softline direct

КАТАЛОГ ИТ-РЕШЕНИЙ И СЕРВИСОВ ДЛЯ БИЗНЕСА

СПЕЦВЫПУСК 06/2019

ИТ В ФИНАНСАХ

Решения и проекты для финансовой сферы

Как тебе живется, банк? | Fraud Detection System as a Service | Бизнес-аналитика для финансистов | Наши проекты для банков и многое другое

ПО для разработки графического дизайна

CorelDRAW Graphics Suite 2019 можно приобрести в магазине www.allsoft.ru

CorelDRAW® GRAPHICS SUITE 2019

Инновационный и продуктивный

С новыми высококлассными функциями вы сможете достичь высочайшего уровня производительности. Кроме всего прочего, новое приложение CorelDRAW.app обеспечивает удаленный доступ ко всем вашим проектам.

Креативный и настраиваемый

Профессиональные инструменты для работы с векторными объектами и макетами страниц, стили документа, а также недеструктивные эффекты для растровых и векторных изображений обеспечат максимально комфортные условия для создания оригинальных иллюстраций, вывесок и логотипов для печати и публикации в интернете.

Простой в освоении и использовании

С интуитивными инструментами, учебными материалами, советами и подсказками вы сможете быстро приступить к работе и добиться отличных результатов в самые рекордные сроки. Разнообразные новые шаблоны устраняют необходимость в разработке проектов с нуля и поэтому существенно ускоряют процесс создания плакатов, открыток, изображений для размещения в социальных сетях и других материалов.

CorelDRAW® GRAPHICS SUITE 2019

Доступна версия CorelDRAW Graphics Suite 2019 For Mac!

Уважаемые читатели!

В этом выпуске Softline-direct мы рассказываем о решения и проектах, которые Softline реализует в финансовой отрасли. Банки, кредитные, инвестиционные и страховые организации исторически находятся на первой линии технологического прогресса. И дело даже не в том, что у этого сектора есть средства на инновации. Просто отдача от цифровизации здесь наиболее высока, а потери в случае отставания могут стать катастрофическими. Ведь сегодня никому не придет в голову обратиться в банк, который не предоставляет обслуживания через интернет.

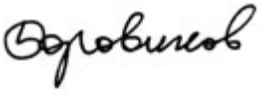
Для Softline финансовые организации составляют большую и важную часть клиентской базы. Это интересные и требовательные заказ чики, ими востребованы сложные высокотехнологичные решения с высокой интеллектуальной составляющей. Тот факт, что они доверяют нам ответственные и дорогостоящие проекты, говорит, что Softline оправдывает их ожидания, предоставляя инновационные решения и сервис высочайшего качества.

Для компаний финансового сектора цифровая трансформация уже стала привычным образом жизни. Они отлично знают свои цели и способны обоснованно составлять дорожную карту своих цифровых изменений. Работу с такими заказчиками мы считаем большой честью и ответственностью. Мы помогаем финансовым организациям работать лучше, быстрее, эффективней и сами получаем в таких проектах неоценимый опыт.

Ни в какой другой отрасли кибербезопасность не играет такой значительной роли, как в финансовом секторе. Поэтому финансисты демонстрируют, пожалуй, самый серьезный и обдуманный подход к защите своих данных, приложений, информационных систем. Накопленный опыт и компетенции позволяют Softline обеспечивать заказчикам высочайший уровень защиты и снижать их расходы на безопасность.

Я уверен, что финтех останется на гребне волны технического прогресса и в будущем. Компании этого сегмента встроены практически во все экономические цепочки и во многом стимулируют прогресс в других отраслях — от горнодобывающей до онлайн-ритейла. А мы со своей стороны концентрируем свои усилия на том, чтобы помогать заказчикам из финансового сектора быть конкурентоспособнее и выводить на рынок новые невиданные ранее продукты и услуги.

Игорь Боровиков,
Председатель совета директоров Softline



Каталог
ИТ-решений
и сервисов
для бизнеса

Softline
direct

#06-2019

2019-6(194)–RU

Учредитель:
АО «СофтЛайн Трейд»

Издатель:
Игорь Боровиков

Главный редактор:
Максим Туйкин

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

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

Над номером
работали:
Георгий Теплов,
Станислав Воронин,
Илья Тихонов,
Светлана Ащеулова,
Юлия Буданова,
Полина Дуйкова,
Владимир
Александров,
Александр
Дворянский,
Екатерина
Скороходова, Елена
Яковлева, Мария
Агаркова.

и др.

Тираж: 60 000 экз.

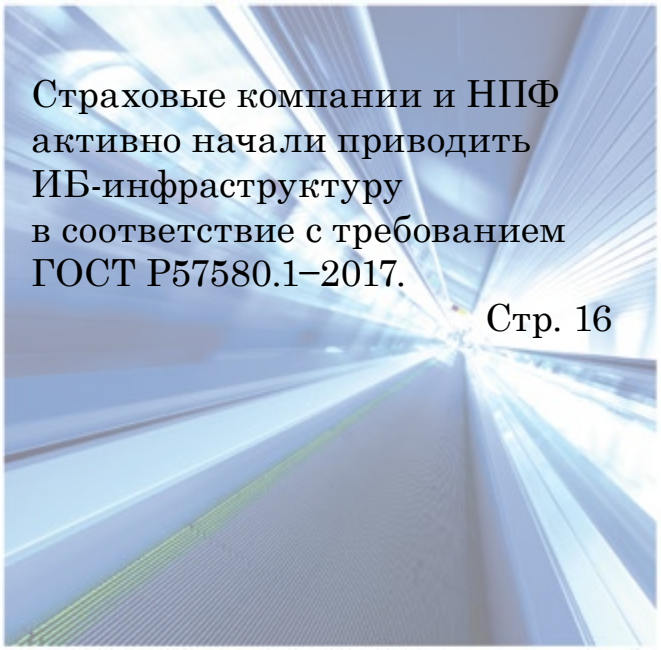
Зарегистрировано
в Государственном
комитете РФ
по печати,
рег. ПИ № ФС77-71088
от 13 сентября 2017 г.

СОДЕРЖАНИЕ

СПЕЦИАЛЬНЫЙ ВЫПУСК:
ИТ В ФИНАНСАХ

Softline в соцсетях

SoftlineCompany Softlinegroup SoftlineCompany softlinegroup



Страховые компании и НПФ активно начали приводить ИБ-инфраструктуру в соответствие с требованием ГОСТ Р57580.1–2017.

Стр. 16

Финансовый сектор — этакий «город контрастов». С одной стороны, продвинутый и футуристичный, с другой — весьма зарегулированный.

Стр. 8

Как отслеживать преступные действия в системах дистанционного банковского обслуживания? С помощью системы Fraud Detection System as a Service!

Стр. 18

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

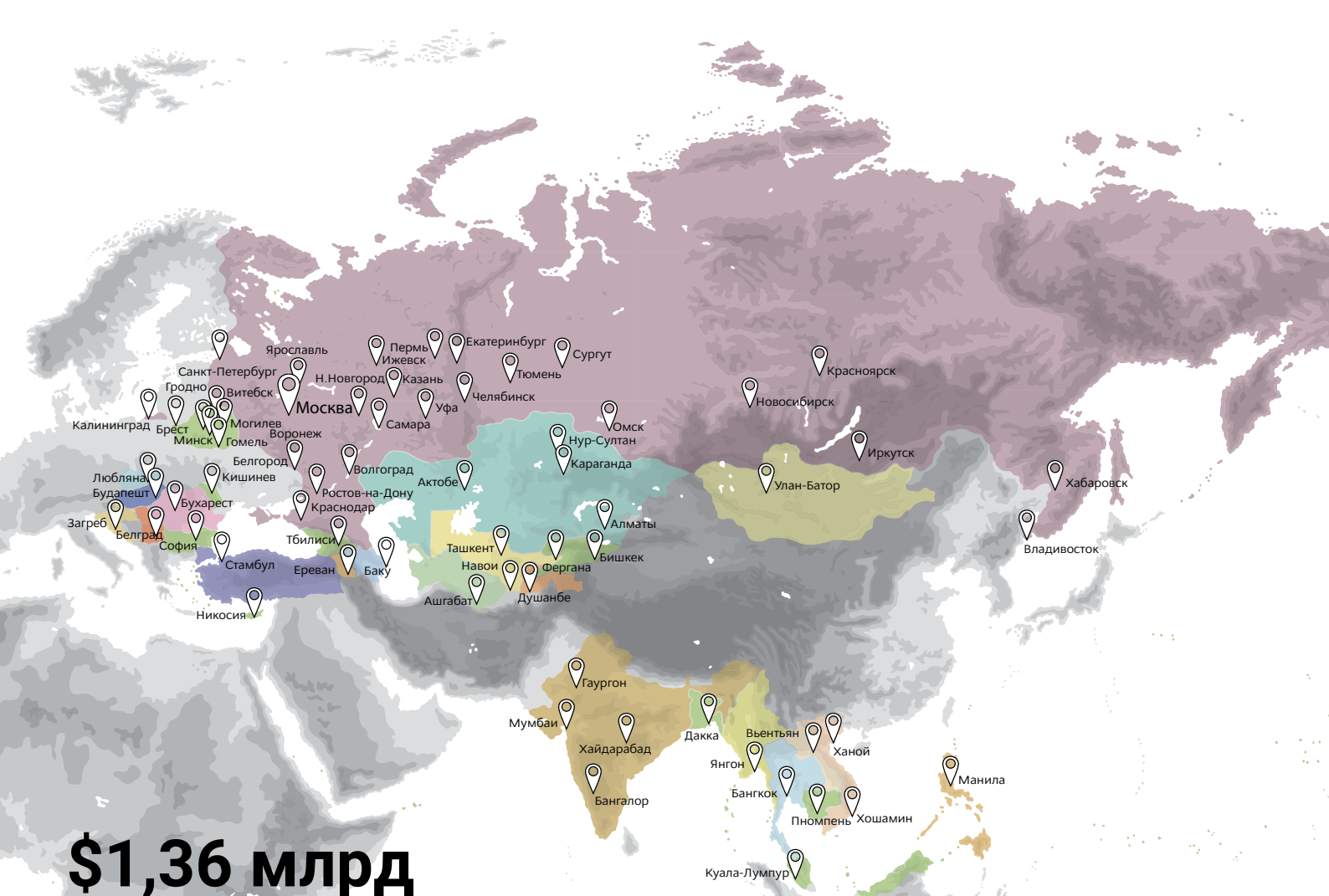
Microsoft Partner

- 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 · Hewlett Packard Enterprise Gold Partner

Authorised Systems Integrator · IBM Gold Business Partner · intel Software Elite Reseller · CITRIX PARTNER Platinum Solution Advisor

Acronis Gold Partner · VERITAS Partner Force Platinum Partner · APC · eset Corporate Premier Partner



$1,36 млрд
оборот по группе компаний в 2018

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

+32% рост (руб.) 2017/2018 по группе компаний

+19% рост ($) 2017/2018 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

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

3000+ поставщиков программного и аппаратного обеспечения

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 | РИРВ | 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

ЦЕННЫЕ КОМПАНИИ: как тебе живется, *БАНК*?

Финансовая сфера по праву считается одной из самых технологически передовых: банки, страховые, инвестиционные, брокерские компании идут к новому быстрее и раньше других. Решения, которые, например, в промышленности только внедряются, в банках используются давно; аналогичные результаты получим и при сравнении финсектора с другими отраслями.

Вначале было...

Существует мнение, что вначале был банк, а потом наступила эра ИТ-банков. Удивительная метаморфоза превратила привычную структуру в пост-ИТ организацию. Простой пример: всем знакомый «Сбербанк» развивает сервисы, построенные на информационных технологиях, и не связанные напрямую с банковской сферой. Это уже не просто финансы, это высокотехнологичное ИТ.

Что востребовано?

Финансовый сектор — этакий «город контрастов». С одной стороны, продвинутый и футуристичный, с другой — весьма зарегулированный. Технологические системы востребованы не менее, чем соответствие требованиям многочисленных законов и указов. Поэтому многие ИТ-проекты, заказываемые здесь, посвящены именно консалтингу — например, касательно ГОСТ 575801 и различных постановлений, в том числе 382-П Центробанка.

Особые ингредиенты

Что до специфических систем, интересных компаниям-финансистам, то здесь выделяются АБС — автоматизированные банковские системы, а также биометрические решения. С недавнего времени банки собирают биометрические данные граждан (такие как голос и рисунок радужки глаза) и вносят их в Единую биометрическую систему. Интересно, что собранную информацию сам банк может в своей работе и не использовать вовсе.

Различные требования регуляторов ограничивают возможности банков в плане обустройства своего ИТ-хозяйства. Персональные данные российских граждан должны храниться на терри-

тории России, а не за рубежом; в облаке или локально — неважно. Облако Softline сертифицировано по 152-ФЗ, об этом мы рассказывали не раз. А вот к несертифицированным облакам возникает вопрос, в России ли они на самом деле?

В чем залог конкурентоспособности

Как банку выделиться на фоне себе подобных — ну уж точно не за счет того, что есть у всех, например, интернет-банкинга. Здесь ставки стоит делать на нечто гораздо более нетривиальное. Скажем, на интеграцию банковского сервиса с чем-то смежным — учетом и взаимозачетом средств, компенсацией определенных услуг сторонней компании (например, такси), кросс-селлингом. Вы открываете счет — и на всю оставшуюся жизнь получаете пятидесятипроцентную скидку в хорошем ресторане. Это вовсе не приятные бонусы для клиентов, это новая суть бизнеса: в ближайшем будущем банки будут зарабатывать не на собственно банковских услугах, а на том, какие сервисы будут предоставлять и прикреплять к вашему счету через шины интеграции.

Угрозы!

Говорим «банк» — читаем «мишень». Банки как желанную цель хакеры пробуют вскрыть любыми доступными методами и средствами — в том числе через вербовку людей на даркнете. Вы еще не видели объявлений вроде «Ищу инсайдера»? А они есть.

Что еще актуально? Фрод, проникновение за периметр, внутренние нарушения, фишинг — в такой атмосфере выстраивать глубоко эшелонированную защиту просто необходимо. Но легко ли держать оборону, в которой важен каждый элемент? Конечно нет. Неудивительно, что новости не устают пестреть заголовками об атаках на финансовые организации и, к сожалению, о потерях со стороны последних.

Они первыми поняли важность антивирусов, актуальность защиты рабочих станций, виртуальных серверов, периметра, и стали делать ставку на комплексную защиту.

Парадокс в том, что во многих банках не хватает рук для того, чтобы просто поддерживать все ИБ-системы, не говоря уже о том, чтобы расследовать и полноценно реагировать на атаки и инциденты, а не только отражать их. Именно поэтому для многих актуален тот или иной вид ИТ-аутсорсинга.

Security Operation Center (SOC)

Звучит здорово, серьезно, внушительно. Центр управления инцидентами объединяет в себе технологическую часть, досконально описанные процессы и компетентных специалистов. В конечном итоге, SOC — это алгоритмы, глубокое понимание того, как работать с инцидентами и как каждое действие будет влиять на будущие результаты.

Об этом классе систем задумывается практически каждая финорганизация, но отношение к данной технологии зависит от психологии управляющего звена. Тут обнаруживаются две устойчивые группы: первая — «Все у себя, ничего наружу», и вторая «Мы за открытый подход с положительным отношением к аутсорсингу».

Под центром мониторинга и реагирования различные компании понимают разное, но суть на практике такова, что данные решения обладают весьма широким набором функций и характеристик, которые в совокупности дают нужный эффект, и недорогой продукт не может их заменить. Многие банки развивают собственные компетенции в направлении управления инцидентами, однако это процесс долгий и очень дорогой. Не все имеют на реализацию такой глобальной задачи собственные ресурсы. Собственный грамотный SOC на уровне лучших мировых практик могут позволить себе исключительно банки из ТОП-10. Подходит ли остальным уже упоминавшийся выше аутсорсинг? Безусловно. Сервис стоит недорого, а результат оправдывает ожидания.

Что еще?

Безопасность — разумеется, не основная область сотрудничества Softline с организациями финансового сектора. Поставку программного и аппаратного обеспечения также доверяют нам: наши специалисты снабжают бизнес любыми сетевыми компонентами, системами хранения данных, ПК, построят ЦОД. Поставки осуществимы и в экстра-крупных объемах: мы знаем, что банки используют и софт, и железо интенсивнее многих других компаний. ▮

НУЖНО ВСЕГДА!

Бизнес-аналитика и электронная экосистема

История подавляющего большинства финансовых организаций, как и банковской сферы в целом, пронизана консерватизмом. Банк — это нечто устойчивое и монолитное, и клиентская база у них должна быть стабильной и лояльной, и партнеры надежными. Во всей этой картине стабильности ярким пятном выделяется необходимость постоянных перемен, особенно технологических.

Традиционные каналы обслуживания все больше отходят на второй план: в крупных городах даже пенсионеры зачастую предпочитают воспользоваться банкоматом или интернет-банкингом, нежели идти в отделение. Непрерывно подгоняя друг друга в конкурентной борьбе, финансовые организации эволюционируют. Одновременно меняются и реалии рынка. Всего 5 лет назад в России мы наблюдали присутствие на рынке трех групп компаний: лидирующих, «средних» и догоняющих. Их количество значительно уменьшилось в последние годы, и теперь в игре либо крупные топовые банки, либо малоизвестные, которые по факту вряд ли являются соперниками для первых.

Что нового?

Тем не менее и небольшая финансовая структура может реализовать абсолютно прорывную бизнес-концепцию. Например, на основе таких технологий, как искусственный интеллект, анализ больших данных и их монетизация, а также роботизация процессов. В Softline понимают и наблюдают это каждый день, поэтому не так давно мы начали развивать направление защиты баз данных. Банковская Big Data уязвима, особенно, если изначаль-

но при ее создании к работе не привлекали специалистов по безопасности. Как грамотно построить системы, где большие данные будут обрабатываться и храниться, — одна из ключевых компетенций Softline.

Если активно подключать роботизацию в бизнес-процессы, нужные результаты можно получить в десять раз быстрее, чем без нее. То, что раньше удавалось сделать за год-два, с помощью автоматизации вполне реально реализовать за несколько недель. Интеллектуальные роботизированные механизмы сводят рутину на нет, умеют автоматически извлекать факты из документов, классифицировать контент, проводить экспертизу рисков и умный поиск.

Документооборот

В качестве примера давайте вкратце рассмотрим суть новейших систем электронного документооборота, которые имеют колоссальные возможности масштабирования и настройки сквозных процессов в распределенных корпорациях.

Тот, кто ранее на деле не сталкивался с преимуществами современных СЭД, не сразу может в них поверить. Система документооборота может выступать центром инфраструктуры обмена электронными документами, обеспечивая их хранение, интеграцию с сервисами межкорпоративного обмена и учетными системами. Только представьте себе полностью цифровое взаимодействие и объединение в единую экосистему сотрудников, процессы, контент, партнеров, контрагентов. Удобство для пользователей, интеллектуальная роботизация, набор подходящих бизнес-решений, мощная платформа, юридическая значимость, омниканальность — все это и есть современный электронный документооборот.

СЭД в финансовой организации может одинаково успешно функционировать в проектных, договорных и кадровых процессах, в закупках, делопроизводстве и управлении услугами, ведении финансового архива, а также в работе с межкорпоративными первичными учетными документами и многом другом.

BI как услуга? Отличный вариант

Бизнес-аналитика — инструмент, применимый в самых разных направлениях банковской деятельности. Например, при составлении оперативной отчетности, поскольку каждый день руководящему звену важно отслеживать, как идет бизнес и достигаются ли ключевые показатели. Предиктивная аналитика активно используется банками для определения вероятности дефолта индивидуальных и корпоративных заемщиков.

BI помогает минимизировать не только внешние, но и внутренние операционные риски. Например, за счет выявления мошеннических схем, придуманных недобросовестным персоналом.

Возможно ли поручить работу с бизнес-аналитикой штатным специалистам, закупив соответствующее программное обеспечение? Конечно но, если это дорого или долго, имеет смысл привлечь провайдера BI-услуг, например, Softline.

Поскольку банки предъявляют очень строгие требования к безопасности информации, провайдер будет получать для анализа только обезличенную информацию, чтобы все реализованные процессы оставались конфиденциальными.

Если ваша компания хочет воспользоваться бизнес-аналитикой как сервисом, то нужно будет только оплачивать ежемесячную подписку на него. Затрат на ПО и внутренних аналитиков не будет. В готовой услуге большая часть работы уже сделана интегратором: система создана и апробирована в деле, методология также готова — остается только уточнить формат получаемых данных конкретного банка и в рамках тестового периода работы конкретизировать специфические моменты.

Обратитесь в Softline!

Компании-интеграторы условно можно разделить на два типа. Первые — с глубокой, но ограниченной экспертизой. Вторые — широкоспециализированные, но более поверхностные. Глобальный охват ИТ-тематик и отличные компетенции за счет партнерства с вендорами позволяют Softline предлагать огромный спектр услуг «из одного окна». Даже очень сложную задачу можно решить, обратившись только к одному партнеру — Softline. Для финансовых организаций это дополнительная возможность аккумулировать свои усилия на активах, которые напрямую связаны с их деятельностью, и «не распыляться». ▮

БИЗНЕС-АНАЛИТИКА В ФИНАНСОВОЙ СФЕРЕ

Автор:
Станислав Воронин, руководитель направления внедрений систем бизнес-аналитики департамента бизнес-решений Softline

Важным трендом бизнес-аналитики в финансах является использование предиктивных технологий, позволяющих выявлять закономерности и тенденции в структурированных и неструктурированных данных. С их помощью можно прогнозировать поведение пользователей, оценивать благонадежность кредиторов, привлекать новых клиентов, создавать дополнительные продукты и оценивать их востребованность.

Система предиктивной аналитики тесно связана с Big Data и искусственным интеллектом. Она основана на машинном обучении.

Что это и как это выглядит?

Готовых, коробочных решений, в этой сфере не существует, поэтому практически любой банк, любая организация, связанная с финансами, имеет свой штат разработчиков или отдает задачи по созданию новых продуктов на аутсорсинг компаниям, которые профессионально этим занимаются.

В зависимости от того, что именно требуется заказчику, создается соответствующий программный продукт, как правило, использующий нейронные сети, то есть самообучающийся и самосовершенствующийся. Он собирает большое количество информации, обрабатывает ее, находит взаимосвязи, корректирует тактику и стратегию принятия решений.

Применение в финансовой сфере

Повышение эффективности работы с клиентской базой. В настоящее время все уже так или иначе пользуются услугами банков и страховых компаний, поэтому больший доход приносит переход клиентов из одного учреждения в другое (передел рынка), а также реализация новых дополнительных продуктов (создание виртуальных карт, предложения по вкладам и многое другое).

У каждого банка или страховой компании есть своя база клиентов, по которой периодически совершаются обзвоны. Решения предиктивной аналитики способны повысить эффективность этого процесса, выбрав только те номера телефонов, владельцы которых с большей вероятностью заинтересуются тем или иным предложением. Поскольку часто проводить обзвоны клиентов не рекомендуется, то возможность распределить предложения по целевым группам сильно повышает вероятность успеха.

Определение кредитоспособности клиентов. Актуально для банковской сферы. На основе анализа пола, возраста, полноты заполнения анкеты и других параметров продукт может принимать решение о возможности выдачи кредита, назначать проценты по нему, учитывая риски.

Определение степени риска наступления страхового случая. Программа определяет стоимость того или иного полиса, анализируя пол, возраст, профессию, частоту предыдущих обращений за страховыми выплатами, а также другие параметры.
Маркетинговый и клиентский анализ. Позволяет определять перспективные направления работы, создавать новые интересные продукты, анализируя поведение клиентов и их запросы. Для этого необходимо большое количество собранных данных, но выгоды от таких решений могут быть астрономическими.
Работа с персоналом. Этот пункт актуален для любой сферы. Он позволяет оценивать качество работы сотрудников, выявлять узкие места по каждому специалисту, а также сохранять ценные кадры, вовремя предлагая им повышение, перевод, программу повышения лояльности или курсы повышения квалификации.

Основные инструменты предиктивной аналитики

Azure Machine Learning, SAS, IBM SPSS, Loginom, R и Phyton.
Все эти продукты отличаются функциональностью и удобством. Некоторые из них позволяют создавать предиктивные модели, некоторые — интерпретировать их, а некоторые могут делать и то, и другое.
В зависимости от того, что именно требуется в каждом конкретном случае, выбирают свой инструмент. Важными являются следующие параметры.
Поддержка полного цикла аналитики. Насколько успешно инструмент умеет исследовать данные и создавать по ним модели, оценивая затем их эффективность.
Интеграция знаний и ее поддержка. Данные, полученные после проведения анализа, должны интегрироваться в другие сферы бизнеса. Также нужно умение получать данные из различных источников.
Удобство и «дружелюбный» интерфейс, понятный для разных типов пользователей.
Адаптивность и автономность. Умение работать при минимальном вмешательстве программистов и технических специалистов.

Softline к вашим услугам

Грамотных специалистов, способных работать с инструментами предиктивной аналитики, не так много на рынке и стоят они немало. Можно создать целый отдел разработки, но куда выгодней воспользоваться услугами сторонней компании, обладающей всей необходимой экспертизой и своим собственным штатом, потому что таким образом:

- Не нужно заниматься подбором кадров и поиском специалистов.
- Не нужно платить зарплату тогда, когда нет заданий и загрузки.
- Есть уверенность в конечном результате и сроках.

Компания Softline имеет свой собственный отдел разработки, укомплектованный специалистами высокого уровня, способными создавать продукты для решения любых задач, связанных с финансовой и любыми другими сферами.

Роботы оценивают риски

Для банка оценка рисков крайне важна. Любой риск — это реальная возможность недополучить доход или же потерять средства. Выдавая кредит, банк должен быть уверен, что перед ним платежеспособный человек. Сейчас для этого не нужно задавать тысячи вопросов — достаточно просто проанализировать поведение человека в социальных сетях.
Такая технология уже была внедрена в одном из крупнейших российских банков. Она позволяет составить психологический портрет личности и оценить его благонадежность, анализируя пять черт характера по социальным сетям: добросовестность, открытость, общительность, законопослушность, эмоциональная неустойчивость. Применяя эту методологию, банк уже получил $50 млн чистой прибыли.

ФИНАНСОВЫЕ УСЛУГИ.

ПРОГНОЗЫ FUJITSU НА 2019 ГОД

1. Активное внедрение публичных облачных сред в финансовом секторе. В условиях, когда почти 30% ИТ-директоров планируют уменьшить инвестиции в ИТ-инфраструктуры и центры обработки данных, облачные технологии становятся идеальным вариантом для замены аппаратного и программного обеспечения. Кроме того, теперь, когда финансовые организации последние два года занимались приведением своих облачных решений в соответствие с нормативными требованиями, внедрение публичных облачных сред наберет еще более высокие обороты в 2019 г. Банки среднего размера будут переходить на коллективные облачные решения, для которых не требуется наличие большого объема профессиональных знаний. Кроме того, поставщики облачных решений во главе с AWS, Microsoft и Oracle предложат заказчикам новые функциональные возможности PaaS в дополнение к новым IaaS-платформам, что позволит банкам начать разрабатывать собственные облачные приложения.

2. Новые подходы, новые процессы. Банки приступят к оценке и внедрению новых походов на базе облачных технологий, которые позволят им отказаться от использования дорогих морально устаревших сред. Для этого они будут внедрять динамичные методики разработки программного обеспечения, что в свою очередь будет стимулировать последовательное развертывание программного обеспечения на базе мультиоблачных решений.

3. Нехватка квалифицированных специалистов будет усиливаться. По мере увеличения востребованности ключевых профессиональных ИТ-знаний, финансовые компании столкнутся с трудностями в привлечении и удержании квалифицированных ИТ-специалистов в области искусственного интеллекта, облачных технологий и технологии блокчейн. В результате, компании приступят к пересмотру своих корпоративных стратегий в области найма и профессионального обучения персонала, однако на данном этапе это приведет к снижению темпов работы и внедрения инновации.

4. Прорыв области технологии блокчейн. В 2019 г. блокчейн найдет практическое применение по мере того, как криптовалюты и решения на базе распределенного реестра выйдут на новый уровень развития. В следующем году мы станем свидетелями большого количества опытных проектов и пилотных испытаний в таких областях, как межбанковские операции, M2M-платежи и электронные кошельки.

5. Начало трансформации индустрии страхования. В этой области мы сможем наблюдать целый ряд интересных проектов на основе Интернета вещей, в рамках которых будут внедряться перспективные сценарии использования современных цифровых технологий для снижения рисков и повышения прибыльности. Однако в банковской сфере компании столкнутся с проблемами, связанными с низкой эффективностью использования технологий на основе Интернета вещей.

6. Повышение открытости. Клиенты банков хотят воспользоваться более удобными и эффективными банковскими услугами, поэтому в следующем году мы будем наблюдать развитие информационно прозрачного банковского обслуживания. И хотя эта тенденция открывает новые возможности для отдельных финансовых организаций, многие банки столкнутся со сложностями начального периода по мере того, как они будут пытаться выделиться в новых межотраслевых экосистемах. Тенденция по увеличению открытости затронет и индустрию страхования — отдельные компании начнут переход к концепции открытого страхования, подразумевающей активный обмен информацией с другими участниками различных экосистем.

Паскаль Хейберс (Pascal Huijbers), технический директор в сфере финансовых услуг компании Fujitsu в регионе EMEIA

FUJITSU

СТАНДАРТНЫЙ ВОПРОС

Приводим ИБ-инфраструктуру в соответствие с новым ГОСТ

Страховые компании и НПФ активно начали приводить ИБ-инфраструктуру в соответствие с требованием ГОСТ Р 57580.1–2017. Если еще в начале 2019 года такие проекты были единичными, то за период с апреля по июль в работе у Softline появились уже десятки запросов. Самыми активными оказались страховые компании — от них поступает порядка 50% от всех заявок на проведение аудита.

Новый стандарт

ГОСТ Р 57580.1–2017 — это новый стандарт информационной безопасности для кредитно-финансового сектора, который вступил в силу с 1 января 2018 года. В соответствии с требованиями документа в область оценки соответствия защиты информации входит совокупность фактически всех объектов информатизации финансовых организаций, включая автоматизированные средства и приложения, используемые для выполнения процессов, связанных с предоставлением финансовых и банковских услуг, а также услуг по осуществлению переводов денежных средств.

Кого касается?

Само по себе появление ГОСТ не вызвало ажиотажа, так как он носит рекомендательный характер и не содержит указаний, кому и когда применять рекомендации. Обязанность по его выполнению появилась лишь в апреле текущего года с выходом Положений Центробанка 684-п для некредитных и 683-п –для кредитных организаций.

Согласно Положению 684-п, под действие ГОСТа попадают страховые компании, негосударственные пенсионные фонды, инвестиционные фонды, участники рынка ценных бумаг и другие некредитные организации. Обязательства по внедрению стандартов пока отсутствуют для небольших организаций: страховых компаний с суммой активов до 20 млрд руб., НПФ с суммой пенсионных резервов до 10 млрд и так далее.

Оценки, сроки и санкции

Реализация проекта по приведению ИБ-инфраструктуры в соответствие с требованиями нового ГОСТа включает в себя несколько этапов: обследование и анализ существующей инфраструктуры и получение оценки уровня соответствия требованиям ГОСТ от 0,5 до 1, а также дальнейший подбор и внедрение необходимых средств защиты. К июлю 2023 года все некредитные финансовые организации должны иметь уровень оценки не ниже 0,85. В документах прописаны и сроки сдачи отчетов в ЦБ о внедрении нового стандарта — в большинстве случаев крайним сроком является 1 января 2021 года. Нарушителям могут грозить серьезные санкции со стороны Центробанка вплоть до отзыва лицензии.

Если банки как представители одной из самых зарегулированных отраслей экономики уже давно начали готовиться к появлению нового стандарта информационной безопасности, то для большинства некредитных организаций его появление оказалось неожиданным. Первыми озаботились приведением ИТ-инфраструктуры в соответствие с новыми требованиями регуляторов страховые организации — на данный момент в проработке у Softline порядка 10 таких проектов. Есть активность со стороны НПФ. Пока большая часть запросов поступает от компаний ЦФО — другие регионы не так активны.

Пора начинать!

Усиление интереса к услугам аудита и консалтинга в области соответствия ГОСТ Р 57580.1–2017 ожидается в 2020 году — большинству компаний необходимо провести подготовительные работы для проведения аудита и консалтинга, а также запланировать бюджет. Не стоит откладывать работы на конец следующего года, так как ГОСТ содержит довольно много требований. Проведение аудита, как правило, занимает от двух месяцев до шести, еще несколько месяцев уйдет на подбор, поставку и внедрение средств защиты.

Сэкономить время и средства, потраченные на реализацию проекта по внедрению стандартов нового ГОСТа можно, если привлечь опытного ИТ-провайдера уже на начальном этапе реализации проекта. Эксперты Softline внимательно следят за изменениями в финансовой сфере. Благодаря накопленной экспертизе мы помогаем заказчикам оптимально распределить бюджет и подобрать средства защиты, а также оформить всю необходимую документацию к началу проверок со стороны регуляторов.

Остались вопросы?

Задайте их автору статьи — эксперту департамента информационной безопасности группы компаний Softline Илье Тихонову.
Пишите: Ilya.Tikhonov@softline.com
Звоните: +7 (495) 232-00-23 доб. 1153

FRAUD DETECTION SYSTEM

Сервис по противодействию финансовому мошенничеству

Как отслеживать преступные действия в системах дистанционного банковского обслуживания? С помощью системы Fraud Detection System (FDS) — решения, предназначенного для онлайн-обнаружения мошенничества в процессе удаленного банковского обслуживания.

Повышенный уровень безопасности достигается путем автоматической проверки платежа на соответствие заданным правилам и типовой модели поведения клиента в системах ДБО. Разработчик — компания «Инфосекьюрити».

Возможности FDS

Масштабируемое решение позволяет эффективно бороться с более чем 99% случаев фрода. Возможна установка «в разрыв», когда ни один платеж не может быть проведен до момента обработки антифрод-системой. Все действия операторов сохраняются, есть веб-доступ для работников филиалов. Система демонстрирует высокую скорость обработки данных, доступна интеграция с любой АБС и СДБО. Качественная управленческая отчетность, полная статистика по работе системы и возможность разработки собственных правил вычисления оценки — в списке дополнительных преимуществ.

В разработке «Инфосекьюрити» применен элемент искусственного интеллекта, который определяет вероятных мошенников по пользовательскому поведению.

Сервис и сопровождение для банка

01 июня 2018 г. «Инфосекьюрити» запустила решение FDS по сервисной модели в коммерческом банке «Пойдём!», который насчитывает более 218 офисов в 120 городах России, более 2 тыс. сотрудников и свыше 1 млн клиентов.

В рамках сервиса обеспечивается мониторинг транзакций в платежных системах заказчика, а также обучение операторов и предоставление рекомендации по внедрению процессов реагирования на инциденты.

С начала эксплуатации решения банком «Пойдем!» число эпизодов, связанных с попыткой фрода, уменьшилось более чем на 90%. В пакет сопровождения входит все необходимое для обеспечения технической работоспособности серверной инфраструктуры с FDS, а также компоненты превентивной защиты: отслеживание и фиксирование всех действий операторов системы, аналитические отчеты, рекомендации по модернизации инфраструктуры. Возможность доработки и модификации правил и регламентов поиска потенциального фрода является важным преимуществом, позволяющим своевременно реагировать на новые разработки мошенников.

Спустя год использования

Прошел год, и банк продлил подписку на Fraud Detection System. Специалисты «Инфосекьюрити» продолжат оказывать сервис в режиме 24/7/365. Помимо FDS «Инфосекьюрити» взяла на себя мониторинг и профилирование других типов киберинцидентов. За год компания осуществила интеграцию FDS с установленной в банке системой OpenWay:Way4, предоставила комплект пользовательской и эксплуатационной документации и базу знаний по использованию решения. Благодаря этому ИБ-специалисты банка теперь могут моментально изменять или добавлять источники событий, которые должна фиксировать FDS.

Пойдём! Первый Добрый Банк

«Нам было важно, чтобы вендор самостоятельно осуществлял поддержку своего решения. С «Инфосекьюрити» мы работаем по принципу одного окна: компания объединяет в себе статус вендора, сервис-провайдера и ИТ-консультанта. Фильтры и критерии анализа и поиска мошеннических транзакций будут дорабатываться для защиты наших клиентов и в соответствие с новым указанием Банка России №4753-У «Об инцидентах, связанных с киберхищением средств».

Дмитрий Смирнов,
начальник управления
информационной безопасности
КБ «Пойдём!»

Об «Инфосекьюрити»

INFOSECURITY

«Инфосекьюрити» — специализированный сервис-провайдер, оказывающий услуги в сфере информационной безопасности, системной интеграции и консалтинга. Компания является лицензиатом ФСБ России и ФСТЭК России; ее бизнес-процессы построены в соответствии с международными практиками и стандартами.

Ключевые сервисы «Инфосекьюрити» — реагирование на инциденты информационной безопасности (Security Operations Center), предотвращение утечки данных, защита от угроз нулевого дня, поддержка IT-инфраструктуры. Компания успешно внедряет и сопровождает системы защиты информации в различных отраслях — финансы, промышленность, государственный сектор, медицина и др. В состав «Инфосекьюрити» входит Лаборатория компьютерной криминалистики, специалисты которой участвуют в раскрытии киберпреступлений, проводят тесты на проникновение и исследования различных цифровых объектов.

Кроме того, «Инфосекьюрити» развивает собственные решения по информационной безопасности. В их число входит система мониторинга и автоматизации реагирования на инциденты.

Подробнее — на gk-is.ru.

Внедрение Office 365 для Национального банка Республики Беларусь

В результате внедрения Office 365 сотрудники Национального банка РБ получили современные инструменты для оперативной и комфортной работы с документами, что позволило повысить эффективность бизнес-процессов и сократить затраты на ПО.

Ситуация

Использование различных версий офисных приложений, файлового хранилища, отсутствие инструментов для совместной работы над документами вызывало трудности при взаимодействии между сотрудниками.

Руководство Национального банка РБ приняло решение внедрить единое средство для быстрой и надежной корпоративной коммуникации — пакет офисных инструментов Office 365.

После проведенного анализа процессов коммуникации сотрудников, аудита текущей системы совместной работы, были сформированы основные задачи, которые должны были решить инструменты Office 365:

- снижение затрат на техподдержку;
- повышение уровня интеграции с другими системами Microsoft;
- повышение уровня безопасности доступа;
- обеспечение расширенного аудита действий администраторов и пользователей;
- возможность контроля как за передачей информации, так и за её хранением;
- снижение издержек на поддержку инфраструктуры, аппаратного и программного обеспечения.

Заказчику требовалось обеспечить своих сотрудников инструментами для совместной работы и получить обновленные офисные приложения. Настроить ИТ-сервисы было необходимо в соответствии с требованиями корпоративной системы безопасности.

Для анализа текущей ситуации использования ПО Microsoft, специалистами Softline был проведен SAM-проект, по результатам которого заказчик получил подробные рекомендации по решению поставленной задачи и экономическое обоснование использования облачных сервисов.

Решение

После обследования IT-инфраструктуры Национального банка специалисты Softline предложили заказчику перейти к использованию Microsoft Office 365. Решение включает актуальную версию локальных приложений

НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ

О заказчике

Национальный банк Республики Беларусь — центральный банк и государственный орган Республики Беларусь, обеспечивает стабильность банковской системы в Беларуси и надежное функционирование платежной системы.

Office (все обновления включены в стоимость подписки), а также единый центр администрирования.
За счет подключения до 15 пользовательских устройств по одной подписке Office 365 позволяет снизить затраты на дополнительное ПО. Передовые меры безопасности решения помогают обезопасить данные сотрудников и защитить необходимые файлы.
Проект был реализован в соответствии со стандартами безопасности Национального банка РБ. По завершении настройки процессов специалистами Softline было проведено обучение ИТ-персонала заказчика по вопросам использования сервисов и их технической поддержке.
Для руководителей и сотрудников заказчика был проведен тренинг по работе с новыми приложениями Office 365 и показаны основные сценарии их использования.

Результаты

Сотрудники Национального банка РБ получили удобные инструменты для эффективной командной работы, с помощью которых они всегда могут оставаться на связи и оперативно решать задачи.
Внедрение Office 365 позволило Национальному банку РБ повысить эффективность бизнес-процессов и сократить затраты на ПО. Дальнейшими шагами по оптимизации затрат на приобретение/продление прав на лицензионное ПО станет проект внедрения систем учета лицензий (SAM).

Новый ЦОД
для ЗАО «Америабанк»

Ситуация

В связи с переездом в новое здание для быстрой и надежной работы всех сервисов банку потребовалось создать технологичный масштабируемый центр обработки данных, соответствующий высоким требованиям безопасности и отказоустойчивости.
По результатам конкурса, в качестве партнера проекта была выбрана компания Softline, обладающая всеми необходимыми компетенциями и опытом построения подобных объектов.

Решение

Перед специалистами Softline стояла задача спроектировать инженерные системы будущего ЦОДа и реализовать весь комплекс строительных и монтажных работ. Первый этап — проектирование — был выполнен инженерами Softline в кратчайшие сроки, и после согласования с заказчиком всех технических решений компания приступила к строительству, которое было завершено в декабре 2017 года.
В новом здании банка установлены и смонтированы все необходимые инженерные системы, соответствующие Европейским стандартам ISO в области пожарной безопасности и требованиям к уровню надежности Tier 3.
«Мы давно сотрудничаем с Америабанком по разным направлениям и для нас большая честь и ответственность реализовать такой масштабный и технологичный проект в Армении. Благодаря опыту совместной работы специалистов Softline и Америабанк проект был реализован в заданные сроки на высоком профессиональном уровне», — рассказывает директор по продажам Softline Армения Карине Егоян.

Результаты

По результатам проекта в активах Америабанк появился масштабируемый и технологически оснащенный ЦОД, который сможет обеспечить устойчивую и эффективную работу всех служб банка. ∎

О заказчике

ЗАО «Америабанк» — универсальный банк, предлагающий корпоративные, розничные и инвестиционные услуги в комплексном пакете.

«Наши ожидания оправдались — новая инженерная инфраструктура ЦОД ЗАО «Америабанк» полностью отвечает текущим требованиям и рассчитана на долгосрочное развитие, имея необходимый резерв. Специалисты Softline продемонстрировали высокий профессиональный уровень знаний и умений, способность реализовывать проекты высокого уровня сложности».

Шаварш Восканян,
руководитель Управления ИТ и автоматизации Америабанка

Проект Softline по строительству ЦОДа в Армении вошел в число призеров премии Global CIO

Среди победителей конкурса «Проект года 2018», организованного официальным порталом ИТ-директоров Global CIO — компания Softline. Призмы взяли в номинации «Лучшее решение в области построения ЦОД» за реализацию проекта по созданию нового дата-центра для «Америабанка».

Вендор Schneider Electric отметил наградой первую продажу комплексного решения с использованием LI-ION в СНГЦеремония награждения состоялась 28 февраля в рамках «Партнерского дня—2018», где вендор подводит итоги года.

Сервисы G Suite и лэптопы Chromebook для Forex Club

Все, что необходимо для эффективной совместной работы специалистов!

Ситуация

Территориально распределенной компании нужно было обеспечить быструю и комфортную командную работу специалистов. Кроме того, требовалось оптимизировать поддержку почтовых серверов, систем автоматического обновления драйверов, снизить стоимость управления программными активами.

Решение

Обобщив информацию, полученную из разных отраслевых источников и благодаря экспертизе специалистов Softline, ИТ-команда компании выбрала G Suite. Облачное решение не требовало закупки аппаратного обеспечения и значительных расходов на поддержку.

Первоначально G Suite развернули только для ИТ-департамента. После этого решение распространили на часть сотрудников Forex Club. Они первыми стали работать в новой среде и постепенно обучать коллег. Чтобы снабдить их необходимыми знаниями, заказчик при помощи команды Softline организовал 15 онлайн-тренингов. Далее каждый департамент самостоятельно мигрировал на G Suite. Следующим шагом для Forex Club стал тест ноутбуков Chromebook для повседневной работы сотрудников. Устройства работают на операционной системе Chrome OS, а программы на них установлены в виде веб-сервисов. Это позволяет оперативно разворачивать рабочие места, обеспечивать безопасность данных и их высокую сохранность, чтобы ни случилось с оборудованием.

Результат

Персоналу компании Forex Club доступны сервисы для совместной работы в режиме 24/7. В их числе — синхронизируемые календари, корпоративный чат в Hangouts с возможностью видеоконференцсвязи, облачное хранилище большого объема, Google Forms для проведения опросов, заметки Google Keep для постановки операционных задач. DevOps команда компании может управлять сервисами удаленно при помощи мобильных устройств. А чтобы организовать рабочее место, персоналу достаточно учетной записи и доступа в интернет. Финансовый департамент, ИТ и HR активно используют инструменты совместной работы с документами. Заказчик планирует планомерно расширять парк Chrome-оборудования.

ForexClub

О заказчике

Группа компаний Forex Club — известный международный бренд на рынке онлайн-трейдинга, который с 1997 года помогает трейдерам зарабатывать на финансовых рынках. В группе компаний более 700 специалистов, которые обслуживают более 2,2 млн клиентов по всему миру.

«Миграция на G Suite позволила нам отказаться от громоздкой и сложной инфраструктуры и ее поддержки, по сути мы сократили капитальные расходы. В результате перехода на облачный сервис удалось существенно улучшить совместную работу персонала, увеличить скорость принятия управленческих решений, обеспечить удобный доступ к информации в любое время и с любого устройства».

Дмитрий Островерхов,
руководитель группы поддержки
и административного отдела Forex Club

Модернизация сетевой инфраструктуры Банка ВТБ (Беларусь)

Развертывание платформы виртуализации позволило банку повысить безопасность и эффективность бизнес-процессов, снизить операционные затрат на обслуживание сети.

Ситуация

С развитием бизнеса и расширением спектра оказываемых услуг у Банка ВТБ появилась потребность в новом подходе к организации корпоративных сетей. Возникла необходимость быстрого развертывания новых сервисов и безопасной организации новых сегментов сети.

На конкурсной основе в качестве партнера была выбрана компания Softline. Эксперты компании помогли сделать сравнение и продемонстрировали лучшие решения на рынке в этой области. После анализа существующих технических решений, банк остановился на платформе виртуализации сети VMware NSX. Решение лучше всех отвечало поставленным требованиям.

Выбираемая технология сегментирования должна была решить задачи по организации сетевой инфраструктуры банка:

- сегментации сети;
- построению уровня абстракции от аппаратных сетевых решений;
- повышению уровня безопасности при создании новых виртуальных сетей;
- защите инвестиций за счет внедрения долгосрочного решения.

После определения основных задач эксперты Банка при поддержке Softline и VMware начали поэтапное внедрение NSX.

Решение

VMware NSX — платформа виртуализации сети нового уровня. Решение позволяет полностью воспроизвести физическую сеть программным методом без привязки к оборудованию.

Продукт был успешно развернут в ЦОДах Банка ВТБ. Управление происходит из единой консоли VMware, что сокращает время и упрощает процесс администрирования.

Для сотрудников банка был проведен тренинг по работе с новой платформой. Эксперты Softline обучили инженеров управлению системой, интеграции NSX с другими решениями, устранению неисправностей. А также оказали экспертную поддержку при настройке технологии на начальных этапах. Поддержка осуществлялась на высоком профессиональном уровне и практически круглосуточно. Возникающие проблемы оперативно устранялись в том числе с прямой поддержкой экспертов вендора.

Результат

Платформа NSX позволила сотрудникам банка:

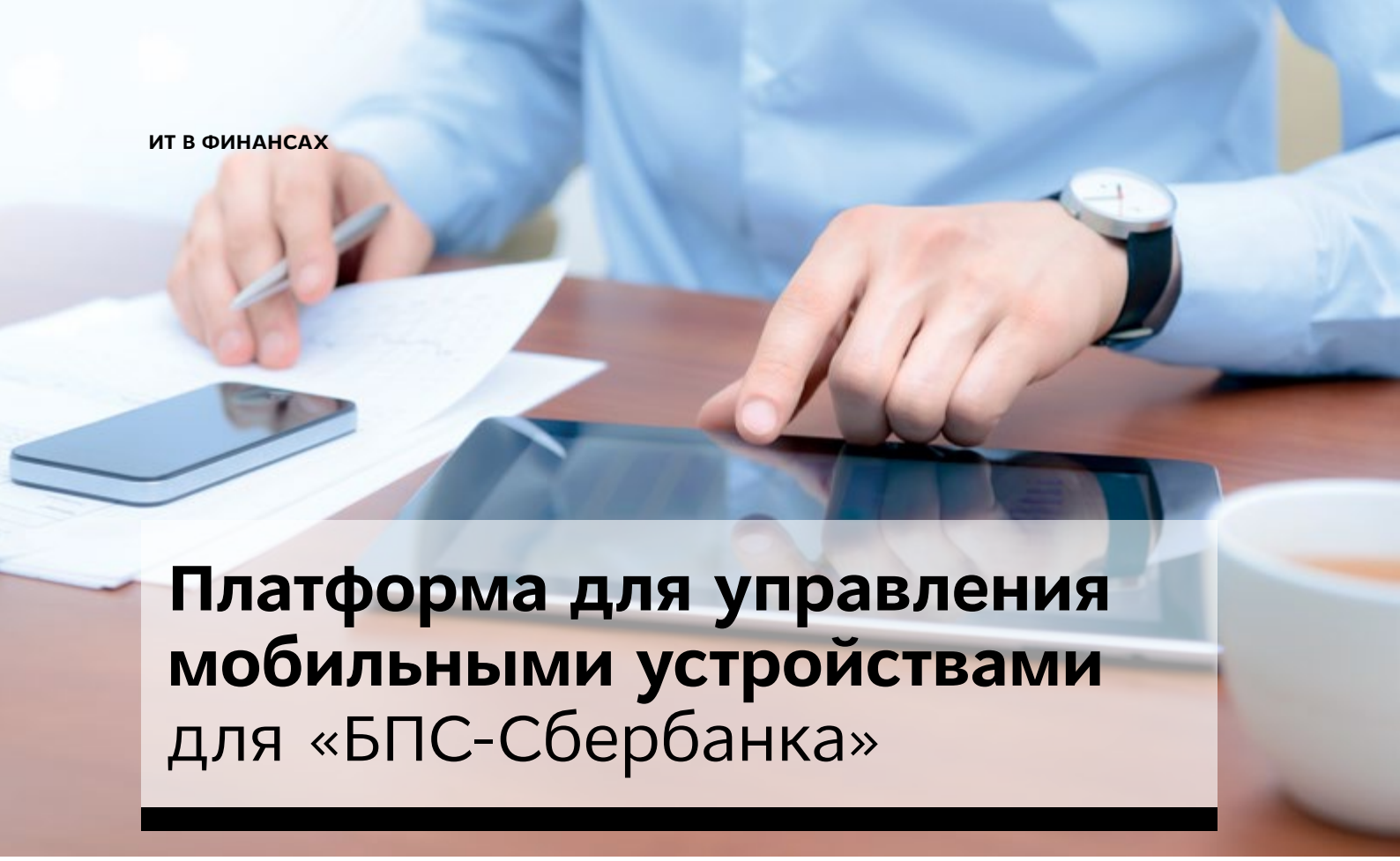
- получить гибкие политики безопасности, динамичность, улучшенную систему безопасности;
- сократить время развертывания новых сервисов с нескольких дней до нескольких минут;
- переносить рабочие нагрузки между ЦОД и внутри них с сохранением сетевой инфраструктуры.

О заказчике

Банк ВТБ (Беларусь) работает на рынке Беларуси с 1996 года и стабильно входит в десятку крупнейших банков в стране. Банк принадлежит к международной финансовой группе и решает задачи клиентов любого уровня сложности, обеспечивает финансирование крупных проектов, предоставляет индивидуальные тарифы корпоративным клиентам.

«Основным результатом проекта для Банка ВТБ стало внедрение нового подхода к организации корпоративных сетей. Благодаря платформе NSX мы можем быстро и безопасно разворачивать новые сервисы без покупки дополнительного оборудования и трудозатрат на его настройку».

Ю. Казак, директор Департамента банковских и информационных технологий Банка ВТБ



Платформа для управления мобильными устройствами для «БПС-Сбербанка»

Компания Softline Беларусь внедрила единую платформу для управления мобильными устройствами для «БПС-Сбербанка». Решение было построено на базе продукта VMware Workspace ONE. В настоящее время в эксплуатацию введено более 500 мобильных устройств.

Ситуация

Развитие инфраструктуры и расширение сервисов обусловили потребность во внедрении мобильной платформы для оптимизации работы сотрудников, привлечения новых клиентов, развертывания необходимых сервисов. Появилась потребность в централизованном управлении всеми мобильными устройствами, обеспечении удаленного доступа к корпоративной среде с выполнением всех требований службы безопасности. В качестве партнера была выбрана компания Softline, специалисты которой обладают необходимым опытом и подтвержденными компетенциями в области систем управления мобильными устройствами (MDM).

Одним из требований к MDM-системе была возможность развертывания всей инфраструктуры в ЦОД заказчика без привязки к облачным сервисам, а также наличие встроенных ресурсов для обеспечения безопасного доступа к корпоративной среде и базовый DLP-функционал. В рамках проекта предполагалось задействовать внутри предприятия более 500 мобильных устройств на платформах iOS и Android.

С помощью MDM-системы необходимо было организовать безопасный доступ с мобильных устройств к следующим системам банка:

- электронная почта;
- CRM-система;
- демонстрационные версии мобильных приложений для клиентов;
- система видеоконференций;
- внутренний портал банка;
- система Help Desk.

Кроме того, необходимо было обеспечить полную интеграцию с каталогом Active Directory и централизованное управление правами доступа к мобильным ресурсам через группы безопасности домена.

Решение

В ходе проекта было проведено комплексное сравнение и анализ всех решений MDM по управлению мобильной инфраструктурой. Проанализировано большое количество платформ по разным критериям: возможность развертывания инфраструктуры «на земле» (on-premise); управление приложениями; обеспечение безопасности; предотвращение утечек информации; поддержка различных устройств и операционных систем; стоимость решения. По итогам анализа оптимальным было признано решение VMware Workspace ONE, которое отвечало всем требованиям. Наиболее важным фактором, повлиявшим на итоговый выбор, была возможность реализации продукта on-premises. Это было ключевым требованием банка к платформе. Компания Softline предоставила возможность протестировать решение, после чего был запущен пилотный проект с внедрением в инфраструктуру банка.

Для реализации пилотного проекта был использован демонстрационный облачный сервис VMware TestDrive, где создали пилотную среду, к которой предоставили доступ сотрудникам предприятия. Был определен набор устройств, приложений и сервисов. Инженеры «СофтЛайнБел» совместно с техническими специалистами «БПС-Сбербанка» провели развертывание необходимых сервисов в тестовой зоне дата-центра банка для интеграции с облаком. В первую очередь таким образом испытывались возможности централизованного управления профилями безопасности и приложениями на мобильных устройствах.

Следующим этапом была проверка работоспособности полного набора всех необходимых приложений и веб-сервисов под управлением MDM-системы. После успешного завершения этапа технические специалисты приступили к планированию развертывания полноценного решения в рабочей среде «БПС-Сбербанка». Была выбрана необходимая архитектура продукта, определены и выделены ресурсы для развертывания VMware Workspace ONE. После приобретения лицензий было произведено развертывание инфраструктуры VMware Workspace ONE в дата-центре банка и перенос всех разработанных политик, профилей и конфигураций из облачного сервиса VMware TestDrive на подготовленную рабочую среду.

Результат

В рамках реализации проекта «БПС-Сбербанк» получил MDM-систему Workspace ONE — платформу цифровой рабочей области, обеспечивающую удобное и безопасное предоставление любых приложений и управление ими на любом устройстве. Она поддерживает развертывание в локальной среде, отвечающей всем заявленным требованиям.

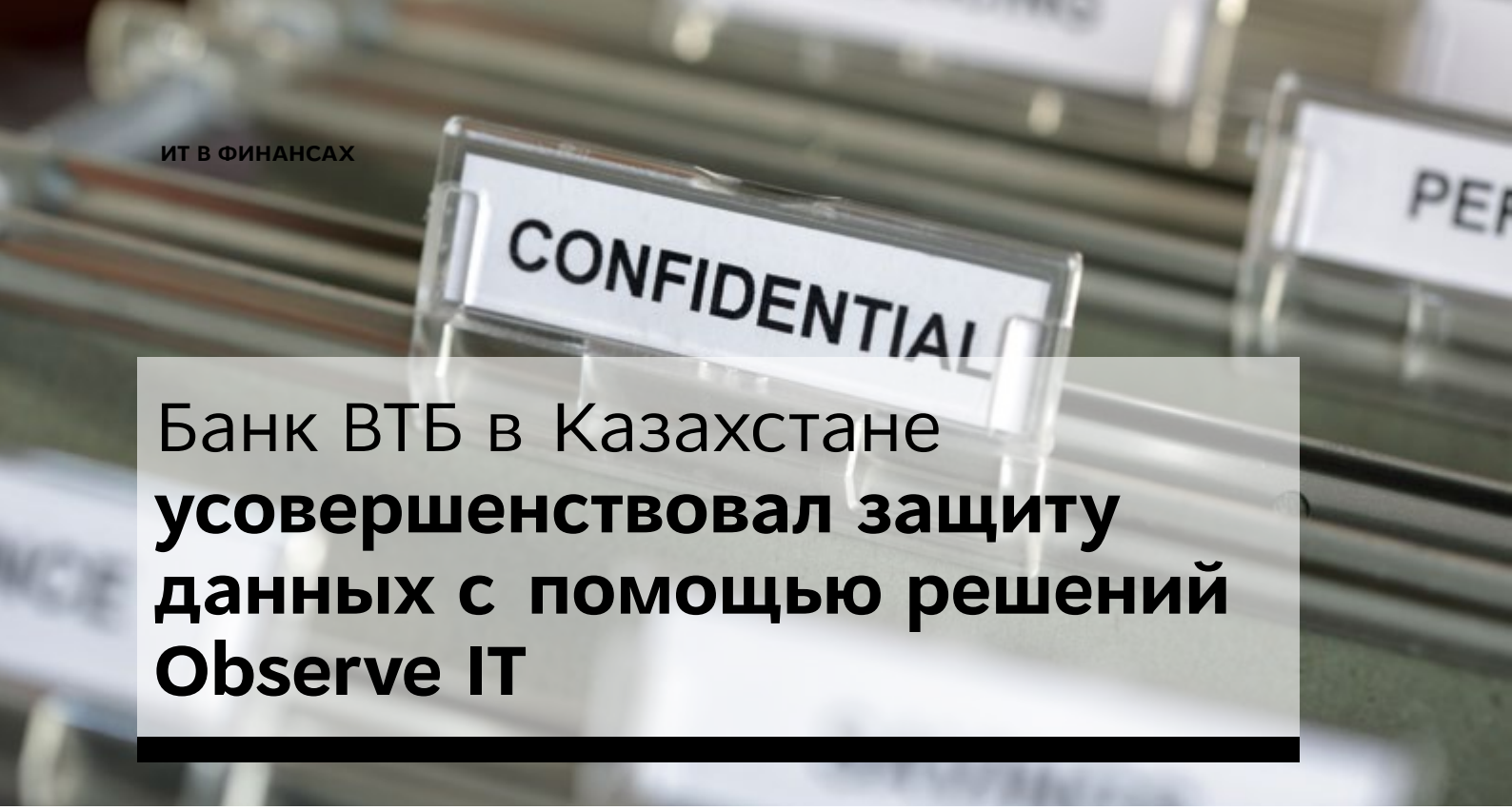
У «БПС-Сбербанка» появилась единая платформа для управления мобильными устройствами независимо от модели владения (в том числе в случае использования личных устройств в полностью управляемой инфраструктуре) и обеспечения конфиденциальности данных предприятия и сотрудников.

Было введено в эксплуатацию более 500 мобильных устройств. Все это позволило «БПС-Сбербанку» оптимизировать внутренние бизнес-процессы, модернизировать рабочую среду путем внедрения современной безопасной мобильной инфраструктуры и перейти на существенно новый уровень цифрового рабочего пространства.

БПС-СБЕРБАНК

О заказчике

ОАО «БПС-Сбербанк» входит в группу Сбербанка России. Это один из самых крупных банков Беларуси. Обслуживая счета предприятий и предпринимателей, банк предоставляет разнообразные услуги в области финансирования, кредитования, депозитов и прочего. В числе его клиентов значатся крупнейшие предприятия всех отраслей белорусской экономики. Филиалы и подразделения банка имеются во всех регионах Белоруссии.



Банк ВТБ в Казахстане **усовершенствовал защиту данных с помощью решений Observe IT**

Компания Softline Казахстан внедрила в банке ВТБ решение для аудита кибербезопасности и мониторинга активности привилегированных пользователей. Заказчик получил решение задачи по анализу, выявлению и предотвращению неправомерных действий при работе с критичными информационными системами.

Ситуация

В банке ВТБ хранятся большие массивы конфиденциальной финансовой информации и клиентских данных, которым необходимо обеспечить надежную защиту, согласно требованиям по регулированию финансового рынка в Казахстане. Поэтому руководство банка приняло решение внедрить решение для предотвращения инцидентов кибербезопасности и ошибок, в том числе обусловленных человеческим фактором.

Решение

Совместно с управлением информационной безопасности банка и ведущими производителями решений по защите информации специалисты Softline провели ряд пилотных проектов, подготовив аналитические данные по каждому продукту. Исходя из них, клиент выбрал оптимальное для него решение — Observe IT.

Программное обеспечение Observe IT предназначено для мониторинга активности пользователей с видеозаписью, логированием их действий в корпоративной системе, поведенческим анализом и поддержкой политик безопасности.

Результат

Команда Softline внедрила, настроила и интегрировала в инфраструктуру банка решение Observe IT, соблюдая указанные заказчиком сроки. Плодотворное сотрудничество со специалистами ВТБ позволило найти изящные решения нетривиальных задач.

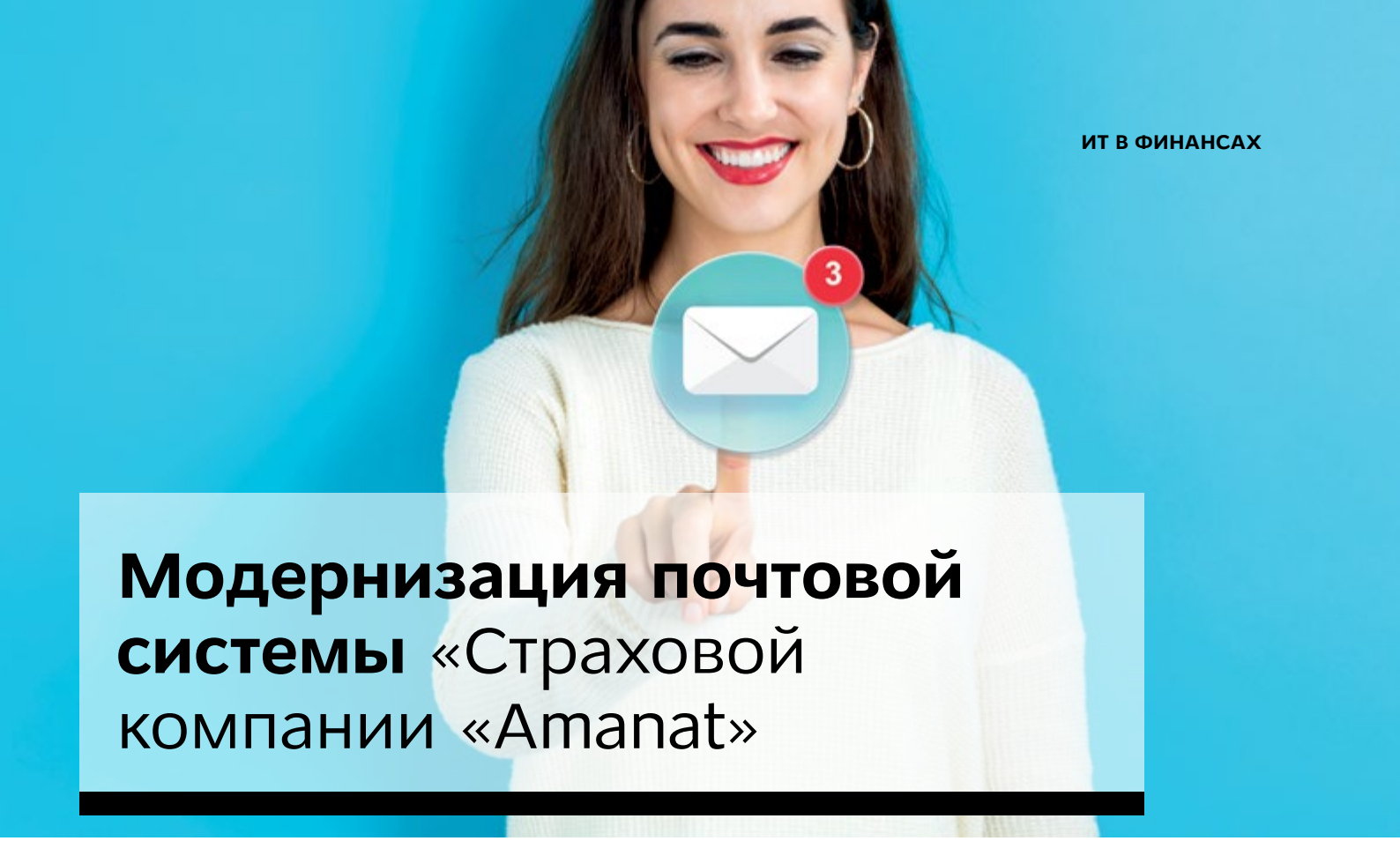
VTB

О заказчике

Банк ВТБ (Казахстан) оказывает услуги юридическим и физическим лицам, делая основной акцент на работе с корпоративными клиентами и малым и средним бизнесом. Цель Банка — предоставлять продукты и услуги европейского уровня, оперативно реагируя на потребности своих клиентов.

«Благодаря Observe IT у нас появилась возможность детально анализировать инциденты кибербезопасности. Получая все необходимые данные, мы легко находим информацию о произошедших инцидентах, разбираем эти кейсы вместе с персоналом, что повышает уровень ответственности сотрудников банка»

Петр Дудкин, главный специалист отдела защиты информации и сетевых технологий ДО АО «Банк ВТБ (Казахстан)»



Модернизация почтовой системы «Страховой компании «Amanat»

Компания Softline помогла «Страховой компании «Amanat» осуществить миграцию корпоративной почты на новую версию Microsoft Exchange Server. Реализация проекта позволила сократить трудозатраты на её обслуживание и повысить качество коммуникаций сотрудников.

Ситуация

Перед руководством компании стояла задача повышения функциональных возможностей почтовой системы и качественного уровня коммуникаций сотрудников. Для этих целей решено было осуществить переход с Microsoft Exchange Server 2007 на современную версию Exchange, поскольку она в наибольшей степени соответствовала требованиям. В частности, решение отличалось простотой поддержки, оптимальной стоимостью и возможностями кастомизации.

Решение

Реализация проекта заняла меньше месяца, в течение которого специалисты Softline разработали оптимальный план миграции, установили Exchange Server, осуществили переход и необходимые настройки системы.

Результат

Новое почтовое решение позволяет защитить деловые коммуникации и конфиденциальные данные компании, обеспечивая соответствие как внутренним правилам, так и требованиям регулирующих органов. Решение обеспечивает возможность работать с корпоративной электронной почтой, календарем и контактами через браузер, на телефоне или ПК. Упрощенный подход к обеспечению высокой доступности и аварийному восстановлению позволяет выйти на новый уровень надежности, гарантируя безопасность конфиденциальных данных.

О заказчике

АО «Страховая Компания «Amanat» является одной из крупнейших страховых компаний Казахстана и представлена обширной региональной сетью. На данный момент успешно работают 17 филиалов и 100 офисов во всех крупных городах страны.

«Главное преимущество данного решения в возможности повышать производительность пользователей: теперь они смогут решать большое количество задач, на любом устройстве, справляясь с растущими объемами сообщений электронной почты и более эффективно работая в команде».

Денис Березовский, управляющий директор по информационным технологиям АО «Страховая компания «Amanat»

БИЗНЕС ГОТОВ К ВСТРЕЧЕ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Сфера документооборота стремительно меняется. Если еще недавно создание электронных архивов казалось революционным прорывом, то сегодня системы ECM внедрены в большинстве крупных компаний и все чаще появляются в компаниях сектора SMB и технологических стартапах. Теперь у бизнеса есть возможность перейти на новый этап и создать полную цифровую экосистему, в которой все процессы обмена информацией связаны между собой и управляются искусственным интеллектом.

Что может интеллектуальная система

Цифровая экосистема построена на полностью электронном взаимодействии. В ее основе лежит платформа, которая объединяет данные из всех бизнес-приложений, даже если они не интегрированы между собой. Таким образом, вся открытая информация доступна для ознакомления в любой момент времени. Система должна поддерживать юридически значимый документооборот, быть интеллектуальной, удобной, функциональной и омниканальной, когда сотрудники имеют доступ к информации не только внутри ECM, но и через мобильные приложения, чат-боты и корпоративные порталы.

Руководитель направления внедрений СЭД/ECM департамента бизнес-решений ГК Softline Полина Дуйкова

Внедрение автоматизированной системы в области юридически значимого документооборота значительно упрощает процесс общения с контрагентами. Современные компании обмениваются тысячами договоров, актов, товарных накладных, счетов-фактур. Работа с документами, поступающими в компанию, начинается с первичной обработки и регистрации. Интеллектуальная ECM исключает ручные операции на этом этапе и автоматически (на основе обученной модели) распределяет входящий поток по видам документов, журналам регистрации и ответственным. Информация извлекается из бумажных и цифровых документов, обрабатывается и при необходимости автоматически сверяется с оригиналом, что важно, например, при взаимодействии с внешними контрагентами для специалистов в области управления рисками, юристов и бухгалтерии.

Система позволяет автоматизировать работу кадровой службы: например, на основании одной анкеты, заполненной кандидатом, в автоматическом режиме формируется полный пакет документов, которые в дальнейшем передаются в работу HR. Полностью в электронном виде можно планировать командировки и отпуска, знакомить сотрудников с внутренними регламентами, оформлять увольнение.

Интеллектуальная ECM способна облегчить работу каждого из бизнес-подразделений компании и сделать процесс общения между ними проще и эффективнее.

Цифровая система в области документооборота дает компаниям ряд преимуществ:

1. Экономию на бумаге и услугах курьеров.
2. Ускорение процессов согласований.
3. Снижение юридических рисков при работе с контрагентами.
4. Снижение вероятности ошибок при работе с финансовыми документами.
5. Интеллектуальную обработку электронных документов с использованием машинного обучения (распознавание, заполнение реквизитов и регистрация).
6. Омниканальность — доступ к информации с любого устройства, подключенного к системе.
7. Быстрое вовлечение новых сотрудников. Механизмы встроенного обучения повышают качество внедрения новых процессов и ускоряют адаптацию новичков.
8. Мощную основу для построения цифрового предприятия. Интегрируемость и различные возможности совместной работы систем в рамках единой ИТ-инфраструктуры.

С чего начать

Внедрение интеллектуальной системы документооборота всегда происходит поэтапно, и оптимально, если для реализации проекта вы привлечете ИТ-компанию с большим опытом работы в области ECM. Главная задача ИТ-консультанта — в диалоге с заказчиком выяснить основные потребности бизнеса и определить, какие процессы необходимо автоматизировать в первую очередь. Далее определяются индивидуальные особенности каждого из подразделений и производится анализ существующей ИТ-инфраструктуры. После этого можно рассчитать стоимость решения для конкретной компании и выстроить индивидуальный график реализации проекта.

Приблизительный план перехода компании к единой информационной экосистеме выглядит следующим образом:

1. Инициация и организация проекта. На данном этапе необходимо определить состав команды внутри компании, спланировать и организовать выполнение работ. Важно, чтобы первоначально в проекте были задействованы сотрудники подразделений, наиболее заинтересованных в автоматизации: чаще всего это секретари-референты, руководители высшего и среднего звена, юристы, делопроизводители. Обеспечив их лояльность, вы создаете позитивный пример пользования системой. С первого дня к решению технических и методических вопросов должны привлекаться ИТ-сотрудники предприятия, так как в дальнейшем они будут сопровождать и развивать систему самостоятельно.
2. Выбор ИТ-консультанта. Специалисты подрядчика прежде всего производят сбор и анализ информации: исследуют автоматизируемые процессы заказчика, выявляют и уточняют требования бизнеса.
3. Анализ рынка ECM. На данном этапе компания совместно с ИТ-консультантом определяется с выбором платформы, наиболее удовлетворяющей запросам компании, и выбирает надежного интегратора.
4. Разработка концепции автоматизации бизнес-процессов. ECM должна быть адаптирована к действующим бизнес-процессам предприятия, поэтому важно произвести их всесторонний анализ. В то же время работа подразделений также должна мягко трансформироваться в соответствии с требованиями выбранной для автоматизации платформы.
5. Проектирование системы и переход к тестовой эксплуатации.
6. Обучение пользователей: перед переходом к опытно-промышленной эксплуатации важно подготовить сотрудников к работе с новой системой.
7. Опытно-промышленная эксплуатация — проверка работы системы в реальных условиях с реальными данными.
8. Промышленная эксплуатация. На данном этапе ИТ-консультант переходит в режим сопровождения системы, который включает в себя обновление версий системы, консультации по настройке и администрированию при изменении бизнеса и законодательства, информационную поддержку.

Разработка четкого плана внедрения с прописанными целями — это важнейший этап реализации проекта, так как он позволяет избежать появления новых задач по ходу работы, а значит, экономит время и деньги. Кроме того, необходимо, чтобы на каждом из этапов внедрения системы в проекте принимало активное участие руководство компании, поскольку только топ-менеджеры могут оперативно решать организационные вопросы, неизбежно возникающие в ходе внедрения (определять ответственных, контролировать выполнение графика внедрения).

Голосовое управление в тренде

На сегодняшний день большая часть крупнейших заказчиков технически и морально готовы к использованию новых технологий в процессе документооборота, на рынке появляются реальные примеры внедрения компонентов искусственного интеллекта в работу ECM-систем. Несмотря на новизну предложения, в настоящее время в проработке у Softline находятся десятки проектов в области создания цифровой экосистемы предприятия.

Чаще всего клиенты интересуются внедрением чат-ботов — современные решения возможно использовать не только для работы внутри команды, но и для проведения тендеров. В ближайшим будущем, по нашим прогнозам, востребованным станет голосовое управление системами документооборота, аналогичное голосовым помощникам поисковых систем вроде Siri и Алисы. Внутри Softline мы также рассматриваем возможность реализовать пилот по внедрению такого решения.

Примеры внедрения

Причина повышенного интереса к подобного рода проектам — их доказанная эффективность. Известен пример компании Wildberries, в которой проект по полному отказу от бумаги стартовал в 2014 году и показал отличные экономические результаты уже через несколько месяцев.

АО «Объединенная двигателестроительная корпорация» после трех месяцев работы с решением для интеллектуальной обработки входящих сообщений сообщила о повышении точности классификации по виду документа на 96% и снижении трудоемкости его регистрации на 15-20%. Продовольственный холдинг «КОМОС-ГРУПП» внедрил у себя чат-бот для бизнеса, «общаясь» с которым пользователи взаимодействуют с СЭД через смартфон. По словам руководителей организации, уже в первые месяцы в компании сократилось время на исполнение поручений и повысилась исполнительская дисциплина.

Состав решения, его цена и срок окупаемости зависят от потребностей организации. При грамотном подборе продуктов и оптимальной схеме их внедрения результат не заставит себя ждать.

3 причины эффективности точечного фишинга

Похоже, сегодня уже дня не проходит без того, чтобы не сообщали о потере данных, взломе сетей, мошенничестве с переводом денег или других преступлениях в сети, которые начинаются с фишинговых атак. Защита электронной почты всегда была одним из приоритетных направлений для специалистов по безопасности ИТ-инфраструктур, и фишинг не зря вызывает такую серьёзную озабоченность — сегодня это одна из наиболее часто эксплуатируемых угроз.

Способы фишинга развиваются и меняются, постоянно совершенствуясь и подстраиваясь под формальную переписку целевого эккаунта. И если всё сделано правильно, то сразу определить, что такое письмо содержит угрозу, будет тяжело. Это связано с тем, что точечный фишинг рассчитан на человеческие отношения. Злоумышленники тратят много времени на разработку стратегий, исследование объекта атаки и изучение его переписки, совершенствуют свои методы, пока не добьются успеха или не примут решение двигаться дальше.
При серьёзном анализе фишинговых атак становится ясно, почему они не перестают быть эффективными. Вкратце можно выделить три основные причины успешной деятельности преступников в сфере фишинга.

Иллюзия нормальных отношений

Злоумышленники не хотят, чтобы их раскрыли, поэтому они подделывают почтовые домены, чтобы их адреса выглядели надёжными и убедительными. Около 53% этих атак подделывают Microsoft и Apple, а остальные имитируют такие имена, как UPS, Chase и Amazon. Злоумышленники разрабатывают специальные шаблоны электронной почты, чтобы выглядеть как представители больших и известных компаний, что повышает вероятность доверительного отношения адресата. В тексте письма может содержаться предупреждение о нарушении безопасности или запрос на подтверждение какой-либо информации, чтобы получатель нажал на ссылку и подтвердил свои данные для входа в учетную запись или сообщил другие персональные данные.
Ссылки в таких письмах могут выглядеть формально правильными, однако, нажав на ссылку, жертва попадает на фишинговый веб-сайт, который используется для кражи учётных данных для входа. Если злоумышленник смог получить учётные данные пользователя, то ему не составит труда получить доступ к другим ресурсам от его имени или использовать персональные данные для запуска новых атак в ИТ-инфраструктуре организации. Фактически, одной из причин, почему чаще всего атакам подвергается программное обеспечение компании Microsoft, заключается в том, что учётные данные Office 365 — это самый короткий путь к ИТ-инфраструктуре любой организации. Если злоумышленникам удаётся получить учётные данные пользователя для доступа к облачным приложениям, они легко входят в сеть и продолжают развитие атаки.

Иллюзия сотрудничества

Если вы не знакомы с атаками типа Business Email Compromise (BEC), вы точно не одиноки. Они составляют всего 6% от фишинг-атак, но обходятся организациям невероятно дорого. ФБР заявляет, что финансовые потери от атак BEC с 2013 года по настоящее время составили более 12,5 миллиардов долларов. Но это только верхушка айсберга, потому что большая часть осталась неучтённой из-за нежелания компаний рассказывать о подобных проблемах.

Основные типы фишинговых атак

Почему потери от этого вида мошенничества так высоки, если они составляют всего всего 6% от всех фишинговых атак? Причина заключается в том, что подобного рода письма написаны, якобы от тех людей, которым пользователь может доверять — это может быть непосредственный начальник, руководитель корпорации, сотрудник отдела или любое другое лицо, имеющее полномочия для отправки запроса на перевод денежных средств или предоставление конфиденциальных данных. Суммы достигают огромных размеров. Об этом свидетельствуют атаки на Facebook и Google. Два технологических гиганта уже потеряли около 100 миллионов долларов, переведя их на счета злоумышленников. В результате утечки данных возникает ответная реакция в виде штрафов и ужесточения требований регуляторов, что снова приводит к потерям десятков и даже сотен тысяч долларов.

Иллюзия шантажа и запугивания

Каждая десятая фишинг-атака нацелена на шантаж или запугивание жертвы при помощи якобы существующих компрометирующих материалов. Злоумышленники часто начинают рассылать подобные требования, получив комбинацию адреса электронной почты и пароля в результате одной из атак. Эти учётные данные собираются в darknet, а затем используются в качестве возможного доказательства того, что у злоумышленника

есть личная информация о жертве. Установив «достоверность» учётных данных, злоумышленники начинают предъявлять требования о выкупе. Обычно речь идёт о каком-нибудь видео, фотографии или информации о просмотре неблагонадёжных веб-страниц. Преступник редко обладает серьёзной информацией такого уровня, но многие не хотят рисковать и просто платят, не получая потом никакого ответа.

Необходимость защиты

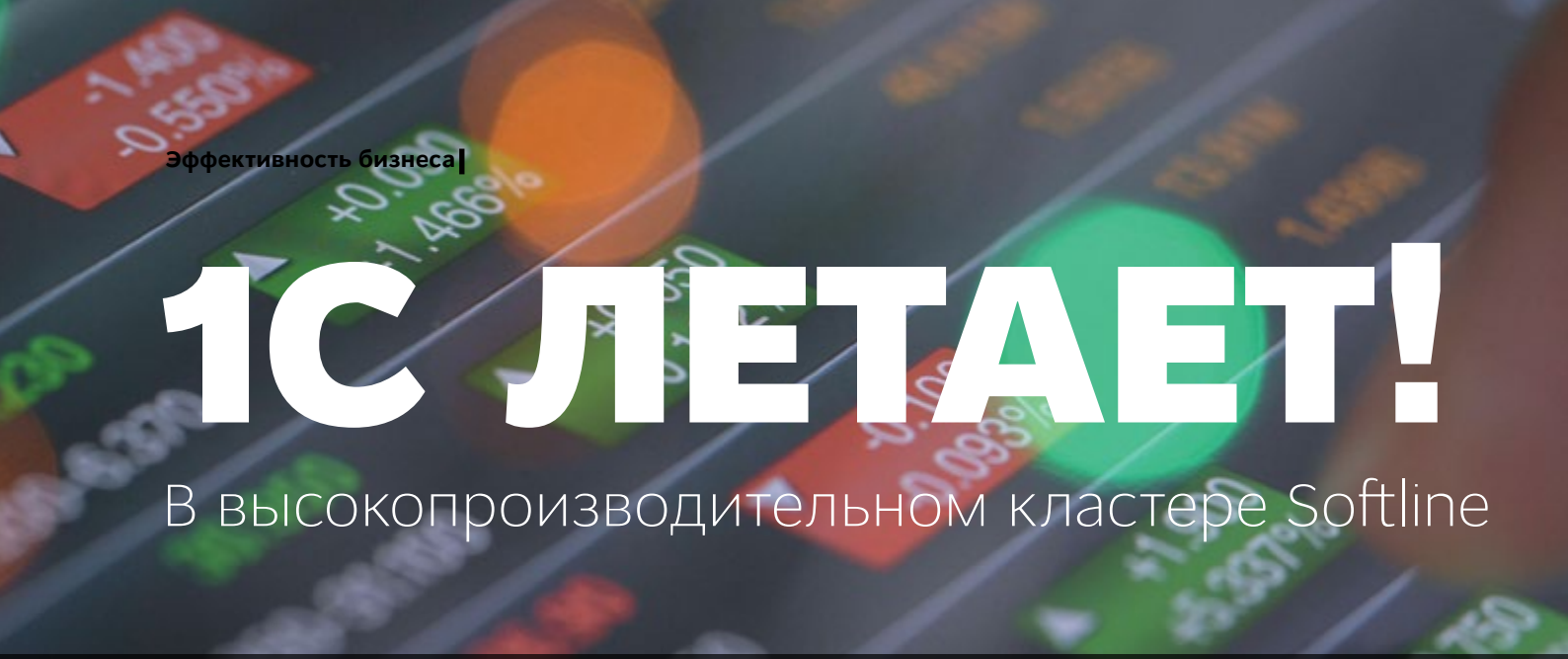
Точечный фишинг по-прежнему работает, потому что традиционная защита электронной почты не всегда эффективна при подобных атаках. Шлюзы безопасности электронной почты являются важной линией защиты, но фишинговые письма могут проникать через них и атаковать людей.

- Атаки тщательно продуманы и направлены, наблюдение за предполагаемой жертвой занимает несколько месяцев. Они составлены как реальные письма и рассылаются штучно.
- Очень часто для начала атаки используют такие почтовые сервисы, как Gmail, что означает, что отправляющий домен имеет высокую репутацию. Поэтому эти письма не блокируются.
- При отсутствии явно вредоносных ссылок или вложений, как в случае атаки BEC, традиционные признаки того, что сообщение электронной почты является атакой, отсутствуют.

Точечный фишинг: «Основные угрозы и тенденции» — это бесплатный отчёт, в котором подробно описываются все атаки, как они работают и почему традиционных средств безопасности для их отражения недостаточно. Отчет основан на исследованиях специалистов компании Barracuda и включает в себя ряд примеров атак на известные бренды, описание часто используемых сюжетных линий и многое другое. Также включены ссылки на передовой опыт и рекомендуемые тренинги и технологии.

Для защиты от фишинга компания Barracuda предлагает следующие решения: Sentinel, Essentials и Email Security Gateway. Они защищают все устройства пользователей, помогая безопасно, эффективно и экономично внедрить Office 365, а также защищают пользователей от опасных вымогателей и фишинговых атак. Данное решение минимизирует время простоя, обеспечивает соблюдение нормативных требований и позволяет быстро и эффективно восстанавливать данные Exchange Online, OneDrive и Sharepoint Online, обеспечивая пользователям непрерывную работу и полную защиту в среде Office 365.
Barracuda Networks — известный производитель средств защиты электронной почты, предлагающий кроме того простые, полнофункциональные и доступные решения для защиты данных, безопасности сетей и приложений. ▮

Свыше 150 000 корпоративных клиентов по всему миру доверили продуктам Barracuda Networks защиту своей инфраспруктуры не только внутри сети, а также и в облачной сфере. Основными продуктами компании являются Barracuda CloudGen Firewall, Barracuda Essentials и Barracuda Backup.
http://www.barracuda.com
http://www.softporm-blog.ru



1С ЛЕТАЕТ!

В высокопроизводительном кластере Softline

Облако «не тянет» такое необходимое для бизнеса приложение, как 1С? У вашего провайдера нет готовой платформы с процессорами повышенной мощности? Softline меняет ситуацию!

Особый подход к вопросу

Большой спрос на 1С в облаке — логичное последствие цифровизации российского рынка. 1С — система для автоматизации управления и учета на предприятиях различных отраслей, видов деятельности и типов финансирования, уже стала корпоративным стандартом. В связи с последними тенденциями рынка развертывание приложения внутри компании — вариант дорогой и не самый эффективный. Причина? У подобных приложений есть особенности: они не очень хорошо умеют работать в многопоточном режиме.

ПО, которое умеет нагружать сразу несколько процессорных ядер, способно «разделиться» на потоки и таким образом быстро работать. 1С функционирует по-другому — здесь нужен высокопроизводительный процессор с большим показателем тактовой частоты.

Именно поэтому компания Softline создала специальный облачный кластер с особым профилем нагрузки.

В чем особенности?

Этот кластер устроен так же, как и всё остальное облако, — в нем постоянно держится определенный запас процессорной мощности и памяти. Надежность максимальная: на несколько хостов есть запасной, чтобы в случае выхода из строя виртуальные машины моментально перезапустились. Отличительная черта кластера — процессоры с большей частотой, которая составляет 3 ГГц по сравнению со стандартными 2,2-2,6 ГГц.

Идеальная платформа для 1С в облаке

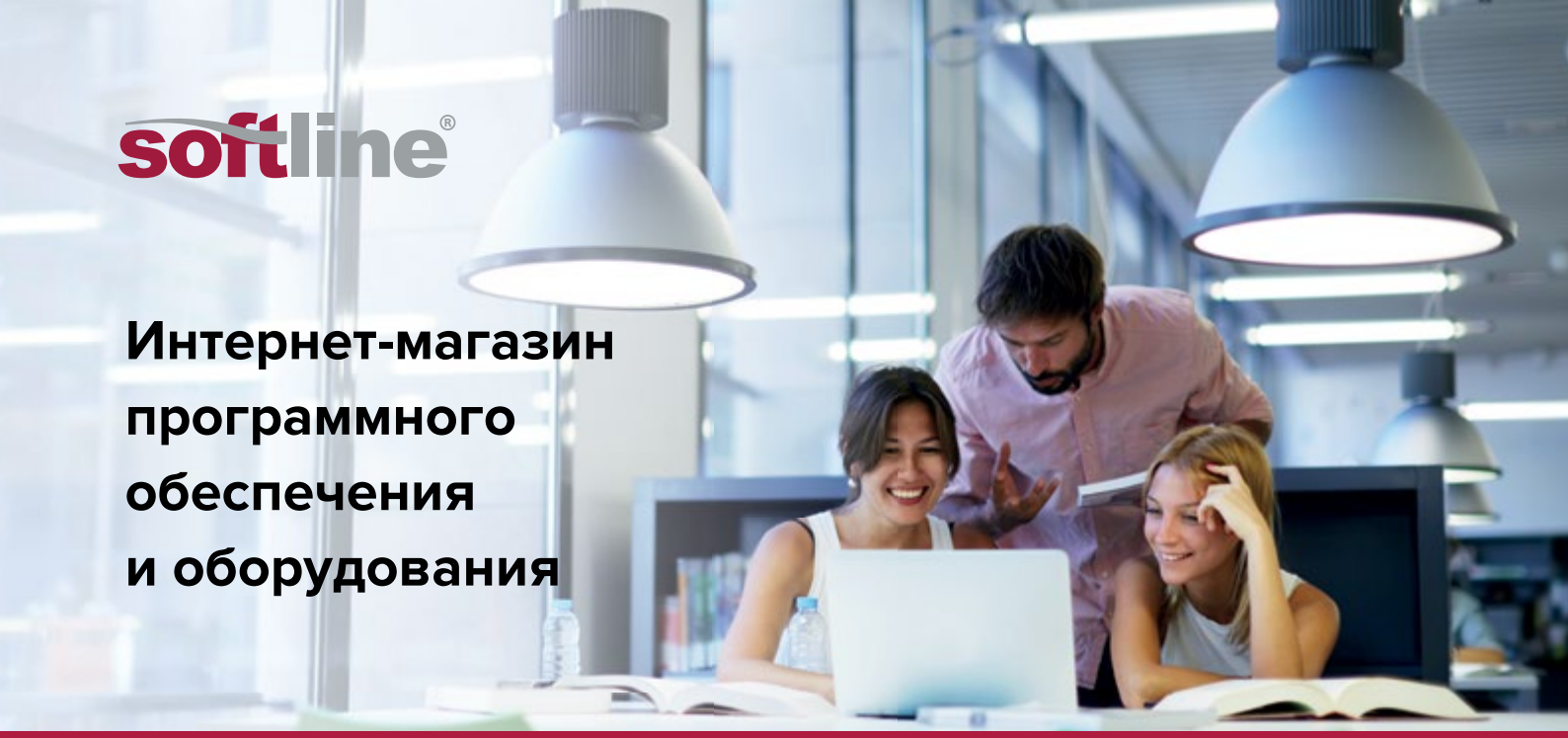
Успешную работу высокопроизводительного кластера уже подтвердили заказчики Softline. Одна из российских компаний обратилась к нам со следующей задачей: набору сервисов, в том числе приложению 1С, необходимо было обеспечить высокую производительность и техническую поддержку. Заказчик протестировал сервисы в облаке и обнаружил, что платформа удовлетворяет всем его потребностям. Специалисты Softline предложили не только правильную инфраструктуру, но и всестороннюю помощь в процессе переезда с других серверов. Миграция в облако Softline заняла две недели. 1С был размещен на четырех виртуальных машинах в кластере частотой с 3 ГГц. Все сервисы объединены в одну сеть.

Обратитесь уже сегодня

Берите в аренду мощности в облаке Softline. Размещайте в нем приложение 1С, и при этом вы не будете зависеть от внешней конъюнктуры или курса валют, поскольку все оплачивается в рублях. Компания будет иметь уверенный доступ к данным из любого места и в любое время. Мы организуем выделенные виртуальные серверы 1С именно для вас, предложим широкие возможности масштабирования, а также администрирование — собственными либо нашими силами.


STATiSTiCA
IoT - Analytics!
Аналитические исследования Интернета Вещей
ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ
от StatSoft®
УНИКАЛЬНЫЕ РЕШЕНИЯ ДЛЯ НЕФТИ и ГАЗА
Постигаем Умные Данные...
academy
StatSoft
IoT-Аналитика, Курсы, Консалтинг
Закажите сейчас:
+7 (495) 78 777 33
sale@statsoft.ru
www.statsoft.ru

softline®



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
- Постоянный доступ к данным заказа и документам
- Возможность работать по электронному документообороту
- Доставка электронных лицензий за 10 мин.
- Доставка по России
- Отслеживание статуса оплаты заказа
- Служба поддержки
- 5 звезд на Яндекс-Маркет
- Достаточно только ИНН.
  Остальные реквизиты заполняем автоматически

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