяйственный отдел, в HR и т. д.

– Как операционное управление связано с цифровой трансформацией?

– Автоматизировав все функции, выполняемые определенными подразделениями, компания достигает централизации и унификации всех процессов и тем самым делает серьезный шаг в достижении цифровой трансформации. С помощью технологий машинного обучения собира-

ется и анализируется информация и выдаются логические, основанные на исторических данных выводы из рабочих процессов. Со временем эти данные накапливаются и на их основе можно организовать полную автоматизацию деятельности компании, когда в процессе работы сотрудника система сама будет предлагать или инициировать следующие его шаги. Например, исходя из накопленной статистики, после формирования актов сверки будет предложен следующий шаг – отправить заказчику и ожидать ответный, а затем следующий – прикрепить акт сверки заказчика к текущей заявке. В HR-отделе после создания задачи на поиск кандидата, в автоматизированном режиме система делает запросы во все HR базы данных и после анализа сведений о необходимой квалификации сотрудника, его опыте отбираются максимально подходящие кандидатуры. Специалист получает возможность выбирать из них, не тратя время на долгий поиск из необработанного потока кандидатов. После назначения даты собеседования система определяет, к примеру, какая переговорная свободна и когда у руководителя есть время. Если кандидат подошел, запускается серия заявок по проверке безопасности, созданию рабочего места, отправке адаптационного плана – всё это автоматически создается и обрабатывается. Цифровизация деятельности предприятия реальна, если ее должным образом информатизировать и регламентировать.

Автоматизация процессов позволит получать информацию, на основе которой можно развивать бизнес, повышать скорость процессов, качество, осуществлять бесперебойную работу.

– А какие проблемы стоят на пути этого?

– Основная проблема сейчас в том, что заявки часто не оформляются в согласованном, закрепленном виде и не систематизируются, а просто висят в воздухе. Это значит, что задания поступают через почту или неформальное личное общение. Например, кто-то попросил сотрудника поменять картридж в принтере, он, конечно, сделает это, но в данном случае не будет контроля за количеством картриджей, расходами на них. Работа данного сотрудника тоже не учтется, так как при таком порядке вещей невозможно посчитать, сколько заявок он выполнил.

Чтобы понять, как с этими проблемами справится, нужно тщательно изучить, как строится работа каждого сотрудника, его должностные обязанности, порядок решения задач, цели. Например, автоматизируя работу ИТ-сотрудников, решается не проблема замены мышек или картриджей, а налаживается система аналитики – сколько раз он меняет их, что ему для этого нужно, если он делает это часто на определённом участке, то почему? Может быть, это нагрузка на оборудование либо повышенное потребление электричества. Автоматизация процессов позволит получать информацию, на основе которой можно развивать бизнес, повышать скорость процессов, качество, осуществлять бесперебойную работу.

– Какие услуги предоставляет Softline в области управления операционными процессами?

– Вся продуктовая линейка и решения Softline представлены в портфолио компании. Мы занимаемся не просто продажей программных продуктов, а предоставляем также консалтинговые услуги по описанию операционных процессов и их автоматизации, помогаем сделать первые шаги к цифровой трансформации внутреннего и внешнего взаимодействия компании. У любой организации, у которой есть потребность быть конкурентоспособной на рынке, есть мелкие проблемы, которые в общей конве самого бизнеса могут быть не видны. Например, на первый взгляд, сделать справку – это не проблема, но, основываясь на многолетнем опыте и статистике учета рабочего времени, можно сказать, что это минимум 15 минут рабочего времени. И вместо того, чтобы выполнять свои прямые обязанности, сотрудник занимается этой рутинной работой. И из-за этих 15 минут за месяц может складываться нелицеприятная картина, а если это делает высокооплачиваемый сотрудник, убытки очевидны. И мы как специалисты, располагая соответствующей экспертизой, аналитиками, консультантами, можем помочь заказчикам найти слабые стороны, систематизировать их, автоматизировать и оптимизировать.

– Как проходит реализация таких проектов?

– Она состоит из нескольких этапов. **Первый** – обследование, в рамках которого проводится анкетирование и интервьюирование участников, изучаются имеющиеся документы и артефакты. На основании полученной информации производится описание текущих процессов, выявление того, насколько они эффективны, соответствуют ли мировым практикам, далее проводится аудит в соответствии с выбранными стандартами.

Второй этап – проведение семинаров, в ходе которых совместно с заказчиком разрабатываются обновленные процессы. Результатом являются согласованные регламенты, описанные в формализованном виде процедуры с закрепленными ролями и ответственностью, а также, что немаловажно, метриками и процедурами развития процесса для перехода к более высокому уровню зрелости. Такой подход позволяет уже на этом этапе сформировать для заказчика правильное видение процессов. Мы адаптируем лучшие практики под специфику конкретного предприятия.

Третий этап – выбор программной платформы или описание требований к настройке ранее внедренной системы. Результат – настроенная система, эксплуатацию которой необходимо будет сопровождать. При реализации этого этапа важно учитывать тот факт, что внедряемый инструмент автоматизации удовлетворяет всем написанным в регламентах процедурам, помогает участникам получать актуальную информацию, контролирует процессы и вычисляет их показатели.

Основой такого подхода является HP ITSM Reference Model. Согласно принципам, описанным в этой методологии, при разработке ИТ-процессов и стратегии обязательно учитываются бизнес-цели. Такой подход позволяет максимально учитывать интересы бизнеса при управлении услугами и инфраструктурой.

Существуют готовые варианты, например, online-сервис WorkFlowSoft – простой инструмент для автоматизации задач, который позволяет автоматизировать бизнес-процессы организации без помощи ИТ-специалистов.

– Какие средства автоматизации операционных процессов существуют на рынке программного обеспечения?

– Средства, автоматизирующие ИТ и бизнес-процессы, разнообразны. Наша задача предложить заказчикам максимально подходящее под их потребности решение. Существуют готовые варианты, например, online-сервис WorkFlowSoft – простой инструмент для автоматизации задач, который позволяет автоматизировать бизнес-процессы организации без помощи ИТ-специалистов. Также существуют решения и системы уровня Enterprise, позволяющие автоматизировать большинство процессов, описанных в ITIL (англ. IT Infrastructure Library — библиотека инфраструктуры информационных технологий) и использующих подходы ITSM (англ. IT Service Management – управление услугами в ИТ), а также отвечающих мировым стандартам по управлению услугами ИТ.

Для составления объективной картины происходящего и разработки сценариев, отвечающих интересам ИТ и бизнеса, я рекомендую прибегать к помощи профессионалов, имеющих опыт разработки, внедрения и автоматизации процессов.

– Как Softline может помочь своим клиентам в автоматизации процессов? Какие рекомендации вы можете дать?

– Первая рекомендация – обратитесь к специалистам. Для составления объективной картины происходящего и разработки сценариев, отвечающих интересам ИТ и бизнеса, я рекомендую прибегать к помощи профессионалов, имеющих опыт разработки, внедрения и автоматизации процессов.

Внедрение стоит начать с обследования текущей практики управления рабочими операциями, услугами, инфраструктурой и выбора инструмента автоматизации. Это сформирует правильные требования к конечному процессу, опираясь на потребности, цели, стратегию и возможности автоматической системы управления. Ее внедрение занимает достаточно короткий промежуток времени – до 4 недель. Это хороший старт для того, чтобы в дальнейшем масштабировать эту платформу на всю компанию в целом.

Для крупных компаний, численностью от 5 тысяч, средство автоматизации ИТ процессов, можно превратить в объединённый центр обслуживания (ОЦО) – это некий результат масштабирования процессов операционного управления ИТ на бизнес-процессы предприятия. ОЦО позволяет централизовать, унифицировать и стандартизировать функции. Это позволяет сделать первый шаг на пути цифровой трансформации операционной деятельности.

ГИС MapInfo Pro 17.0

MapInfo Pro — географическая информационная система (ГИС), предназначенная для сбора, хранения, отображения, редактирования и анализа пространственных данных. MapInfo легко интегрируется в существующую информационную инфраструктуру предприятия и имеет собственный язык разработки специализированных приложений MapBasic.

Сферы применения ГИС MapInfo

Бизнес и наука, образование и управление, градостроительство и архитектура 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 имеет полный набор средств для создания, оформления и высококачественного вывода карт на печать, имеет развитые средства построения тематических карт и включает обширные наборы общепринятых условных обозначений.

MapInfo Pro поддерживает все распространённые форматы векторных и растровых пространственных данных и позволяет получить доступ к картографическим веб-службам WMS, WFS и WMTS.

MapInfo Pro может выполнять функции картографического клиента для всех современных СУБД. Имеется 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.

MapInfo Pro имеет современный ленточный интерфейс, поддерживает Юникод и размер TAB-файлов более 2 Гб, работает на 64-разрядной платформе.

MapInfo Pro Advanced

Это расширенная лицензия 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.

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

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.

Терпланирование для ГИС MapInfo Pro

Приложение для подготовки карт территориального планирования в среде MapInfo Pro.

Система поставляется с настроенными таблицами и справочниками в соответствии с «Требованиями к описанию и отображению в документах территориального планирования объектов федерального значения, объектов регионального значения, объектов местного значения» (Приказ Минэкономразвития России № 10 от 9 января 2018 г).

Система позволяет создавать и редактировать геометрию и атрибутивную информацию по объектам территориального планирования. Основные возможности:

- создание новых карт или использование имеющихся шаблонов;
- хранение сопроводительных документов;
- создание и использование справочников для ввода атрибутивной информации и стилей оформления объектов;
- использование единого хранилища карт, справочников и документов;
- визуальное создание форм ввода данных.

Данное ПО бесплатно предоставляет режим просмотра карт и информации по объектам территориального планирования.
Система Терпланирование работает с MapInfo Pro 12 и более новыми версиями. Она может быть установлена как с 32-битной, так и 64-битной версией MapInfo Pro.

Ознакомительные версии программного обеспечения доступны на сайте: www.mapinfo.ru

Русская версия MapBasic 17.0

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

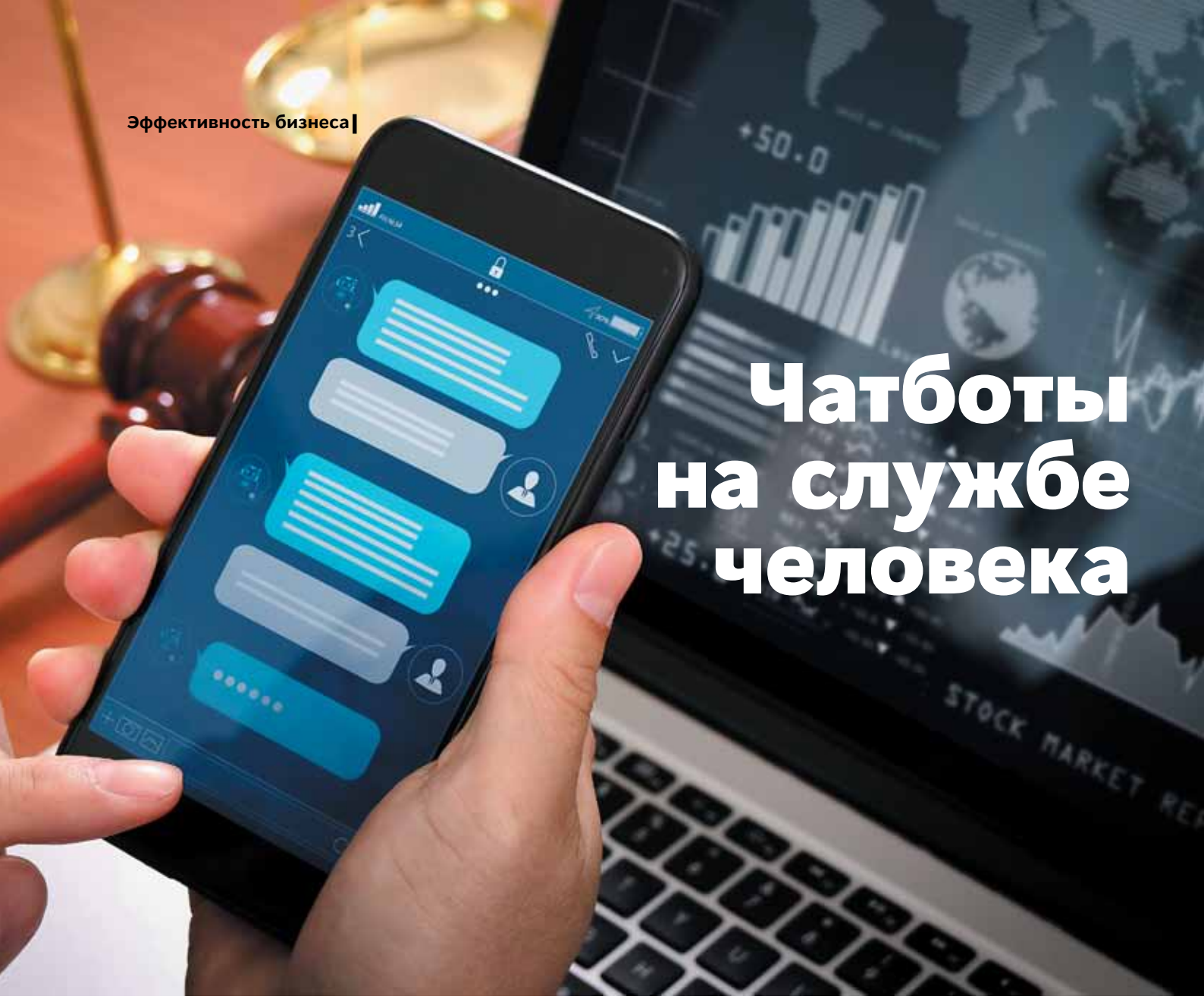
Официальный представитель Pitney Bowes Software Inc. в России и СНГ

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

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

Защита критической инфраструктуры Правительства Калининградской области

Компания Softline приняла участие в проекте по защите критически важной инфраструктуры Правительства Калининградской области. Заказчиком выступил Калининградский государственный научно-исследовательский центр информационной и технической безопасности. Благодаря решению PT Platform 187 от Positive Technologies, на базе КГ НИЦ создается региональный центр кибербезопасности. Он будет обеспечивать защиту Правительства области от компьютерных атак в рамках ФЗ № 187.
PT Platform 187 позволяет Правительству Калининградской области строить центр кибербезопасности поэтапно: распланировав бюджет, постепенно развивать его архитектуру, отрабатывать процесс реагирования на атаки на небольших инфраструктурах и систематично расширять область мониторинга.
В дальнейшем центр планирует обеспечивать взаимодействие с ГосСОПКА и расширять область мониторинга, переходя на enterprise-версии продуктов, входящих в PT Platform 187. К 2020 году в область мониторинга войдут все 3000 сетевых устройств органов власти Калининградской области.



Чатботы на службе человека

Вспомните последний раз, когда вы общались со специалистом по обслуживанию клиентов. Ваши эмоции были на пределе, вы закипали, но спокойный и рассудительный менеджер по ту сторону экрана или телефонной трубки быстро решил вашу проблему. Вы остались довольны? А вы уверены, что взаимодействовали с человеком? Согласно статистике, 80% предприятий уже используют или планируют использовать чатботы к 2020 году. Сюрприз! Вас обслуживал искусственный интеллект, или его крошечный агент — чатбот.

Как появились чатботы

Слово chatbot происходит от «chatterbot». Этот термин впервые ввёл Майкл Маульдин в 1994 году. Чатботом может называться любая компьютерная программа, которая взаимодействует с людьми через мобильные приложения, веб-сайты или мессенджеры и отвечает на запросы клиентов. Технология Chatbot старше 50 лет, но максимальное развитие она получила в последние пять лет.

1966 год - Джозеф Вайзенбаум разработал чатбота Элизу в Лаборатории искусственного интеллекта Массачусетского технологического института, чтобы показать, как может происходить общение между людьми и машинами.

1972 год - психиатр Кеннет Колби разработал программу Пэрри для лечения шизофрении.

1995 год - Ричард Уоллес создал первого виртуального собеседника A.L.I.C.E., программу, способную вести диалог с человеком на естественном языке.

2006 год – IBM предложила компьютерную программа, которая могла отвечать на вопросы и конкурировать с людьми на популярном телевизионном шоу Jeopardy!

2010 год — Apple создает Siri — первого интеллектуального персонального помощника, который беседует с пользователями, которые инициируют голосовые запросы посредством обработки естественного языка. Это было инновацией, за которой последовали виртуальные помощники от Google, Amazon & Microsoft.

2016 год - Facebook Messenger стал самым большим «домом» для чатботов. В настоящее время в нем размещено более 1 000 000 ботов из разных сегментов.

2017 год – Бот от здравоохранения Woebot был разработан для взаимодействия с пациентами, страдающих депрессией и дальнейшей реабилитации их.

Современное использование.

Благодаря своим универсальным качествам технология чатботов приобрела широкое распространение. Фактически, умный помощник способен ответить на любой вопрос, достаточно только качественно обучить его.

Выделяются четыре основные направления использования ботов:

1. Консультирование. От заказа букета цветов до медицинской консультации. 24 часа в сутки. Мы каждый день встречаемся с подобными ботами, не всегда замечая разницу. Звонок в авиакомпанию, изменение тарифного плана, остаток на банковском счёте – задача ботов общаться с клиентами и решать их проблемы. Раньше люди серфили в интернете в поисках ответа на вопросы. Сегодня мессенджеры заменили всё. Больше не нужно искать, можно просто задать свой вопрос в чате, и мгновенно получить ответ.

Кейс: Создатели бота компании «Вкусвилл» считают, что эпоха мобильных приложений стремится к закату. Их стало неприлично много. Встроенный в Telegram бот поможет изменить любимый продукт, покажет все скидки и предложения, найдет ближайший магазин и постарается ответить на любые вопросы клиентов.

2. Рутинные задачи. Бизнес-помощники избавят вас от простых задач, которые съедают время специалистов, и сделают их жизнь проще. Повторяющиеся взаимодействия с поставщиками, первый уровень технической поддержки офиса, расписание конференции, бронирование помещений для переговоров, печать документов и покупка авиабилета – поручите эти дела интеллектуальному помощнику, и займитесь чем-то действительно нужным.

Кейс: Весной этого года Альфа Банк запустил интеллектуального чатбота, который каждый день принимал более сотни звонков от сотрудников с вопросами по условиям и правилам открытия расчетных счетов клиентам в рамках зарплатных проектов. Это были стандартные вопросы, ответы на которые также достаточно однообразны и унифицированы. Как заявляют представители банка, бот умеет общаться на простом и понятном языке.

3. Сокращение расходов и экономия времени сотрудников. В будущем боты смогут заменить целые бизнес-подразделения. Но, это не означает, что люди останутся без работы – у них появятся другие, более интересные задачи, в которых они смогут лучше реализовать свой потенциал.

Кейс: Рекрутеры крупных компаний тратят половину своего времени на первоначальный отсев кандидатов: место жительства и готовность к переезду, уровень образования и прочее. «Пятёрочка» ввела в эксплуатацию бота, который связывался с кандидатами в мессенджере, задавал им вопросы, «отсеивал» неподходящих и автоматически назначал интервью с подходящими. Бот позволяет HR отделу сэкономить до 200 человекочасов в месяц и снизить время на подбор сотрудника с 7–20 дней до пяти с половиной.

4. Продвижение и продажи. Сегодня 95% пользователей мирового интернета используют мессенджеры в повседневном общении. Время использования подобных приложений превышает отметку 2 часа в день. В среднем в смартфоне россиянина установлено от 3 до 6 мессенджеров. Согласно опросу Facebook, более 50% клиентов говорят, что они с большей вероятностью совершают покупки у бизнеса, с которым они могут общаться с помощью чата.

Кейс: Чатбот H&M не только дублирует функции сайта и мобильного приложения, где помогает оформить заказ, но и может порекомендовать клиенту тот или иной предмет одежды, исходя из истории поиска и предыдущих сообщений.

На волне

Сейчас наблюдается большой интерес у бизнеса к интеллектуальным разговорным агентам. Рынок чатботов растет с огромными темпами и достигнет 1,34 млрд. долл. США в 2024 году. Этот рынок создает возможности для роста. Основываясь на первоначальных достижениях «чатботов» для базового поиска информации, такие продукты, как Alexa и Google Home, демонстрируют новые подходы к использованию разговорных средств коммуникации. Объединяя мощь автоматизированной речи с персонализированной информацией о клиентах, агенты, управляемые AI, напрямую взаимодействуют с клиентами, чтобы быстро обрабатывать претензии, перечислять средства в банковской сфере, обновлять маршрут поездки или регистрироваться в программе лояльности.

Возможность говорить естественным образом с обученным «агентом виртуальных услуг», который имеет способность обнаруживать интерес клиента и связывать эти интересы с индивидуальным набором решений, может существенно повысить ценность услуг. Новые, более эффективные, модели виртуальной помощи, построенные с использованием предобученного алгоритма, устанавливают новый уровень для взаимодействия с клиентами. Они повышают удовлетворенность клиентов, уверенность и лояльность.

Цифровая лаборатория Softline обладает не только знаниями, но и реальным опытом использования инновационных технологий для создания цифровых сервисов для различных сфер бизнеса.

Сейчас лаборатория разрабатывает виртуального помощника для одного из крупнейших российских food ритейлеров. Проект включает в себя создание чатбота на платформе DialogFlow, который полностью заменит собой первый уровень внутренней поддержки. Технологии ИИ на базе современной платформы обеспечат сотрудникам компании помощь практически в любых задачах: от вопросов административного свойства до ИТ - сопровождения бэкофиса. Проект решит сразу несколько насущных проблем компании:

5. Снизит нагрузку на сервисный отдел ИТ департамента.
6. Соберет информацию о сотрудниках компании, чтобы в будущем повысить уровень ответов и выдавать целевые рекомендации.
7. Повысит лояльность к работодателю и увеличит вовлеченность сотрудника в процессы компании.

В разработке бота используются передовые технологии, мы изучаем отраслевую экспертизу, передовой мировой и российский опыт. Практики и идеи цифровой трансформации из нашей базы знаний помогают сформировать наилучший продукт.

В планах цифровой лаборатории Softline внедрение голосового интерфейса – в будущем специалисты компании смогут общаться с ботом, не отрываясь от дел в реальном времени. Мы уверены, что это улучшение откроет новые возможности для разных категорий сотрудников.

Интернет-магазин Softline готов к росту ИТ-рынка

Интернет-магазин **store.softline.ru** известен как поставщик программного обеспечения в сегменте B2B, хотя на сегодняшний день активно продает компьютерную технику и офисное оборудование не только компаниям, но и физическим лицам. Магазин уделяет большое значение развитию клиентских сервисов и готов к любым изменениям на рынке ИТ.

В 2019 году ожидается рост мировых расходов на устройства. Эксперты Gartner считают, что в новом году расходы на ПК, планшеты и мобильные телефоны вырастут на 2,4%, достигнув $706 млрд против $689 млрд в текущем году.
Также по данным исследования, в 2019 году мировой рынок ИТ-услуг достигнет уровня в $1 трлн, что на 4,7% выше, чем в 2018. Ожидается также более чем 8% увеличение расходов на корпоративное программное обеспечение.

Предупрежден, значит, вооружен. Интернет-магазин **store.softline.ru** готов к росту спроса на ИТ-решения даже с учетом одновременного возрастания популярности онлайн-покупок. Большое значение уделяется улучшению сервисов, сокращению цикла покупки, оптимизации взаимодействия с клиентами. Команда **store.softline.ru** активно тестирует и внедряет новые инструменты, анализирует результаты уже зарекомендовавших себя сервисов с целью улучшения их эффективности.

Это интересно!
88% опрошенных Gartner ИТ-директоров во всем мире в последующие 12 месяцев планируют повысить уровень кибербезопасности в компаниях. Уже сейчас среди покупателей интернет-магазина store.softline.ru наблюдается повышенный спрос на корпоративные антивирусные решения таких вендоров, как «Лаборатория Касперского», ESET и многих других.

Быстрый заказ от 10 мин

В store.softline.ru оптимизирован и ускорен процесс онлайн-покупки электронных лицензий таких популярных вендоров, как Microsoft, Adobe, Corel и др. Теперь ключи отправляются автоматически за время от 10 минут. Не все электронные лицензии возможно доставлять так быстро в связи с особенностями лицензирования.

Оптимизация процесса доставки

Интернет-магазин постоянно работает над увеличением скорости доставки и оптимизацией ее стоимости. Это особенно актуально для регионов, удаленных от Москвы.

Персонализация

Немаловажным фактором полноценной автоматизации является максимальное количество данных: история покупок, поведение пользователей на сайте (просмотр страниц, длительность посещения и др.) и т.д.
Система персональных рекомендаций интернет-магазина **store.softline.ru** анализирует поведение посетителей сайта и в режиме реального времени подстраивает его под каждого отдельного пользователя. Важно, чтобы клиент видел свою собственную версию интернет-магазина и без особых усилий мог приобрести то, что ему действительно нужно.
Еще мы отправляем персонализированные рассылки с товарами, оставленными в корзине, и напоминаем о ранее просмотренных категориях страниц и карточек товаров.
Благодаря таким письмам значительно возросло число покупателей, вернувшихся на сайт и завершивших оформление заказа.
Большое количество благодарственных отзывов от клиентов показывает, что наши усилия не остаются незамеченными.

SOLIDWORKS-2019. Проще, быстрее, функциональнее

В SOLIDWORKS 2019 акцент разработчики сделали на 4-х основных моментах: инновации, производительность, экосистема проектирования и внимание к деталям. Особенно заметно улучшение работы новой версии с большими сборками: за счет обновления графического движка манипулировать сложными объектами стало удобнее и быстрее. Андрей Виноградов, технический менеджер SOLIDWORKS, Dassault Systèmes в России и СНГ, на примерах рассказал о нововведениях в этой версии программы

Действительно ли со сложными объектами стало удобнее работать?

Приведу пример. Предположим, у нас есть сборка на 12 тысяч компонентов. В новой версии программы он открылся за 2 минуты. Мы можем легко вращать модель, делать операции, открывать подсборки, редактировать их. Если это делать в предыдущей версии, то даже открыть этот объект будет затруднительно, не говоря уже о том, чтобы работать с ним. Так что здесь на лицо высокая производительность в плане работы с большими, сложными объектами.

Что из себя представляет построение сечений по сетчатой модели?

Возьмем пример с джойстиком. Хотя модель поверхности этой рукоятки и выглядит гладкой, она состоит из треугольников. Для построения сплайновой поверхности в предыдущих версиях пользователям приходилось рисовать промежуточные сечения: команда лофтинга, протягивание по сечениям, отрисовка поверхности. А сейчас можно взять эту сетчатую модель из треугольников и рассечь ее десятью плоскостями с заданным шагом. SOLIDWORKS-2019 автоматически рисует сплайны. При этом, когда вы будете создавать сечения, есть опция точ-

но рисовать или приблизиться к этому сплайну, аппроксимировать. А потом можно сетчатую модель убрать, и по этим сечения построить необходимое вам тело.
Появилась новая команда – «Структурная система». Предположим, что мы делаем рамную конструкцию, состоящую из разных профилей. На ежегодном российском форуме SOLIDOWRKS в своей презентации я показывал рамную конструкцию, удерживающую главное зеркало на телескопе. Рамная конструкция действительно сложная, 3-4 метра длиной. В предыдущей версии ее тоже можно было построить, но для этого необходимо строить 3D-эскизы. В новой версии в дополнение к прежней технологии, можно использовать поверхности. Например, если мы нарисуем 2D-эскиз прямоугольник и выдавим его как поверхность, то получим параллелепипед из 12 ребер, их можно использовать для построения рамной конструкции. Мы на порядок быстрее построили скелетную основу для нашей рамной конструкции. Это существенное ускорение по сравнению с предыдущим способами.

Как работает генерация текстурных поверхностей?

Представьте, что у нас есть текстурная поверхность. Если это какие-то выступы (прямоугольные, или круглые, любые), то еще можно затратить время и нарисовать окружность или прямоугольник, выдавить его, потом размножить с помощью команды «Массив», сделать округление и т.д. Но это достаточно кропотливая и «героическая» работа. Если вместо прямоугольников будут окружности, то придется делать новую конфигурацию и продолжать построение.
Что предлагается в новой версии SOLIDWORKS 2019? Выбираем файл с расширением .bmp (это черно-белая картинка), проецируем и масштабируем на редактируемую поверхность - это будет трехмерная текстура. И даем команду превратить ее в 3D. Передвигая слайдер, задается величина – глубина и точность текстуры. В результате за один проход мы получаем на криволинейной поверхности сложную текстуру.

В новой версии, как мы знаем, реализована возможность работы с сенсорными экранами. Считаете ли вы сенсорные экраны перспективной технологией для моделирования сложных объектов?

Я бы назвал это постепенным развитием инструментария для проектирования. Сенсорные экраны появились недавно, и у них определенно есть потенциал. На них можно и нужно работать. Владелец сенсорного экрана может, к примеру, рисовать картинки, но не все могут себе позволить проектировать конструкции на таком экране. Такую возможность предоставляет как раз SOLIDWORKS-2019. В инженерной среде не настолько распространился сенсорный экран, но, если вспомнить, не так давно мониторы с трудом вмещались на стол, а теперь уже таких «толстых» мониторов и не найдешь.

Как обстоят дела с дополненной реальностью?

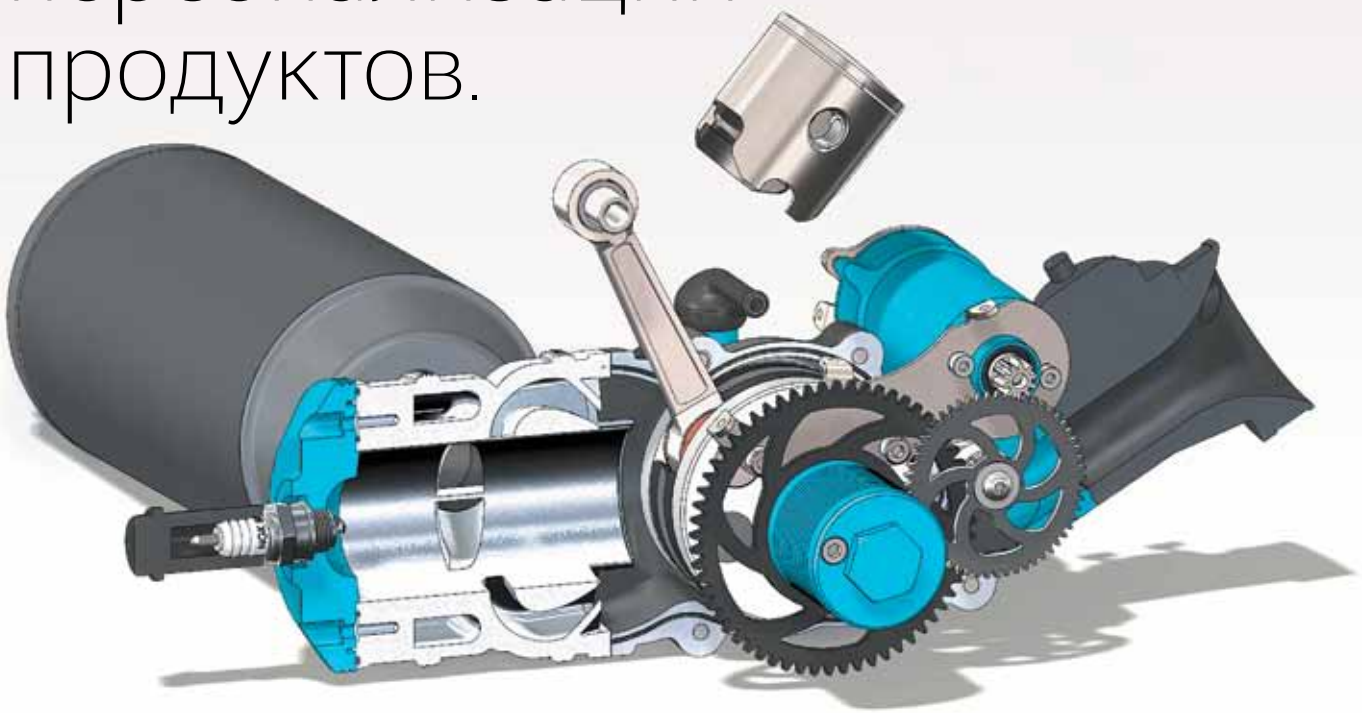
Дополненная реальность реализована в модуле E-Drawings. К примеру, если мы что-то проектируем: я проектирую, а вы – заказчик. У меня появилась идея, и я вам начинаю объяснять ее по телефону. И естественно мы никогда не договоримся: это займет слишком много времени. Но у меня есть возможность трехмерную модель сохранить в формате 3д pdf и отправить вам на почту. И вы можете наглядно увидеть трехмерную модель, изучать ее, делать сечения, замеры, смотреть конфигурации.

Есть ли способы не раскрывать перед заказчиком все детали проектируемого объекта или скрывать часть из них?

Действительно, не всегда хочется раскрывать свои хитрости, как тот или иной узел работает. Для этого есть функция упрощения сборок. В 19-й версии можно упростить модель так, что она будет узнаваема.
Возьмем пример с лебедкой. После упрощения остается внешний кожух и крепления к направляющим рельсам. Остальные элементы: гайки, пластины, блоки управления двигателем, какие-то можно упростить в виде параллелепипедов.
А вот двигатель нельзя упростить, он будет неузнаваем. Для этого есть инструмент создания силуэтов: делаем силуэт с одного бока и с торца, и Solidworks нам рисует трехмерный узнаваемый объект. Заливаются внутренние области. Упрощенная сборка передается заказчику. ▮

Андрей Виноградов, технический менеджер SOLIDWORKS, Dassault Systèmes в России и СНГ

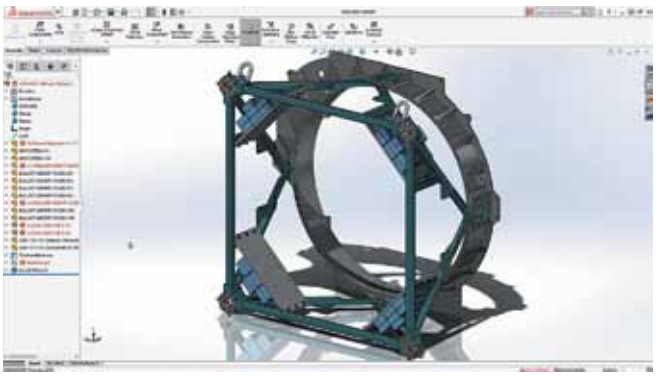
SOLIDWORKS Sell: облачная 3D технология персонализации продуктов.



Технология, позволяющая использовать инженерные данные в продажах и продвижении продукции компании.

Что из себя представляет?

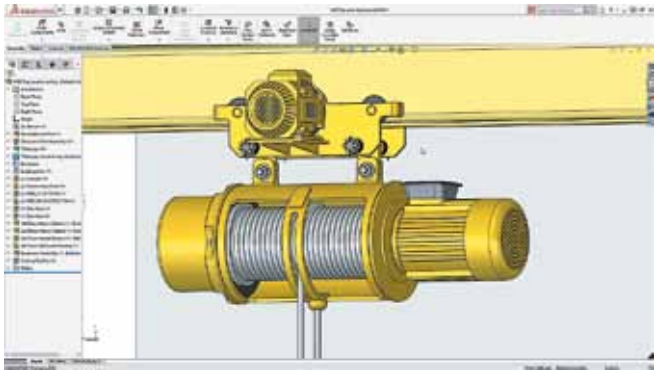
SOLIDWORKS Sell – это решение, которое позволяет инженерам поделиться данными 3D моделей с руководством для принятия решений, с отделом маркетинга для продвижения продукции, с отделом продаж для демонстрации продуктов покупателям. Или же сразу разместить модель в интернет магазине для заказчиков. Важнее всего, что SOLIDWORKS Sell позволяет моментально создать конфигуратор изделия и вместо каталога на 500 страниц можно использовать одну страничку в интернете. Похожие технологии есть у автопроизводителей, когда клиент выбирает комплектацию, цвет и видит соответствующие изменения изображения автомобиля.



Доступно каждому

Создать конфигуратор изделия может любой инженер. Интуитивно понятный облачный сервис содержит необходимые заготовки полей и видовых окон. Инженеру достаточно загрузить модель, выбрать какие конфигурации будут доступны для изменения, какие должны меняться вместе, перетащить готовые блоки в область верстки сайта и конфигуратор готов. Далее достаточно перейти по ссылке и можно формировать свою конфигурацию изделия. Если необходимо разместить конфигуратор на сайте компании, то будет предоставлен код для вставки на страницу.

Возможности



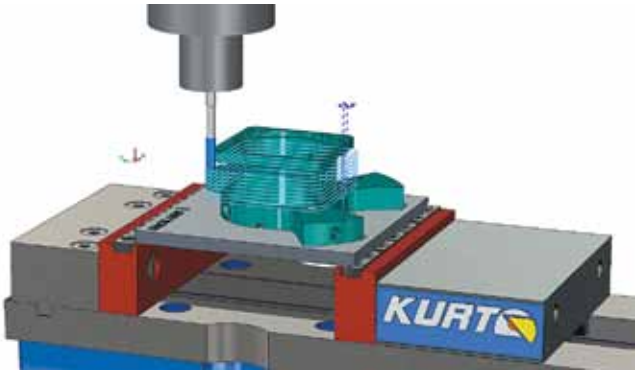
Попав на страничку с изделием в SOLIDWORKS Sell пользователь имеет ряд преимуществ перед обычным конфигуратором:

- Возможность просматривать 3D модель с любого ракурса
- Возможность сохранить несколько конфигураций и переключаться между ними
- «На лету» формировать фотореалистичные изображения текущего ракурса
- Получить габаритные размеры модели
- Увидеть цену конкретной уникальной конфигурации
- Посмотреть на товар в естественном окружении. Поддержка дополненной реальности позволяет примерить очки, посмотреть как будет смотреться шкаф в комнате, или прикинуть станок в цех и т.п.
- Возможность сразу добавить товары в корзину и заказать их.

Помимо перечисленных преимуществ для пользователя, компания получает аналитику. Собираются данные о том сколько пользователей посетило сайт, какие конфигурации пользуются популярностью. Можно добавить средства аналитики и получать информацию о том, сколько раз человек улыбнулся, конфигурируя изделие.

Преимущества

Данное решение дает клиенту легко создать товар уникальный, «для себя». Допустим у нас есть стул с пятью видами спинок, тремя видами ножек пяти цветов, пятью сидушками и с пятью цветами отделки для спинки и для сидушки. Итого 9 375 вариантов стула. Конечно проще использовать одну страничку чем печатать каталог, в котором больше 9 000 элементов.

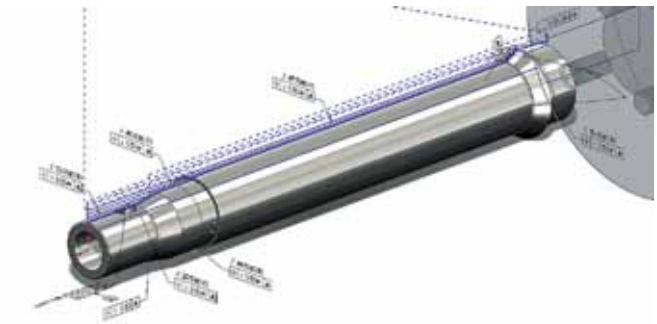


Компания, производящая уникальные конфигурации очков под заказ, рассчитывала на продажи в районе 1% через сервис, а в итоге 75% продаж Aspire Custom так или иначе связаны с SOLIDWORKS Sell.

Оценить удобство решения и посмотреть примеры использования можно на сайте **www.solidworks-sell.com.**

Несомненно, менеджеру на объекте будет проще выбрать необходимую конфигурацию вентиляторов, например, или светильников и сразу в корзине сохранить спецификацию, чем возиться с каталогом и с запоминанием пожеланий заказчика.

Схемы работы сервиса



SOLIDWORKS Sell предлагается для использования в трех видах:

- Customize
- Digital Catalog
- eCommerce

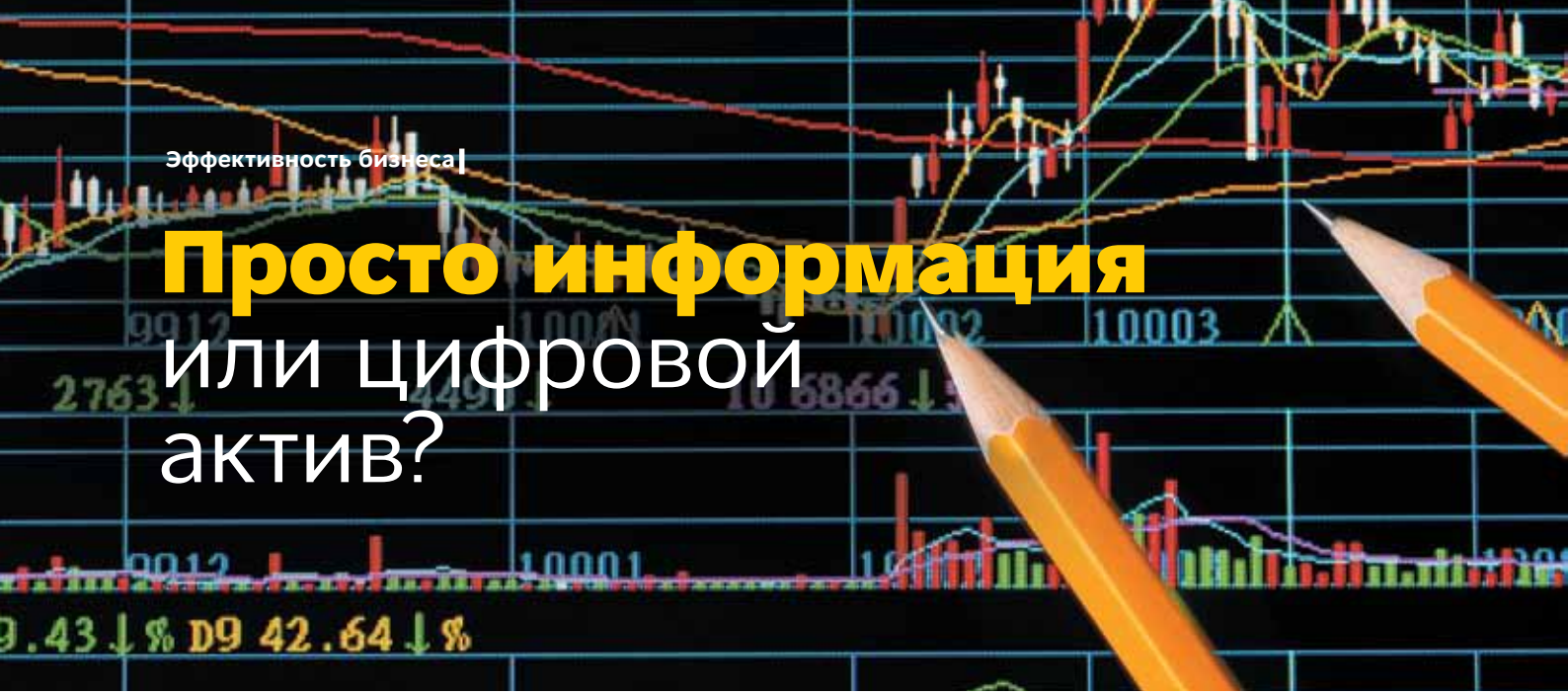
Customize – Это решение базового уровня с ограничением по количеству одновременно работающих пользователей в 5 человек, размещается конфигуратор в домене SOLIDWORK, подходит для внутренних задач. Для инженеров и отдела маркетинга и продаж.

Digital Catalog – Электронный каталог. Располагается на сайте компании производителя. Для клиентов.

eCommerce – Для клиентов. В данном варианте конфигуратор дополняется элементами интернет магазина, такими как корзина и онлайн оплата.

Остались вопросы? Обращайтесь к специалисту:

Виталий Лоза, ведущий специалист PLM/CAD/CAM Департамента САПР и ГИС, Softline



Просто информация или цифровой актив?

Цифровая трансформация – не просто общемировой тренд, но и метод получения организацией новой прибыли. Для повышения эффективности и сокращения расходов меняются как внешние, так и внутренние бизнес-процессы. А любая информация рассматривается как актив, который потенциально можно монетизировать. Извлекаете ли вы максимум из данных, которыми располагаете?

Как это сделать, понятно не всегда

Цифровые активы есть у каждого бизнеса, но не все умеют грамотно им распорядиться и найти данные, которые могут принести прибыль. Это первая ошибка, возникающая из-за ограниченного взгляда на процессы. Вторая – работать только с ограниченным количеством источников информации. Третья – не иметь никакой методологии работы с данными. Все эти ошибки помогают устранить консультанты, аналитики big data и специалисты по Интернету вещей.

Один из лучших поставщиков данных?

Интернет вещей! Датчики, установленные на технике, производственном оборудовании и людях, позволяют собирать информацию и на ее основе предсказывать вероятность потенциальных поломок и сбоев, недостаточной загруженности и целый ряд других ситуаций и событий. При этом, если того требует законодательство, данные могут быть абсолютно деперсонализированными.

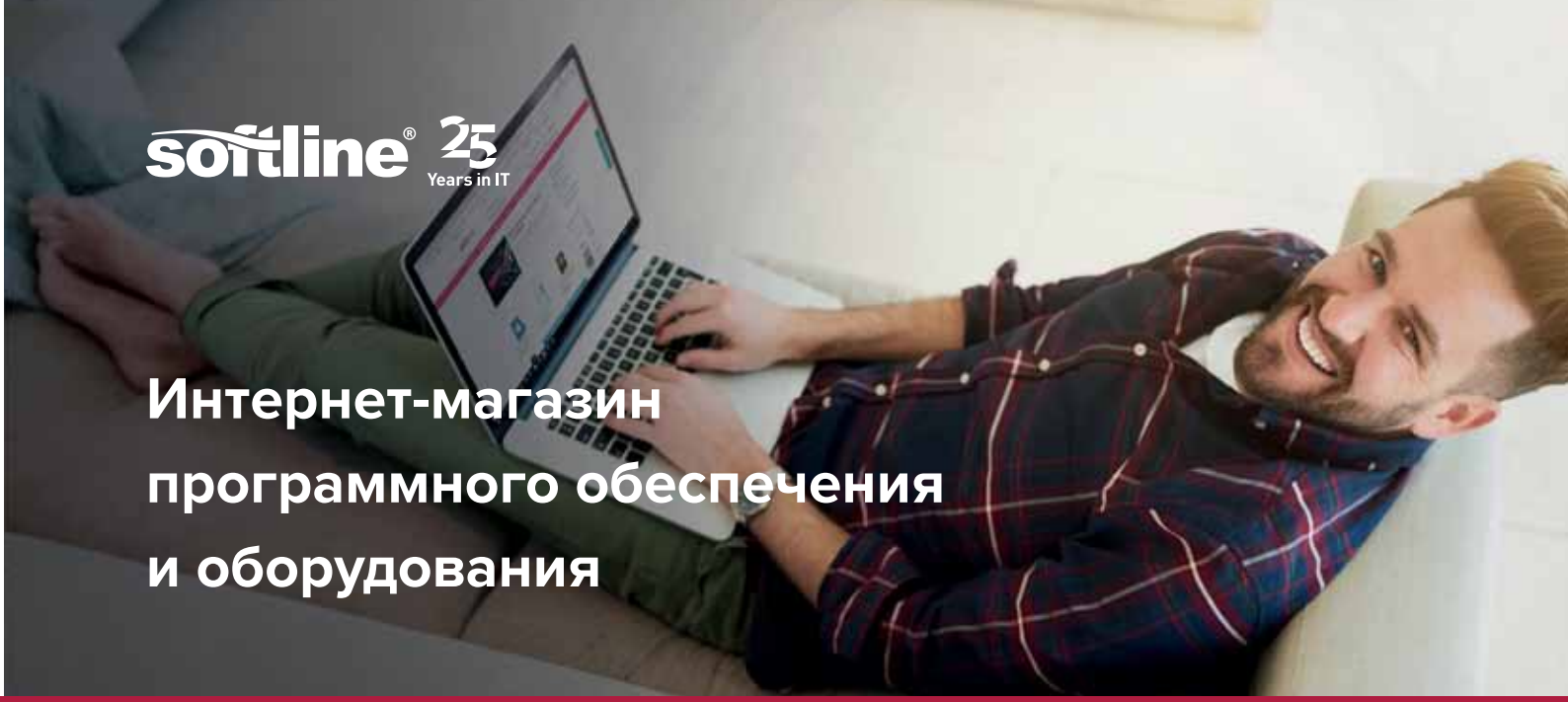
Повышайте эффективность бэк-офиса

Начиная проект, связанный с искусственным интеллектом или интернетом вещей одновременно автоматизируйте и бэк-офис, все департаменты, ежедневно решающие изо дня в день ряд повторяющихся задач. Бухгалтерия, кадровики, логисты, контентщики, секретари – сколько всего процессов проходит через их руки каждый день?

Обратите внимание на систему управления бизнес-процессами WorkFlowSoft, которая значительно сокращает объем электронных писем, упрощает коммуникацию и упорядочивает дела. Работать в ней можно со стационарного компьютера или мобильного девайса. WorkFlowSoft не только ускоряет бизнес и уменьшает количество ошибок, но и собирает данные для анализа и отчетов. Вы увидите, сколько задач выполнено и кем, какие оценки по итогам каждого процесса получали исполнители.

Работать в WorkFlowSoft удобно за счет простого интерфейса системы. Никаких навыков программирования для работы в системе не требуется. Такая внутренняя автоматизация имеет свое значение в деле накопления данных, которые могут впоследствии стать цифровом активом. Информация меньше теряется, лучше систематизируется, формируется в списки и т.д.

Еще больше возможностей WorkFlowSoft вы найдете на официальном сайте. Узнайте, какие три бизнес-процесса вы можете упростить уже сегодня:
https://workflowsoft.com/ru/blog/forbeginners



softline® 25 Years in IT

Интернет-магазин программного обеспечения и оборудования

Для малого и среднего бизнеса, государственных организаций, учебных заведений и других организаций

Преимущества:

- Более 25 000 позиций оборудования и программного обеспечения
- Мгновенное получение счета и шаблона договора
- Автоматическая отправка бухгалтерских документов на e-mail
- Отслеживание статуса оплаты заказа
- Возможность работать по электронному документообороту.
- Доставка по России
- Постоянный доступ к данным заказа и документам
- Служба поддержки
- 5 звезд на Яндекс-Маркет
- Достаточно только ИНН. Остальные реквизиты заполняем автоматически.

Microsoft · Adobe · embarcadero · Hewlett Packard Enterprise · ASUS · KASPERSKY lab

Authorised Systems Integrator · AUTODESK. Gold Partner · DELL · ABBYY · Acronis · ATLASSIAN

Altium · DevExpress · COREL · eset · TeamViewer · VEEAM

Ещё более 1000 производителей доступно на сайте

store.softline.ru

STATiSTiCA

IoT - Analytics!

Аналитические исследования Интернета Вещей

Постигаем Умные Данные...

@cademy

StatSoft®

IoT-Аналитика, Курсы Академии Анализа Данных!

Закажите прямо сейчас: sale@statsoft.ru

+7 (495) 78 777 33 | www.statsoft.ru