softline direct

КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2 (35)
2019 BY

Think BIG!

Приложения для бизнеса, которые упростят вам жизнь
Стр. 16

История успеха: Softline помогла Mercedes-Benz усовершенствовать бизнес-процессы
Стр. 20

Как атакуют белорусские компании?
Стр. 28

+375 (17) 336-55-95

www.softline.by

5 причин выбрать Softline

15+
лет работы на ИТ-рынке Беларуси

25+
партнерских статусов и наград ведущих поставщиков hardware, software и cloud

500+
успешных реализованных проектов

50+
сертифицированных инженеров

5
офисов в каждом областном центре

Уважаемые коллеги, партнеры, друзья!
Мы рады представить вам новый выпуск каталога Softline-direct.

Цифровая трансформация – это не только внедрение электронного документооборота. Это новый способ сделать работу удобнее, повысить маржинальность при минимальных затратах, а также возможность предложить своим заказчикам то, чего они действительно хотят.

В этом выпуске мы расскажем, как оптимизировать бизнес-процессы с помощью экосистемы Office 365. На примере нашего кейса с Mercedes-Benz вы увидите, как сотрудники автомобильного дома «Энергия ГмбХ» наладили коммуникации, получили эффективную систему защиты и оптимизировали затраты на ПО.

Корпорация Microsoft сейчас находится в процессе глобальных изменений. Заняв в прошлом огромную долю мирового рынка программного обеспечения как производитель Office 365 и ОС Windows, сегодня она успешно трансформируется в поставщика облачной платформы, и центральным продуктом становится Azure. Microsoft вкладывает много усилий для того, чтобы сделать свою облачную платформу лучшей в мире, и это им удается. Сегодня доля Azure растет быстрее, чем доля таких конкурентов, как Amazon и Google.

По причине роста интереса к ИТ-сфере увеличивается и число киберпреступлений. По статистике, за январь-август 2019 года количество атак увеличились примерно в 2 раза по сравнению с аналогичным периодом 2018. Руководитель направления информационной безопасности Softline Александр Дубина расскажет, как сегодня атакуют белорусские компании и на что нужно обращать внимание при защите данных. Кроме того, мы сделаем акцент на том, почему важно выполнять требования регулятора в сфере ИТ-безопасности и как Softline может помочь в этом вопросе.

Правильно спроектированная ИТ-инфраструктура позволяет полностью автоматизировать бизнес-процессы компании. В этом выпуске мы познакомим вас с новой платформой для оркестрации контейнеров Kubernetes, которая не просто автоматизирует процессы, но и значительно упрощает жизнь разработчикам и пользователям.

Уже 18 лет мы помогаем белорусским компаниям изменить подход к бизнес-процессам и сделать современные технологии доступными. Softline наращивает собственную экспертизу и концентрирует свои усилия на том, чтобы помогать нашим заказчикам быть конкурентоспособнее и выводить на рынок новые технологичные продукты и услуги.

Мы приглашаем вас к сотрудничеству. Вместе мы сможем создать действительно работающие инструменты для реальных бизнес-задач!

С пожеланиями успеха,
Андрей Овсейко,
генеральный директор компании Softline Беларусь

Softline

СОДЕРЖАНИЕ

Каталог ИТ-решений и сервисов для бизнеса

Softline direct

ДЕКАБРЬ

2019-2(35)-BY

Учредитель:
ООО «СофтЛайн Директ»

Главный редактор:
Савончик Инна Николаевна

Выпускающий редактор:
Яна Ламзина

Дизайн и верстка:
Алексей Воропанов

Адрес редакции:
220062, г.Минск, пр-т Победителей, 108, 4 этаж, помещение 10.

Распространяется бесплатно.

Тираж:
3000 экз.

Подписано в печать – 05.12.2019
Отпечатано в типографии:
ОДО «Дивимакс»
220007, г. Минск, ул. Аэродромная, 125, пом. 5В

Лицензия №02330/53 от 14.02.2014 г. выдана Министерством информации РБ.
УНП 190147176
Заказ №2638.

Зарегистрировано в Министерстве информации РБ.
Свидетельство о регистрации №2/87 от 19.07.2016.

Контактная информация:
marketing@softline.by

Softline в соцсетях  SoftlineBelarus  @softline_belarus  Softline Belarus

Mercedes-Benz

Компания Softline помогла усовершенствовать бизнес-процессы

стр. 20

Информационная безопасность и требования регуляторов

Интервью со специалистом по информационной безопасности Softline Дмитрием Сугако

стр. 32

ЕРИП

Компания Softline помогла обеспечить процесс управления инцидентами информационной безопасности

стр. 35

ОАО «Паритетбанк»:

Модернизация инфраструктуры

стр. 48

Think BIG!

ПОРТРЕТ КОМПАНИИ

Наша миссия

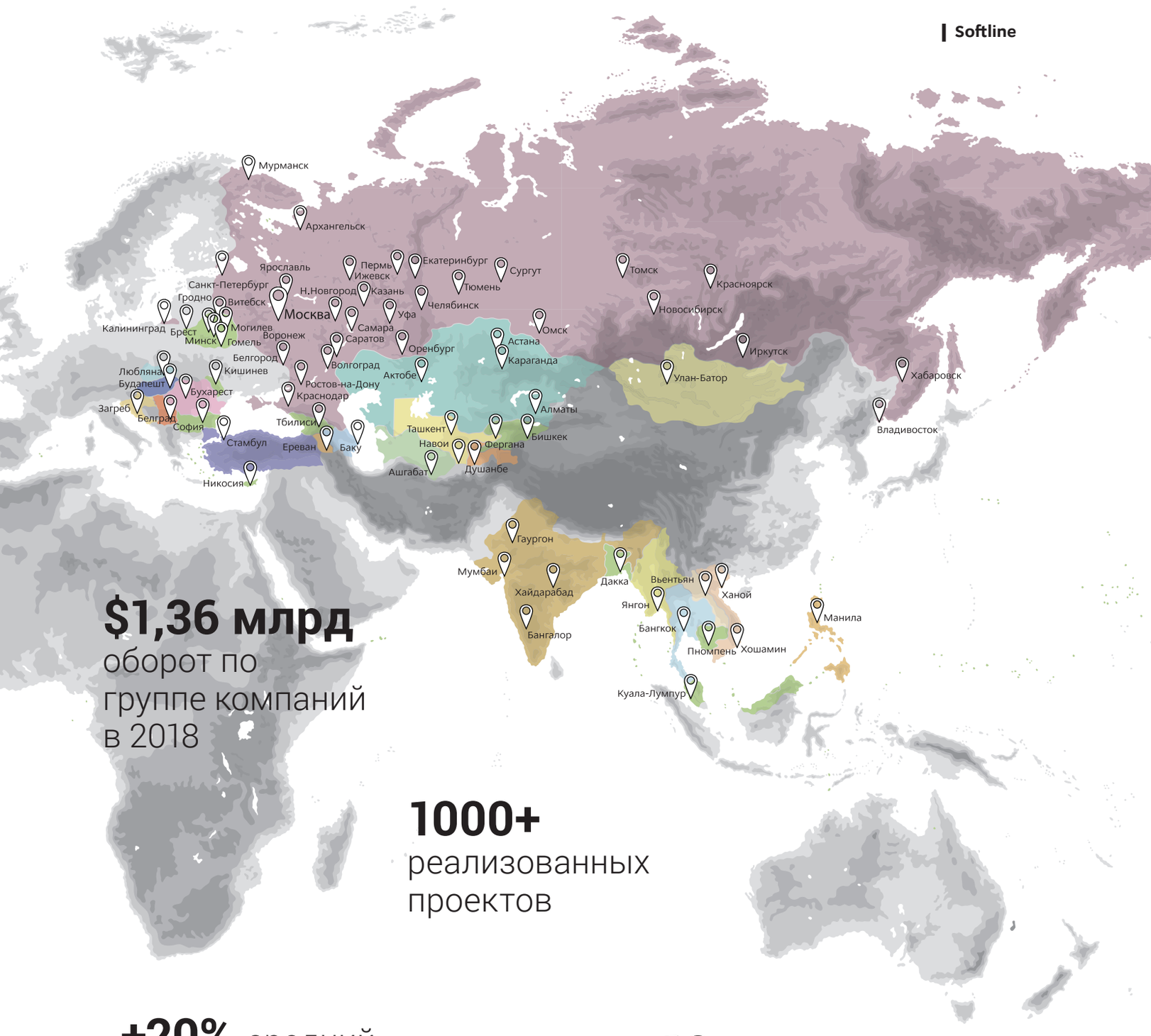
Мы осуществляем цифровую трансформацию бизнеса наших клиентов на основе передовых информационных технологий и средств кибербезопасности.

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 30+ странах и 80+ городах
5. Softline доверяют ведущие игроки рынка, государственные организации, средние и малые компании

Digital Transformation & Cybersecurity Solutions Service Provider

Статусы Softline



$1,36 млрд
оборот по группе компаний в 2018

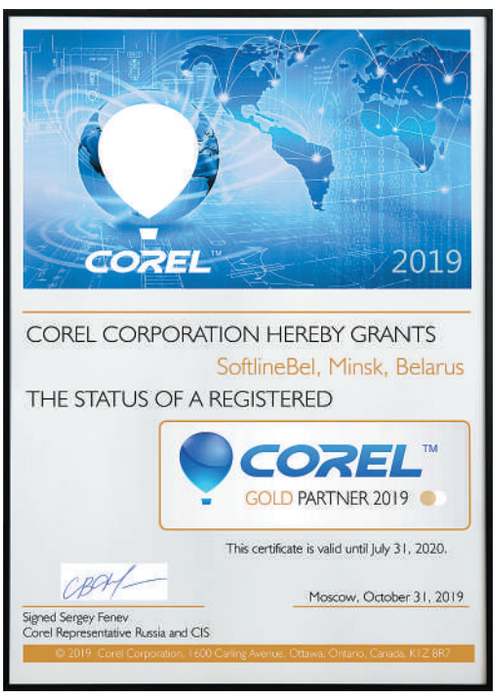
1000+
реализованных проектов

+20% средний ежегодный рост продаж

18 лет на ИТ-рынке Беларуси

Компания Softline получила золотой статус Corel

По итогам успешной работы компания Softline получила Золотой статус Corel – лидера на рынке графического, офисного и цифрового мультимедийного ПО.
Компания Corel высоко оценила профессиональные результаты и активную деятельность Softline. Наличие статуса Gold Partner позволяет нам предоставлять квалифицированную и оперативную поддержку поставляемых решений. ▮



Подтвержден золотой статус партнерства с Lenovo

Успешно выполняя проекты на основе оборудования Lenovo, компания Softline зарекомендовала себя как надежный партнер и благодаря этому подтвердила статус Lenovo Data Center Gold Partner.
Наличие Золотого статуса гарантирует высокое качество услуг, связанных с использованием решений Lenovo. ▮

Команда Softline приняла участие в Минском полумарафоне-2019

В первые выходные сентября, помимо Дня города Минска, отмечается праздник спорта и здоровья. На центральных проспектах и улицах города в этот день собираются профессионалы и любители бега. Это десятки тысяч участников со всех уголков мира, море позитива, счастливых улыбок и невероятный заряд эмоций!
15 сентября 2019 года прошел ежегодный Минский полумарафон, в котором приняли участие сотрудники Softline. Вместе мы успешно справились с дистанциями в 5, 10 и 21 км.
Герои Softline и дистанции: Александр Орлов (20,097 км), Игорь Майоров (20,097 км), Сергей Мельников (10,55 км), Виктор Синяк (10,55 км), Алексей Горшков (10,55 км), Максим Хвиневич (5,5 км), Ольга Ермакович (5,5 км), Ольга Семак (5,5 км), Анастасия Пупко (5,5 км), Наталия Баньковская (5,5 км), Елена Крыж (5,5 км), Наталья Ковальчук (5,5 км), Инна Кушнер (5,5 км), Люся Стасько и Михаил Стасько (5,5 км).

Для команды Softline участие в Минском полумарафоне уже стало доброй традицией. В этом году наш состав расширился до 15 человек. Softline любит спорт, заботится о здоровье и всегда рада принимать участие в спортивных состязаниях. Вместе мы можем всё! ▮

Softline Belarus принимает участие в «Премии HR-бренд Беларусь» 2019

Компания Softline Belarus оказалась среди номинантов конкурса «Премия HR-бренд 2019» со своим проектом «Глазируем впечатления. Система повышения счастья сотрудников и, как следствие, дохода бизнеса». Основная цель проекта – показать переход от подхода «здесь-и-сейчас» к целостному управлению человеческим капиталом, подразумевающему постоянную обратную связь, действия и мониторинг на всех этапах «жизненного цикла» сотрудника: от поиска кандидата до выходного интервью.

«Участие в премии HR-brand 2019 – это новый опыт и прекрасная возможность рассказать о нашей невероятной команде и HR-процессах. Мы любим то, что делаем. Мы любознательны, постоянно развиваемся и уверены в собственных силах. Эта уверенность основана на реальном опыте, она позволяет нам брать на себя серьезные обязательства и нести ответственность за результат. Каждый из нас – талант. Каждый делает Softline сильнее и подчеркивает успешность нашей команды и бренда», – рассказала HR Business Partner region Belarus Softline Екатерина Сильченко.

«Премия HR-бренд Беларусь» – конкурс в области управления персоналом, благодаря которому лучшие HR-проекты получают признание и известность, а профессионалы – возможность обмена опытом и знакомства с лучшими HR-практиками. В этом году премия проходит в Беларуси шестой раз. ▮

Впервые в Беларуси состоялась кибер-игра KIPS

27 сентября в Minsk Marriott Hotel впервые в Беларуси прошла кибер-игра Kaspersky Interactive Protection Simulation (KIPS).

KIPS – это игровой тренинг, направленный на повышение уровня культуры кибербезопасности для руководителей компаний и ИБ-специалистов. По правилам, каждая команда отвечает за свою компанию и защищает собственную ИТ-инфраструктуру от киберугроз в условиях ограниченного бюджета. Участникам необходимо защититься, максимально повысить прибыль и сохранить свою репутацию. Все это приближено к реальным кейсам информационной безопасности и позволяет испытать свои собственные навыки и знания.

Игра помогает донести информацию о работе службы безопасности компании, разобрать процессы, с которыми ее сотрудники сталкиваются ежедневно. Руководители часто не понимают, как работают специалисты по ИБ, поэтому так важно понять изнутри особенности их деятельности.

В отличие от традиционных форматов обучения, которые перенасыщены технической информацией и отнимают много времени, KIPS позволяет быстро и на практических кейсах получить понимание, как происходит работа в отделе безопасности, и как она помогает компании приносить прибыль. Когда ИБ-сотрудники и руководители вместе решают одну и ту же задачу, они могут более эффективно подойти к проблеме.

Компания Softline поздравляет команду победителей, которая в нелегкой схватке выдержала финальную атаку хакеров и оперативно создала оптимальную стратегию реагирования на кибератаки.

Отдельная благодарность выражается «Лаборатории Касперского» за организацию и проведение KIPS, а командам – за высокую активность. Надеемся, что полученный опыт пригодится участникам игры как в профессиональной деятельности, так и в других конкурсах по информационной безопасности. ▮

В новом офисе Учебного центра Softline прошел Open Education Day

6 сентября распахнул свои двери новый офис Учебного центра Softline в Беларуси. Open Education Day проходил в две параллельные сессии, поэтому каждый участник смог выбрать для себя подходящую активность.

Руководитель направления информационной безопасности Softline Александр Дубина рассказал слушателям о сервисах и компетенциях компании Softline и Учебного центра (УЦ). Александр отметил: «Сегодня Softline закрывает все ИТ-направления. И за каждым таким направлением стоит целый департамент, люди, инженеры, которые решают задачи любого уровня».

Спикеры УЦ и Softline провели воркшопы. Их выступления были посвящены: информационной безопасности и защите информации; обеспечению безопасности учетных записей пользователей в ОС Windows; защите от вредоносного ПО; тенденциям развития ИТ-инфраструктуры; принципам гиперконвергенции и возможностям технологии VMware vSAN.

Кроме того, эксперты Softline продемонстрировали решения и рассказали об успешном опыте их применения в белорусских компаниях.

Полезные доклады, рассказ об условиях обучения, общение, а также знакомство с преподавателями и коллегами – участники зарядились отличным настроением и новыми знаниями.

Напоминаем, что новый офис учебного центра находится по адресу: **Минск, пр-т Победителей, 110 (5 этаж)**. ▮

Воркшоп Softline, посвященный технологиям виртуализации

Виртуализированная инфраструктура быстро адаптируется под меняющиеся потребности бизнеса за счет управления на программном уровне и автоматизации многих процессов.

На очередном воркшопе Softline эксперты познакомили участников с технологиями виртуализации и продемонстрировали работу VMware vSAN – программного хранилища данных.

Эксперты Softline рассказали, что vSAN встроена в гипервизор и благодаря этому имеет оптимизированную архитектуру, обеспечивающую производительность до 100 тыс. операций ввода-вывода в секунду на узел хранения. Система хранения данных vSAN построена на флэш-накопителях и обеспечивает чрезвычайно высокий уровень производительности и максимально простую вертикальную и горизонтальную масштабируемость. При добавлении каждого нового узла автоматически увеличивается объем хранения и количество операций ввода-вывода в единицу времени.

«Мы постоянно следим за трендами и новыми технологиями в области виртуализации. Приглашаем всех желающих посетить наши воркшопы в офисе Softline (Минск, пр-т Победителей, 108), где мы демонстрируем большинство решений VMware. У вас есть отличная возможность познакомиться и протестировать NSX, vSAN, vSphere, Horizon, Workspace ONE, а также задать все интересующие вопросы экспертам», - отметил продакт-менеджер по направлению «Инфраструктурные решения и виртуализация» компании Softline Игорь Волокитин. ▮

Softline и «Лаборатория Касперского» рассказали о защите ИТ-инфраструктуры

10 октября в Гродно прошел семинар на тему «Максимальная защита бизнеса». Представители компаний Softline и «Лаборатории Касперского» рассказали о защите промышленных систем, виртуальных серверов и рабочих станций.

Эксперт «Лаборатории Касперского» Александр Смирнов выступил с темой защиты промышленных предприятий. Он отметил, что самое главное для промышленных компаний – обеспечить бесперебойность работы, так как даже небольшая ошибка может привести к непоправимым последствиям. А для ИТ-инфраструктуры, в первую очередь, важно обеспечить защиту конфиденциальных данных.

Отдельное внимание было уделено защите от комплексных целевых атак. Спикер рассказал о решении «Лаборатории Касперского», которое противодействует комплексным угрозам, анализирует данные, записывает их и хранит. Благодаря такой системе можно более эффективно расследовать многоступенчатые атаки.

Эксперты «Лаборатории Касперского» отметили преимущества новой онлайн-платформы ASAP – набора интерактивных тренингов, направленных на повышение осведомленности сотрудников об онлайн-угрозах, развитие навыков безопасного поведения в сети.

Компания Softline благодарит всех за участие и теплый прием. Мы всегда рады поделиться своим экспертным мнением и помочь в решении любых задач в области ИБ. ▮

Соглашение о стратегическом сотрудничестве с Dana Holdings

Крупнейшая в Беларуси строительная ГК Dana Holdings и компания Softline подписали меморандум о долгосрочном и взаимовыгодном сотрудничестве. В ходе совместной работы партнеры объединят усилия с целью развития ИТ-инфраструктуры Dana Holdings, внедрения высокотехнологичных решений в области информационной безопасности и разработки проектно-сметной документации.

Компания Softline становится основным поставщиком ИТ-решений для реализации проектов Dana Holdings: «Минск Мир» (Беларусь), «Международный финансовый центр» (Беларусь), БК «Тесла Парк» (Казахстан).

Softline совместно с Check Point рассказали о защите от кибератак «нулевого дня»

3 сентября в офисе Softline успешно прошел практический семинар Sandblast Demo-Day.

Эксперты компании Check Point на реальных примерах рассказали и продемонстрировали, как реализуются современные кибератаки «нулевого дня», и как от них можно защищаться на уровне сети, рабочих станций, серверов и мобильных устройств.

Специалисты Check Point рассказали о новых технологиях защиты от современных угроз, отметили основные тенденции кибератак текущего года: мобильный банкинг, атаки на цепь поставок, электронную почту и облачные хранилища. Вместе с тем назвали один из самых распространенных на сегодня троянов – Emotet. ▮

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Datacenter
Gold DevOps
Gold Data Analytics
Gold Communications

Наши компетенции Microsoft

Компания Softline всегда находится на стороне клиента и предлагает решения, наилучшим образом подходящие к его задачам. Ежегодно мы подтверждаем высокие статусы более 1000 известных отечественных и мировых производителей ПО. Ключевым партнером Softline является корпорация Microsoft.

Партнерская программа Microsoft Partner Network и Microsoft Licensing Solution Partner

Softline обладает рядом компетенций по программе Microsoft Partner Network. Это сообщество, которое помогает партнерам корпорации максимально эффективно использовать свои возможности.

Компетенции уровня Silver, присваиваемые корпорацией Microsoft, дают партнерам больше возможностей для демонстрации своего профессионализма и опыта, а также для получения преимуществ над конкурентами.

Компетенции уровня Gold – это подтверждение наивысшего уровня профессионализма ее обладателя в рассматриваемой категории.

На данный момент компания Softline имеет высший статус Microsoft Licensing Solution Partner (LSP). Этот статус присваивается крупнейшим партнерам Microsoft, подтвердившим свой профессионализм и высокое качество работы с заказчиками на протяжении многих лет. Softline уверенно занимает лидирующие позиции на рынке среди LSP-партнеров как по объему бизнеса, так и по количеству действующих соглашений. Статус LSP дает Softline право предоставлять крупным корпоративным клиентам лицензионное ПО Microsoft на особых условиях в рамках программ корпоративного лицензирования, в том числе Enterprise Agreement (EA), Enterprise Agreement Subscription (EAS), Microsoft Products and Services Agreement (MPSA).

В рамках данных статусов Softline обладает компетенциями: Gold Datacenter, Gold Cloud Productivity, Gold Collaboration and Content, Gold Messaging, Gold Cloud Platform.

Статус Microsoft Cloud Solution Provider (CSP)

CSP (Cloud Solution Provider) – программа, позволяющая перепродавать облачные продукты Microsoft (Office 365, Exchange Online, Azure и др.), а также добавлять к ним собственные ИТ-решения. Благодаря программе Cloud Solution Provider компания Softline сможет обеспечивать бизнес-клиентов:

- облачной платформой Microsoft Azure;
- Office 365, одним из самых востребованных облачных сервисов;
- наиболее гибкими условиями оплаты за использование облачных сервисов Microsoft;
- технической поддержкой по всем сервисам на русском языке;
- обучением сотрудников.

Статус Microsoft SPLA Reseller

Сотрудничество в качестве SPLA Reseller дает Softline возможность расширить круг партнеров и клиентов за счет их участия в программе лицензирования SPLA. Эта программа позволяет использовать ПО Microsoft на правах аренды.

SPLA-партнеры Softline Беларусь могут использовать программное обеспечение Microsoft по модели pay-as-you-go как для оптимизации собственной работы, так и для оказания услуг клиентам. Компания предлагает простой и удобный способ перейти от классической схемы приобретения ПО в собственность к более практичной модели облачного лицензирования, где ПО Microsoft предлагается в качестве услуги. При этом конечные пользователи будут иметь возможность выбора между покупкой программного обеспечения и его арендой.

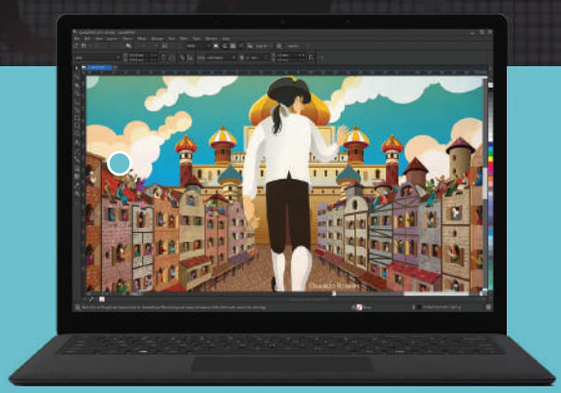
Программа SPLA обеспечивает доступ к большому числу лицензионных продуктов Microsoft, в их числе: Microsoft Office, Microsoft Exchange Server, Microsoft SharePoint Server, Windows Server, Microsoft Dynamics и другие.

Статусы Microsoft свидетельствуют о том, что корпорация признает Softline партнером высочайшей квалификации по своим ключевым технологиям и подтверждает качество услуг компании. Для достижения столь значимых результатов специалисты Softline продемонстрировали должный уровень знаний в продуктах Microsoft, связанных с полученными компетенциями и успешно прошли сертификацию.

ПО для разработки графического дизайна

CorelDRAW® GRAPHICS SUITE 2019

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



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!

Опыт Allevi, стартапа в сфере биопринтинга

Пять лет назад Рики Солорзано создал стартап, который производит 3D-биопринтеры, с помощью которых можно воспроизводить клетки и генерировать целые клеточные структуры. В интервью Рики рассказал, сколько стоит напечатать сердце и каково будущее индивидуальной медицины.

— Рики, расскажите популярно, чем занимается ваш стартап?

— 3D-печать используется для быстрого изготовления деталей самолетов, поездов, автомобилей и других массовых производств. Материалы могут быть самыми разными — от металла до углеродного волокна и пластика. Точно так же эта технология может использоваться в биологии. Наш стартап разрабатывает специальные биопринтеры, которые позволяют воспроизводить клетки и генерировать целые клеточные структуры. То есть придавать тканям нужную геометрию.

— Зачем это нужно?

— Сегодня биологи, которые изучают устройство тела, могут запросто купить в интернете клетки любого типа, поместить их в пробирку и наблюдать, как они реагируют на те или иные химические вещества, лекарства. Но поскольку это просто клетки без какой-либо геометрии, результаты таких исследований не очень точны.

Ученый, который уже 20 лет исследует ткани сердца или печени, прекрасно знает, как они должны выглядеть. Так почему бы ему не взять набор клеток, из которых состоят эти органы, и не склеить их определенным образом, а затем распечатать на 3D-принтере?

Работа тела напрямую зависит от геометрии клеток. Например, клетки мышц имеют вытянутую форму, а клетки печени — круглые. Если с помощью принтера создать из этих клеток ткань, то такой материал подойдет для опытов намного лучше разрозненных клеток в пробирке, и благодаря ему ученые смогут получить более ценные данные.

Над этой задачей, собственно, и работает наша компания. Мы создаем простые в использовании биопринтеры, специальный софт и работаем, используя биочернила — смесь клеток, биоматериалов и биоактивных молекул.

— На вашем сайте сказано, что биопринтеры Allevi позволяют «воспроизводить и изучать тело вне тела».

— Да, изучение тела вне тела — как раз то, чего очень хотят биологи. Возможность придавать клеткам геометрию вне тела — значит видеть их в 10 раз лучше и нагляднее. Наш стартап позволяет проводить такие исследования тканей, которые было невозможно осуществить раньше. Клетки, имеющие нужную геометрию, будут вести себя почти так, как ведут себя внутри тела.

И еще один важный момент: в природе известно более 30 типов клеток, из которых строятся ткани. Индустрия научилась воспроизводить с помощью 3D-принтера только один-два типа клеток, соединенных между собой особым образом. В то время как наш биопринтер Allevi 6 позволяет ученым печатать клетки шести различных типов, чего не умеет ни один другой. Таким образом, мы позволяем ученым создавать более сложные ткани.

Например, можно взять раковые клетки и на их основе сделать модель раковой опухоли. Это актуально для индивидуальной медицины.

Возьмем для примера исследование клеток конкретного пациента. Делается биопсия раковой опухоли, воссоздаются ткани опухоли и на них тестируются конкретные лекарства или их смеси. Такой подход сделает лечение более эффективным. Я думаю, уже через несколько лет он станет реальностью.

Наука постепенно движется к использованию 3D-культуры клеточных тканей вместо 2D. 3D-формат предполагает более сложную геометрию тканей и дает более надежные результаты исследований. Благодаря этому эффект лекарств становится более предсказуемым и безопасным, чем сейчас.

— Ваша компания появилась всего пять лет назад, но биопринтеры уже представлены во многих странах. Как вам удалось достичь столь впечатляющих результатов за столь короткое время?

— Пожалуй, это можно объяснить двумя причинами.

Во-первых, 80% наших клиентов — академии и университеты, 20% — представители разных индустрий. Нам на руку сыграло то, что академические учреждения используют единый подход к тканевой инженерии.

Вторая причина — наличие интернета и курьерской компании UPS. Сначала мы не знали, как доставлять наши принтеры. А потом пришли к выводу, что вообще не должны этим заниматься, ведь есть UPS. Спустя два месяца после начала продаж решили попробовать этот способ доставки с одним из австралийских заказчиков, так как летать туда каждый раз было слишком дорого. Поместили принтер в ящик и уже через три дня UPS доставила его в Австралию.

Со временем к нам стало приходить все больше людей. Свою роль сыграли также стоимость и качество: $10 тыс. долларов за биопринтер — это не $100 тыс. Если сначала люди думали,

что мы сумасшедшие, то потом стали появляться положительные отзывы о нашем продукте. Фактически мы взлетели благодаря сообществу тканевой инженерии и UPS.

— Сколько времени у вас занимает создание биопринтера, и как часто бывают релизы?

— Для конкретного заказчика срок изготовления принтера составляет примерно шесть недель. А разработка MVP занимает год, иногда два. Мы стараемся делать релизы каждый год, но все зависит от разных факторов. Надо провести большую исследовательскую работу, получить обратную связь от потенциальных пользователей, понять, что сработает, а что нет.

— Почему ваши биопринтеры гораздо дешевле других аналогичных продуктов, представленных на рынке?

— Потому что наша ключевая идея — позволить людям понять, чем полезны биопринтеры, а также вдохновить их на поиск новых идей. Предположим, завтра мы создадим биопринтер, который сможет воспроизводить костную ткань. Можно будет продать его за $500 тыс., а можно и за миллион.

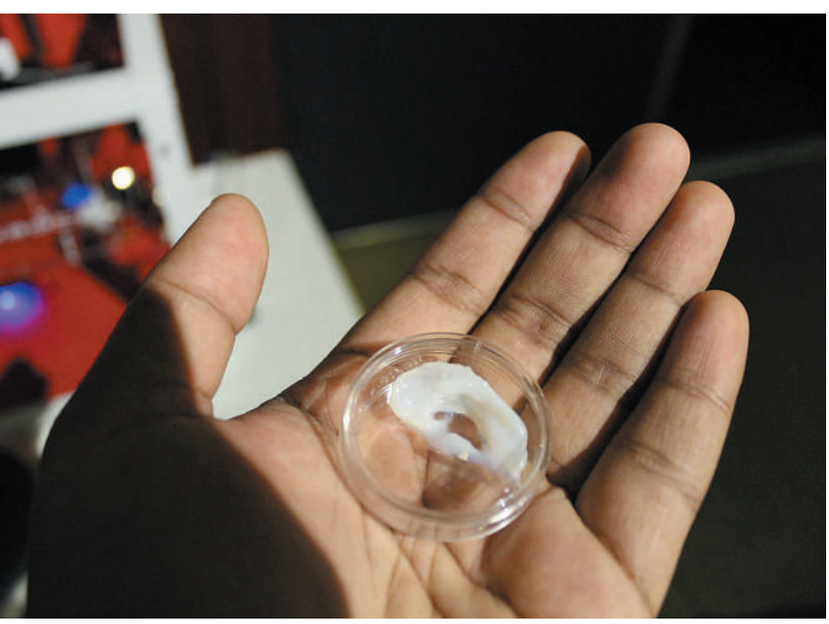
Мы хотим сделать наш продукт привлекательным для рынка. Цена может измениться, так как она зависит от стоимости биочернил и программного обеспечения. Но это не самый важный вопрос. Гораздо важнее — сделать подобные технологии доступными.

— Расскажите о ваших партнерах. Вам интересно сотрудничество с другими стартапами?

— Мы работаем с производителями биочернил для различных типов тканей. Образно говоря, мы как кофемашина Nespresso, которая делает кофейные капсулы и варит кофе: компания покупает кофе различных сортов у Starbucks и Dunkin Donuts, помещает его в специальные капсулы и пропускает через свои машины. Мы тоже покупаем различные типы тканей у других компаний, помещаем их в специальные шприцы и пропускаем через наши принтеры. Так что у нас все почти так же, как в кофейной индустрии.

Наши партнеры знают о биочернилах больше, чем мы. Как правило, они уже какое-то время тестировали свои материалы и получили определенные результаты. Нас это избавляет от необходимости проводить длительные проверки. Мы просто берем то, что нам предлагают, и пропускаем через нашу платформу. В итоге у нас не очень получается производить «кофе», но отлично выходит «пропускать» его через наши «кофемашины». Люди с удовольствием их покупают и быстро «варят кофе» сами, так как наши «кофемашины» просты в использовании.

— Какие материалы вы используете в своей работе и насколько здесь допустимы эксперименты?



Трехмерная модель уха, сделанная на 3D-принтере Allevi.
Фото: 3dprintingindustry.com

— Мы работаем с материалами, которые широко используются в нашей индустрии. Например, с коллагеном. Он позволяет придать клеткам определенную структуру. Также есть искусственно созданные биоматериалы, например, альгиновая кислота, которая очень популярна в биопечати. Мы исследуем, какие материалы уже используются, и думаем, как их структурировать.

— Из чего можно напечатать нос или сердце?

— Пока человечество не создало идеального материала. Мы используем коллаген, но такие органы нельзя никому имплантировать. Пока они создаются только для исследований. Возможно, лет через 5-7 ситуация изменится.

— И сколько стоит напечатать сердце?

— Материал будет стоить примерно $800, а сама печать — примерно $1000. Но пока речь идет сугубо о научно-исследовательской работе. Если со временем внедрить это в медицину, то стоимость увеличится, потому что нужно будет брать образец тканей конкретного человека (чтобы не было отторжения), выращивать новый орган, структурировать, пересаживать его. Но со

временем экономический смысл все равно будет. Например, ребенок, у которого есть медицинская страховка, отрезал себе палец, и страховая компания вынуждена выплатить огромную сумму. В таких случаях имплантация может стоить дешевле. Но это — вопрос будущего.

— Ваш стартап работает на стыке робототехники и биоинжиниринга. Какие задачи стоят перед вами сейчас?

— Вообще самая большая сложность — сделать так, чтобы все работало одинаково хорошо. Чтобы все частицы, из которых состоят другие частицы и из которых состоят третьи, складывались в единую систему и давали хороший результат. Это настоящий вызов! Забавно, но иногда какой-то компонент работает лучше, чем другой и нужно искать идеальный баланс. Например, принтер работает лучше программы, но сам не использует всех возможностей чернил. И ты всегда это чувствуешь. Как в симфоническом оркестре: если одному из музыкантов медведь на ухо наступил, провальной сделается вся композиция. Если какая-то часть системы будет лучше, а какая-то хуже, то результат получится так себе. Ключевая вещь для нас — убедиться, что все синхронизировано и сбалансировано. Это очень важно.

Вторая важная вещь — ответить на вопросы: для чего нужен биопринтер? Кому он может быть полезен? Как его использовать для производства, а не только для науки? Мы ищем ответы на них каждый день.

— Расскажите о своей команде. Как вам удалось наладить все бизнес-процессы, организовать производство?

— У нас молодая растущая команда, всех членов которой объединяет общая цель. Мы используем Agile-методологию, но не в чистом ее виде. Каждую неделю собираемся и обсуждаем, чего достигли за прошедшие семь дней, чего не достигли и почему, делимся друг с другом планами, а также говорим о многих ключевых вещах. Например, о бюджете, так как очень важно, чтобы проекты не выходили за его рамки. Кроме того, мы определяем сильные и слабые стороны продукта, чтобы укрепить более слабые позиции – если программа сработала лучше, чем «железо», начинаем уделять больше вниманию совершенствованию оборудования.

Идет постоянное балансирование между целями, бюджетом и временными рамками. Последнее очень важно для привлечения инвесторов: если вы можете четко предсказать и обосновать, каких результатов достигнете через полгода или год, это повысит вашу привлекательность для инвестиций. Если ваши предсказания сбываются через полгода, то высока вероятность, что они сбудутся и через пять лет. Предсказуемость — огромная ценность стартапа. ▮

Автор интервью: Юлия Нехай

Приложения для бизнеса, которые упростят вам жизнь

Пакет Office 365 включает не только инструменты совместной работы, необходимые любой современной компании, но и набор облачных сервисов корпоративного уровня на мощностях Microsoft. С Office 365 вам больше не нужно развертывать и обслуживать локальные серверы, закупать программное обеспечение и содержать штат ИТ-специалистов.

Остановимся на некоторых приложениях продукта, о которых, возможно, вы не знали: бесплатная корпоративная связь, планировщик задач, корпоративная почта, чат, сервис онлайн-бронирования.

Евгений Андрейчук, эксперт Softline по решениям Microsoft, рассказывает, что же еще умеет Office 365

Teams — единое пространство для совместной работы

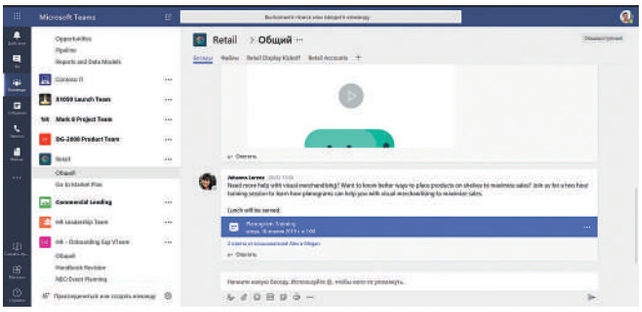
Teams создан для командной работы. Он не только объединяет в себе функционал знакомого всем Skype for Business (аудио и видеозвонки, чат, онлайн-конференции), но включает еще множество других полезных функций — встречи, совместная работа с документами, хранение файлов и пр. Teams поможет снизить расходы на корпоративную связь и повысить операционную эффективность.

1. Чат и обмен файлами

Хорошая альтернатива электронной почте для коммуникаций с коллегами. Есть возможность создавать или вступать в разные беседы/команды: чат с бухгалтерией, маркетингом или с директором для обсуждения важной задачи.

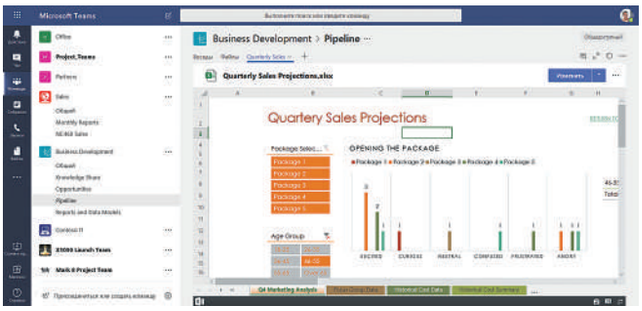
В любой беседе можно:

- совместно редактировать и согласовывать документы прямо в приложении;
- проводить собрания с участниками;
- совершать аудио или видеозвонки;
- обмениваться файлами;
- упоминать конкретного человека с помощью символа @;
- ставить like и отправлять стикеры или gif-ки.



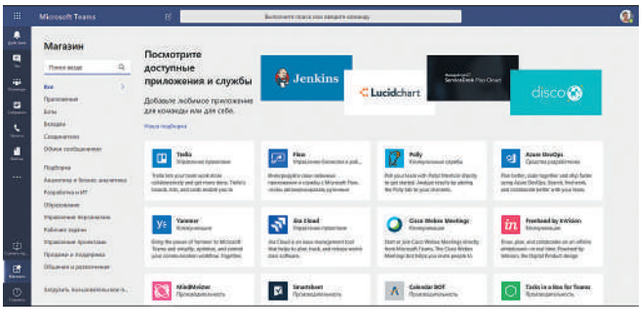
Это особенно удобно, если нужно поддерживать коммуникацию со всеми коллегами в нескольких офисах. Кроме того, в Teams есть удобный поиск по сообщениям, документам, а также облачное хранилище размером 1 ТБ.

2. Совместная работа с документами



Встроенные Word, Excel, PowerPoint, Power BI позволяют открывать файлы прямо из приложения. Кроме того, в Teams интегрируется около 140 сторонних сервисов: Adobe, Jira, Twitter, GitHub, Evernote, Trello, RSS-каналы и др. Это удобно и экономит массу времени — в едином интерфейсе можно совместно с коллегами работать над всеми необходимыми документами.

3. Подключение внешних подрядчиков / партнеров



Гостевой аккаунт позволяет ускорить работу над проектом, пригласив в команду Teams внешних партнеров или клиентов.

4. Бесплатная корпоративная связь

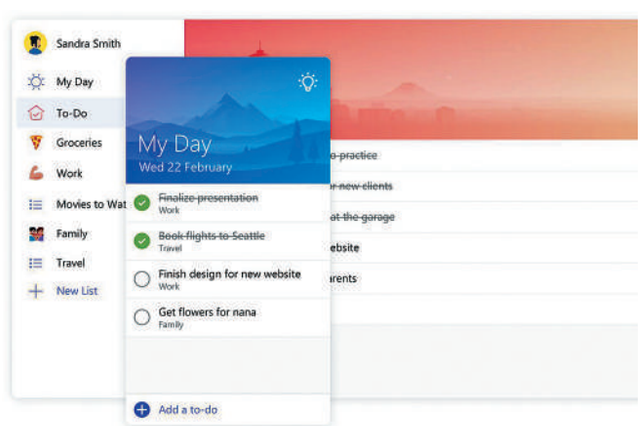
Teams поможет экономить на звонках. Аудио-, видеозвонки, презентации, онлайн-конференции, запись видео — все это доступно бесплатно из любой точки земного шара, главное, чтобы там был доступ в интернет. Вы сможете подключиться к видеоконференции с помощью телефонного звонка, даже если находитесь в пути. Функция записи разговоров поможет в любое время воспроизвести записанные аудио- или видеоматериалы.

5. Чат с ботом

В Teams можно использовать различные внешние службы в виде ботов. Бот умеет не только отвечать на вопросы и предоставлять необходимую информацию в канале, но и работать в роли члена команды.

To-Do — управление личными делами

Приложение помогает упорядочить личный и рабочий список дел. В To-Do можно создавать задачи по категориям (работа, учеба, покупки и др.), планировать дела, расставлять приоритеты.



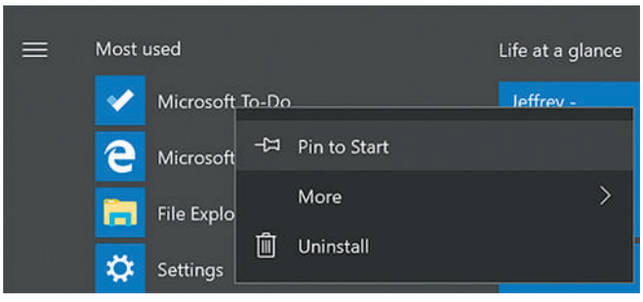
microsoft.com

1. Своевременное выполнение задач

Большинство из нас страдают от информационной перегрузки и постоянно крутят в голове вопросы «Что сейчас важно и срочно?», «Что я буду делать сегодня?» В To-Do можно самостоятельно определить список дел на текущий день и добавить их в список «My Day». Также в приложении есть специальный алгоритм, который предлагает подходящее время для выполнения той или иной задачи. Это особенно удобно, если не хватило времени выполнить какой-либо пункт из вчерашнего списка. ▮

2. Синхронизация данных с Outlook

To-Do полностью синхронизирован с Outlook. При работе в почте сразу, как только ставится новая задача, она тут же отображается в To-Do. Любую задачу из приложения можно легко превратить в сообщение и отправить коллегам по e-mail, указав срок выполнения. И для этого не нужно переключаться на другие системы — все в одном интерфейсе.



microsoft.com

Приложение To-Do синхронизирует данные на смартфоне и компьютере, поэтому список дел всегда под рукой. Задачи можно добавлять прямо в пути, не боясь забыть о чем-то важном.

3. Напоминания в плитках Windows 10

Любую задачу легко можно добавить в список живых плиток Windows 10. Благодаря этому все задачи находятся под рукой в реальном времени.

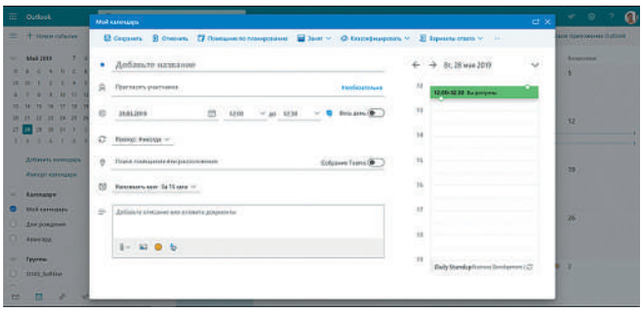
Outlook — не просто почта

Многие используют в своей работе почтовый клиент Outlook. Этот продукт не только работает с электронными письмами, но и имеет множество других полезных функций.

1. Планирование встреч

В разделе «Календари» почтового сервиса Outlook можно быстро создать встречу или мероприятие. Перед созданием собрания достаточно проверить расписание участников, занятость места для проведения или наличие другого необходимого ресурса, а потом выбрать подходящее время.

Сервис Outlook позволяет создать общий календарь, где будет отображаться расписание всех коллег или других ресурсов (переговорных, компьютеров, конференц-залов и пр.), и, кроме того, отдельный календарь для личных встреч. При этом есть возможность просматривать все календари одновременно, что ускорит планирование.



Представителям международной компании, иногда требуется забронировать сразу несколько переговорных комнат в разных частях города/страны. В «Календарях» Outlook можно просмотреть доступные варианты и зарезервировать переговорные.

2. Постановка задач коллегам

Работа с задачами — одно из наиболее ценных свойств почтового сервиса. Outlook позволяет назначать задачи не только самому себе, но и коллегам по работе. При этом легко можно следить за статусами их выполнения: сотрудник видит новую задачу, приступает к работе, добавляет в нее необходимую информацию, меняет статус.

Planner — помощник в управлении задачами

Планировщик позволяет ставить задачи и распределять их между коллегами, управлять маркетинговыми активностями, формировать диаграммы для отслеживания прогресса.

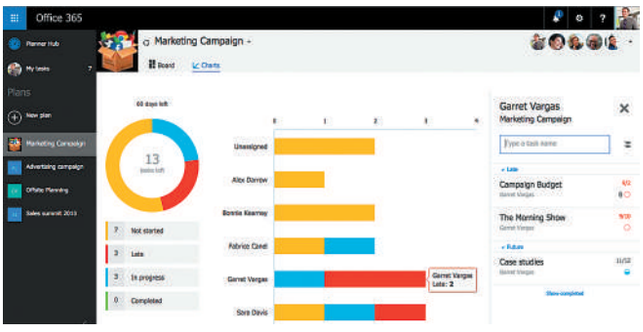
1. Работа с задачами

С планировщиком легко систематизировать все задачи. Каждую из них можно назначить либо на конкретного человека, либо на группу людей, а потом отслеживать прогресс ее выполнения. К задаче можно прикреплять необходимые файлы, добавлять комментарии, цветовые метки и назначать статусы («Не начато», «Выполняется», «Завершено»).

Сотрудник не пропустит важное сообщение от руководителя — при появлении новой задачи он увидит уведомление на почте.

2. Визуализация данных

Визуализация процесса выполнения задач — одна из наиболее ценных функций планировщика. С ее помощью можно просматривать как общую картину всех проектов, так и ход реализации конкретной задачи. Наглядные диаграммы всегда продемонстрируют, сколько задач в работе, какие из них просрочены, кто из сотрудников отстает, а кто свободен для нового проекта.



microsoft.com

3. Интеграция Planner

На досках в Planner можно размещать текстовые документы Word, таблицы Excel, записи из OneNote. Если в них вносятся изменения, то правки автоматически синхронизируются со всеми документами. Кроме того, при создании новой задачи в онлайн-хранилище планировщика автоматически создается новая папка, новая записная книжка в OneNote, запись в календаре и переписка в Outlook.

Bookings — сервис онлайн-записи

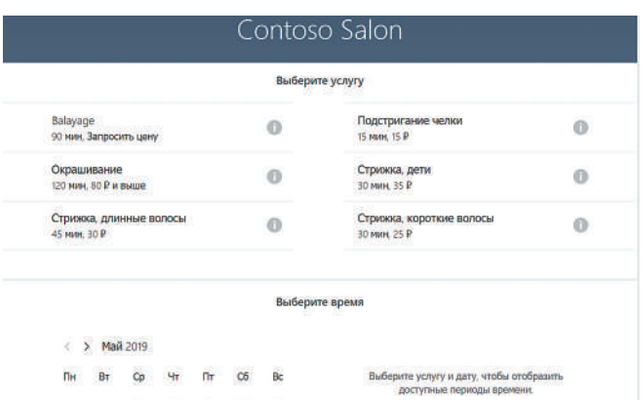
Планирование встреч по телефону – весьма трудоемкий процесс. Во-первых, звонки отнимают много времени. Во-вторых, каждый пропущенный звонок может означать потерянного клиента. Bookings — доступная альтернатива телефонным звонкам. Сервис позволяет создавать страницы онлайн-записи для клиентов. Это может быть визит в банк, в салон красоты, к стоматологу и пр.

Страницу бронирования Bookings можно интегрировать на сайт или добавить на бизнес-страницу Facebook. А можно просто отправить клиентам в виде прямой ссылки, что особенно удобно для небольших компаний, не имеющих собственного сайта.

Подводя итог, отмечу основные выгоды приобретения пакета Office 365:

- Совместная работа всей команды в единой экосистеме.
- Доступность с любых устройств из любого места.
- Автоматическое бесплатное обновление всех приложений.
- Удобная ежемесячная оплата (тарифы можно посмотреть на сайте office365.softlinecloud.by).
- Мощные встроенные функции безопасности.

Попробуйте бесплатный тестовый период и протестируйте работу Office 365 в течение 30 дней. ▮



microsoft.com

Евгений Андрейчук,
руководитель направления по продаже решений Microsoft в странах Восточной Европы и Центральной Азии:
+375(17)336-55-95, доб. 4474
Evgeniy.Andreychuk@softline.com

Компания Softline помогла Mercedes-Benz усовершенствовать бизнес-процессы

О проекте

Отрасль: Автомобильный бизнес

Задача:

- лицензирование пакета приложений Microsoft Office;
- повышение эффективности коммуникаций между сотрудниками.

Решение: Сервисы Office 365

Результаты:

Повышение продуктивности сотрудников, оптимизация бизнес-процессов благодаря единому рабочему пространству с повышенной системой безопасности.

О компании

ООО «Автомобильный дом «Энергия ГмбХ» является дистрибьютором Daimler AG в Беларуси и обладает правами на представление брендов Mercedes-Benz, Mercedes-AMG, Mercedes-Maybach, Setra на белорусском рынке. Помимо поставки автомобилей, компания оказывает услуги по их ремонту и сервисному обслуживанию.

Задача

В современной компании сотрудникам уже недостаточно одного устройства для обеспечения эффективной работы. Точно так же обстоят дела с количеством используемых сервисов и приложений. Один пользуется онлайн-сервисом для совместного редактирования документа, другой делится файлами через облачное хранилище, третий предпочитает переписываться и отправлять документы коллегам и партнерам в мессенджерах. Разнообразие сервисов снижает продуктивность и становится одним из источников проблем в коммуникациях.

Такая ситуация была и у Автомобильного дома «Энергия ГмбХ». Работа с договорами, запросы необходимых сертификатов для клиентов и прочие задачи – инженеры постоянно на связи с отделом продаж и другими офисными специалистами. Чтобы оптимизировать эти процессы руководство компании обратилось к специалистам компании Softline с просьбой наладить обмен информацией между сотрудниками. Также автомобильному дому требовалось лицензировать офисные приложения Microsoft и внедрить современную почтовую систему корпоративного уровня.

Решение

Специалисты Softline предложили заказчику рассмотреть облачные решения Office 365 и продемонстрировали их возможности, в том числе: новейшие версии офисных приложений, корпоративную почту, внутренний портал, инструменты для совместной работы, бесплатные звонки, собрания и многое другое. Решающими факторами для выбора Office 365 стали широкая функциональность продукта, его стоимость и масштабируемость.

В рамках проекта Автомобильный дом «Энергия ГмбХ» произвел миграцию на новую службу электронной почты Exchange, одним из основных преимуществ которой является расширенная защита информации. Специальные инструменты блокируют вредоносные программы и нежелательную почту, а платформа шифрования предотвращает утечку конфиденциальных сведений. Встроенные в службу календари, контакты и облачное хранилище доступны для совместного использования и позволяют быстро и легко планировать встречи, делиться документами. Гарантия бесперебойной работы почтового сервиса обеспечивает дополнительную отказоустойчивость ИТ-инфраструктуры.

Встречи с клиентами и партнерами, выезды в сервисные центры – многие сотрудники заказчика основную часть своего рабочего времени проводят в разъездах. Часто приходится согласовывать и отправлять необходимые документы по сделкам прямо на ходу.

Поддерживать оперативную связь помогает сервис Teams – главный центр командной работы в Office 365. Для быстрой коммуникации специалисты используют чат, где можно совместно обсуждать проекты, согласовывать необходимые документы, проводить собрания, совершать звонки. Благодаря встроенным в Teams офисным приложениям (Word, Excel и др.) редактировать и отправлять актуальные версии файлов стало еще проще и удобнее.

Для многих автовладельцев важно подробно обсудить технические возможности автомобиля, необходимость ремонта, чтобы иметь точное представление о его состоянии. Еще одна ценность сервиса Teams в том, что специалисты Автомобильного дома «Энергия ГмбХ» могут через гостевой аккаунт приглашать внешних партнеров или клиентов в команду Teams, где оперативно обсуждаются возникающие вопросы. Таким образом, повышается лояльность клиентов. А за счет работы в единой экосистеме специалисты экономят свое время: им не нужно переключаться на другие сервисы для решения отдельных задач.

Для упорядочивания документооборота эксперты Softline предложили компании перенести текущее корпоративное хранилище документов и выстроить его структуру в SharePoint. В нем можно безопасно хранить не только внутренние документы, но и все файлы, с которыми сотрудники работают и отправляют друг другу в Teams, Outlook и другие сервисы Office 365. Таким образом, все данные собраны в одном месте и при необходимости сотрудники автомобильного дома могут в любое время к ним обратиться. Это облегчает доступ к важной информации и оптимизирует рабочий процесс.

«Мы подошли к проекту с точки зрения роли сотрудника в организации. Одним специалистам для работы были необходимы офисные приложения, а другим – только сервисы (почта, чат, редактирование документов через браузер и пр.). Мы унифицировали используемые персоналом приложения, сервисы и устройства. Теперь команда работает в единой безопасной среде, и каждый сотрудник использует необходимые для работы инструменты. Это помогло добиться экономии и более низкой стоимости владения сервисами Office 365 по сравнению с локальным размещением отдельного ПО».

Виктор Синяк, менеджер по продажам решений Microsoft в Softline.

Результат

Специалисты Softline помогли заказчику выполнить миграцию, настроить сервисы платформы и обучили персонал основным сценариям взаимодействия с ними. На протяжении дальнейшей эксплуатации решения Softline оказывала компании консультирование и техническую поддержку.

Благодаря использованию единой платформы Office 365 сотрудники Автомобильного дома «Энергия ГмбХ» наладили коммуникации, получили эффективную систему защиты, резервного копирования, а также автоматическое обновление версий офисных приложений. Сервисы Office 365 доступны в любое время, поэтому специалисты компании всегда на связи: они могут оперативно отвечать на запросы, отправлять документы, проверять почту и пр. А если разрядился смартфон или ноутбук, то получить доступ к своим документам сотрудник может и с другого компьютера через браузер. ▮

«Благодаря Office 365 коммуникация стала более комфортной и эффективной. Мы осваиваем новые сервисы и принципы взаимодействия с командой и видим, что сотрудники стали активнее обсуждать проекты, более оперативно реагировать на запросы коллег. Даже удаленно мы можем подключаться к сервисам Office 365 и не прерывать работу. Кроме того, нам удалось оптимизировать затраты на ПО за счет приобретения пакета Office 365 по модели подписки с помесячной оплатой».

Денис Мешкун, специалист по ИТ Автомобильного дома «Энергия ГмбХ».

Azure или гибридная архитектура

как альтернатива SQL Server, Windows Server 2008 и 2008 R2

Последний день обновлений системы безопасности:

9 июля 2019 г.
для SQL Server 2008 и 2008 R2;

14 января 2020 г.
Для Windows Server 2008 и 2008 R2.

С 2019 года компания Microsoft прекращает поддержку и ежемесячные обновления систем безопасности продуктов SQL Server, Windows Server 2008 и 2008 R2, в результате чего эти системы перестанут соответствовать требованиям законодательства и регулирующих органов. Как избежать угроз потери данных и неработоспособности систем на новом оборудовании?

К чему приведет прекращение обновлений систем безопасности?

Компании, использующие продукты без регулярных обновлений системы безопасности, более подвержены кибератакам, в результате которых данные клиентов и бизнес-данные могут быть похищены, а доверие клиентов и уверенность — навсегда утрачены. Прекращение выпуска регулярных обновлений систем безопасности может также повлечь за собой риски правового несоответствия и, как следствие, поставит под угрозу ваши приложения и бизнес в целом.

Есть решение!

Современным компаниям действительно нужна долгосрочная стратегия, включающая непрерывное обновление систем безопасности. Окончание поддержки вышеуказанных систем можно рассматривать как отличную возможность для внедрения инноваций и совершенствования текущей инфраструктуры.

Новейшие версии SQL Server и Windows Server помогут выполнить жесткие требования современных нормативных актов, включая «Общий регламент по защите данных». Запускайте эти серверные системы в Azure, локально или в гибридной среде!

Softline предлагает два сценария

Миграция в Azure. Перенесите рабочие нагрузки в Azure с бесплатными обновлениями безопасности

Softline поможет перенести рабочие нагрузки «как есть» в Azure. Затем вы сможете бесплатно продлить обновления для системы безопасности на 3 года и обновиться до последних версий, когда будете готовы. При этом вы сразу же получите встроенные функции безопасности Azure и более 70 сертификатов соответствия. А благодаря программе «Преимущества гибридного использования Azure» можно сэкономить до 80%, используя существующие лицензии Windows Server и SQL Server (за установку 2008/2008 R2 на Amazon Web Services (AWS) вы заплатили бы в 5 раз больше).
Только в случае переноса SQL Server 2008 в Microsoft Azure вы получаете все преимущества работы в публичном облаке, в том числе экономите на аппаратном обеспечении и администрировании, а также обеспечиваете легкость в масштабировании нагрузки.
Специалисты Softline окажут вам техническую поддержку по любым вопросам в режиме 24/7, обучат и проконсультируют по сценариям миграции, инструментарию, возможным проблемам и их решениям. Наши эксперты проведут обследование существующей инфраструктуры SQL серверов и проверят их готовность к миграции в Microsoft Azure. Данный сценарий предполагает поиск оптимального для данной инфраструктуры и существующих приложений способа миграции; составление детального плана миграции в Microsoft Azure (на виртуальные машины или в управляемые экземпляры баз данных Azure SQL) и перевод всей необходимой инфраструктуры в Microsoft Azure или построение гибридных сценариев.

Обновление до новой версии SQL Server. Модернизируйте локальную версию и запланируйте переход на гибридную систему

Этот сценарий позволяет обновить системы до последних версий и получить современную систему безопасности, улучшенную производительность и более современный функционал. Если вы не успеваете обновить локальные серверы, то тогда можно приобрести расширенные обновления системы безопасности Windows Server или SQL Server 2008 и 2008 R2 на 3 года. В этом случае вам потребуется действующая лицензия Software Assurance или лицензия на подписку по соглашению Enterprise Agreement.
Такой способ подходит тем, у кого есть ограничения на использование публичного облака. Он полностью совместим с SQL Server 2008, и для его реализации применяются отработанные процедуры обновления. К преимуществам этого сценария также можно отнести возможность увеличения производительности работающих приложений в среднем на 10-15% и использования сквозного шифрования, мобильной бизнес-аналитики, инструментов машинного обучения. Новый SQL Server доступен на Linux и контейнерах Docker.

Специалисты Softline обучат и проконсультируют вас по сценариям перехода и инструментарию, проведут обследование текущей инфраструктуры SQL серверов и найдут оптимальный для данной инфраструктуры и существующих приложений способ перехода. В данный сценарий также входит составление детального плана перехода на SQL Server 2017 и его тестирование; поставка (при необходимости) лицензий нового SQL Server и аппаратного обеспечения; перевод всей инфраструктуры на новую версию SQL Server.

Наши технические специалисты всегда на связи и готовы помочь с выбором.
Просто напишите нам - и мы подробно расскажем о преимуществах каждого способа:

Андрей Андреев, менеджер по развитию бизнеса, Softline CIS
Andrey.Andreev@softline.com

МОЩНАЯ АНАЛИТИКА

Бизнес-аналитика – это один из ключевых инструментов управления компанией. Без современных средств анализа данных велик риск упустить прибыльных клиентов, неправильно определить направления развития и нерационально расходовать средства. О лидере рынка систем Business Intelligence — комплексном программном решении Microsoft Power BI – рассказал Станислав Воронин, руководитель отдела внедрений BI-систем компании Softline.

– Станислав, как Power BI помогает организациям работать с данными?

– Power BI – это инструмент для самостоятельного анализа данных. Работая с ним, можно подключать неограниченное количество источников информации, быстро строить гипотезы на основе данных и проверять их, запрашивать и визуализировать отчеты. Все это помогает быстро принимать правильные для бизнеса решения.

Так или иначе данные сегодня собирают все – это основа эффективного бизнеса. Наиболее частым инструментом для этого служит Excel, где пользователи привычно работают с таблицами и листами. Если специалист хорошо владеет Excel, ему не составит никакого труда начать использовать Power BI так, как будто это решение сопровождало его всю жизнь. Его интерфейс прост и удобен несмотря на широкую функциональность продукта, а возможности визуализации действительно впечатляющие.

Несомненно, ключевой плюс Power BI – это легкая интеграция со множеством систем. Коннекторы с таблицами баз данных, web-ресурсами, системами типа Salesforce, CRM, хранилищем OneDrive, приложениями Dynamics и др. значительно упрощают получение данных из информационных систем и их анализ.

– Какие конкретные задачи организации решают с его помощью?

– Power BI создает серьезную аналитическую базу для исследования и прогнозирования проблем бизнеса. А как известно, что предсказуемо, то предотвратимо, поэтому выводы, своевременно сделанные на основе актуальной информации, позволяют находить эффективные решения. В современных условиях, чтобы оставаться конкурентоспособными, приходиться контролировать множество мелких деталей, за которыми человек уже не в состоянии уследить, и аналитические службы в этом смысле наш главный помощник.

Power BI справляется с любыми задачами, которые связаны с обработкой данных. Например, если говорить о продажах, то такие запросы, как «сколько товара продано», «группы основных покупателей», «какая продукция пользуется спросом в этом месяце», «какие товары ухудшили свои позиции по сравнению с прошлым годом», «какова структура канала сбыта» – для него стандартны. Отчеты по ним предоставляются на информационных панелях в виде наглядных и стильных визуализаций. По ним можно проследить как общие закономерности, так и детализировать информацию в разрезе контрактов, покупателей, номенклатурных групп или конкретных позиций, цен, рынков, каналов распределений и т.д.

Для сферы HR, например, ценны такие данные, как общая численность сотрудников, текучесть кадров, производительность труда, сколько женщин в компании, мужчин, людей предпенсионного возраста, какая у них зарплата, какие подразделения загружены больше, какие меньше и т.д. Располагая компактным отчетом, основанном на оперативно обновляющихся сведениях, легче принимать грамотные кадровые решения.

Также и в любой другой сфере – логистика, ИТ, производство, маркетинг, финансы и др. – можно выстроить мощный аналитический аппарат с Power BI.

– В каких отраслях Softline уже реализовывала проекты по внедрению Power BI?

– Проектов было достаточно много, более 50, потому что продукт востребован и на сегодняшний день является лидером BI-систем. Microsoft активно его развивает и дорабатывает, поэтому с каждым днем он становится все более удобным и производительным. Мы реализовывали проекты для блоков продаж в пищевой промышленности, телеком-сфере, оптовой дистрибуции и др. На данный момент работаем над проектами для ритейл-компании в Новосибирске и крупной английской фармацевтической компании.

– Как начать работать с Power BI?

– Сделать это можно легко, просто и быстро. Достаточно скачать бесплатную версию Power BI Desktop, которая полнофункциональна с точки зрения подключения к источникам данных и формированию моделей и отчетов. Установив программу, в систему следует загрузить источники информации, подключить к базам данных. После этого вы сразу же сможете получать первые отчеты и выстраивать визуализации. В интернете в открытом

Когда дело касается крупных компаний со сложной инфраструктурой, где с одной стороны, множеству сотрудников требуется доступ к одной и той же информации, а с другой – разным отделам требуется свой специфический набор данных, необходима помощь специалистов, которые смогут оптимальным образом выстроить архитектуру решения.

доступе много информации о работе с этим инструментом как для новичков, так и для продвинутых пользователей.

Power BI создает серьезную аналитическую базу для исследования и прогнозирования проблем бизнеса. А как известно, что предсказуемо, то предотвратимо, поэтому выводы, своевременно сделанные на основе актуальной информации, позволяют находить эффективные решения.

– Что делать, если систему аналитики необходимо масштабировать?

– Когда в компании возникает потребность делиться отчетами или коллективно над ними работать, приобретается лицензия Power BI Pro. Эта подписка дает возможность публиковать отчеты на портале, настраивать расписание их обновлений, предоставлять доступ пользователям или отбирать его, создавать рабочие области. Так в Power BI образуется корпоративная среда. Многие компании начинают использование системы именно с такого формата.

Если объем обрабатываемых данных начинает значительно расти, то целесообразно перейти на подписку Power BI Premium. В ее рамках в облаке Azure резервируются мощности и снимаются ограничения на объем моделей, которые используются в отчетах. Такой расширенный вариант с поддержкой больших данных максимально эффективен и производителен.

В случае если заказчики не готовы отправлять свои данные в облако, то возможности данной подписки позволяют развернуть локальное решение Power BI Report Server. Или же у компании должен быть приобретен Microsoft SQL Enterprise. Он включает в себя ту же функциональность и может быть развернут на серверах компании.

– Какие услуги по части бизнес-аналитики Power BI Softline оказывает клиентам?

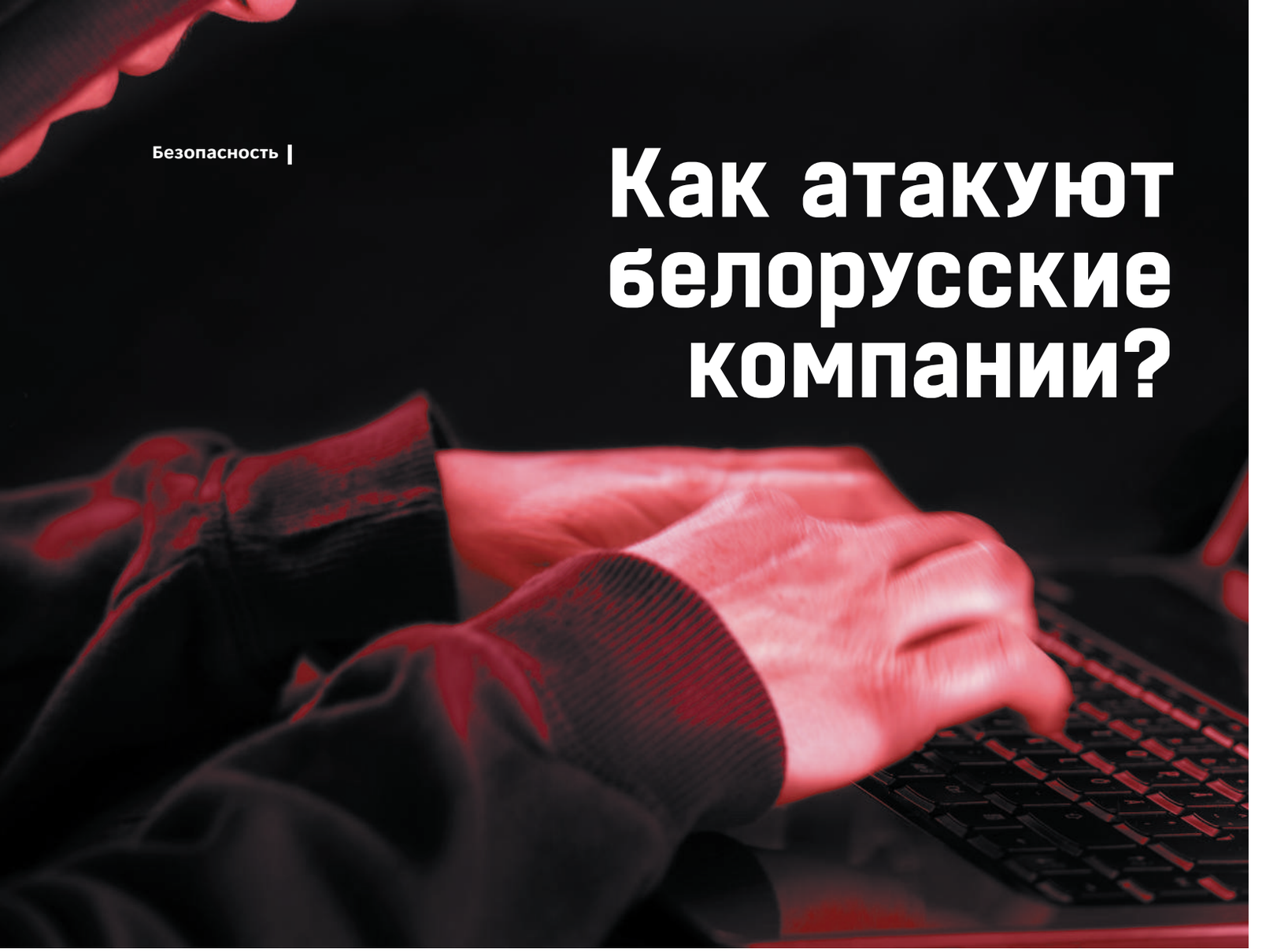
– Конечно, любой пользователь может легко и бесплатно начать использовать Power BI. Однако, когда дело касается крупных компаний со сложной инфраструктурой, где с одной стороны, множеству сотрудников требуется доступ к одной и той же информации, а с другой – разным отделам требуется свой специфический набор данных, необходима помощь специалистов, которые смогут оптимальным образом выстроить архитектуру решения.

Предположим, для отдела продаж какой-либо организации нужно наладить доступ к информации, касающейся закупок, отгрузок, объема сбыта и т.д. Наша задача – исследовать все источники данных и подключить необходимые системы, для того чтобы наполнить аналитическое хранилище. Затем важно заложить определённую логику расчетов и стандартизировать работу с информацией путем формирования оптимальной витрины данных и настройки отчетов. Таким образом мы предоставляем заказчику уже готовую для работы систему.

Команда Softline берет на себя ответственность за настройку Power BI соответственно задачам клиента. Ему остается только подключиться и пользоваться возможностями службы во благо развития своего бизнеса.

Power BI

Как атакуют белорусские компании?



О том, в каком направлении в настоящее время чаще всего ведутся кибератаки, а также о наиболее слабых местах многих современных компаний рассказал руководитель направления информационной безопасности отдела консалтинга компании Softline Александр Дубина.

— Много ли белорусских компаний атакуют хакеры? Таких инцидентов становится больше или меньше? С чем это связано?

— На белорусские компании происходит много нападений. Причем инцидентов становится все больше. Согласно аналитическим данным, в январе — августе 2019 года количество кибератак увеличилось примерно вдвое по сравнению с аналогичным периодом 2018.

К сожалению, статистика учитывает киберпреступления в целом. Например, передача пароля в соцсети «ВКонтакте» и получение доступа к чужому профилю — это тоже киберпреступление, но оно не относится к атакам на бизнес.

Получить статистику о масштабных хакерских атаках на компании затруднительно еще и потому, что атакованные структуры зачастую пытаются скрыть данный факт, ведь он влечет за собой репутационные потери, а в случае принятия проекта закона «О персональных данных» — еще и ответственность.

На увеличение количества атак влияет и рост интереса к ИТ-сфере в целом и кибербезопасности в частности. Появляется все больше новостей, связанных с данной темой. Чем больше информации и интереса, тем больше людей начинают заниматься этим направлением.

Количество атак увеличивается во время каникул и праздников. Следовательно, в данной сфере пробуют себя совсем юные дарования. Зачастую это просто баловство, желание проверить собственные силы, а не стремление получить денежное вознаграждение.

— Какие сферы наиболее часто подвергаются атакам?

— Раньше это была сфера финансов. И, разумеется, интерес к ней сохранится. Однако теперь банки и финансовые структуры принимают серьезные меры для защиты своей инфраструктуры, финансов и транзакций клиентов, что значительно осложняет жизнь злоумышленников. Сегодня нужно иметь очень высокую квалификацию, чтобы атаковать банки.

Кроме того, любой взлом имеет свою цену. С точки зрения трудоемкости атаки и финансовых вложений для ее организации банк и фирма с двумя компьютерами — это две совершенно разные структуры.

По этой причине злоумышленники переключились на другие сферы. Сегодня наблюдается резкий всплеск атак на промышленные сети. В частности, это касается автоматизированных систем управления технологическим процессом (АСУ ТП). Взламываются не серверы, а оборудование, на котором завязаны производственные процессы. Это тревожный тренд, поскольку данная сфера уделяла мало внимания кибербезопасности. Сегодня ситуация активно исправляется, однако, если учесть масштабы, данный процесс не может быть быстрым, ведь даже производители программного обеспечения не подошли к защите технологических сетей глобально.

В настоящее время этот сегмент остается спорным, поскольку такие сети, как правило, изолированы, то есть не имеют доступа к интернету. Ранее считалось, что их взлом невозможен. Однако, как только в данной сфере стали глубже разбираться именитые поставщики программного обеспечения из СНГ, оказалось, что это совсем не так.

Сейчас кибербезопасности промышленных сетей уделяется много внимания, ведь если злоумышленник получит доступ к управлению технологическим процессом в компании, выпускающей, например, химическую продукцию, его действия могут быть чреваты техногенной катастрофой.

Взлом технологической сети — это далеко не простая задача, тем не менее данная сфера все больше интересует злоумышленников.

Еще один интересный для киберпреступников сегмент — средний и малый бизнес. Субъекты МСП, как правило, вообще не беспокоятся об информационной безопасности. Поэтому злоумышленникам гораздо проще получить более скромную выгоду от небольшой компании, чем пытаться взломать банк и, скорее всего, быть пойманными.

— С какой целью чаще всего атакуют белорусские компании?

— Злоумышленники могут не просто проверять свои силы и возможности, но и собирать, например, важные данные. Чаще всего киберпреступники, завладевшие информацией компании, не пытаются требовать выкуп, а просто продаютукраденные данные в соответствующих кругах.

Жертвой взлома может стать любой человек, даже если сам по себе он не интересен. Собственно говоря, в основном так и получается. Дело в том, что злоумышленники тоже люди и стараются найти наиболее простые пути для достижения своей цели. Если проанализировать громкие атаки, которые совершались в мире, то окажется, что хакеры взламывали крупные компании через их контрагентов. Например, большую корпорацию обслуживает страховая компания. Значит, проще взломать именно эту компанию и через нее проникнуть в корпорацию.

— Каковы самые распространенные уязвимости компаний?

— Проблема наших компаний (к счастью, она начала решаться) — лицензирование программного обеспечения.

Обновленная операционная система играет важную роль с точки зрения защиты, равно как и лицензионный антивирус, сертифицированный по нашему законодательству. Это необходимый минимум, ведь глобальные атаки распространяются очень быстро. Понятно, что если мы скачали где-то «ломаный» антивирус со старой базой данных, которую неизвестно когда обновим, то подвергаемся большому риску. А база данных лицензионных антивирусов обновляется чуть ли не каждый час.

— Укрепление информационной безопасности стало трендом в нашей стране?

— На рынке информационной безопасности во всем мире наблюдается резкий подъем. К 2020 году он достигнет $1 трлн. Так или иначе, все понемногу идут в этом направлении. Насколько быстро – зависит от сферы деятельности и размеров компании.

Многие заказчики уже по-другому смотрят на цену лицензионного ПО и считают ее оправданной. Приходит понимание того, что это необходимо. Если сравнить то, что мы, как компания-интегратор, предлагали клиентам три года назад, и то, что предлагаем сейчас, разница

окажется весьма значительной. Постоянно появляются новые разработчики программных продуктов и новые методы защиты.

— Какие сектора в Беларуси активнее всего занимаются своей защитой? Чем это обусловлено?

— Государственный сектор уделяет особое внимание вопросу ИБ, особенно с учетом подписания Концепции об информационной безопасности. Это был хороший толчок, с точки зрения реагирования рынка. И компании, и регуляторы серьезно отнеслись к данному вопросу.

Радует, что многие организации начали осознавать важность информационной безопасности, благодаря чему рынок движется. Чем больше людей вовлечены в эти процессы, тем лучше для каждой компании и страны в целом.

Несмотря на активность госсектора, уровень обеспечения информационной безопасности там не всегда такой, как хотелось бы. Причина: необходимые решения далеко не дешевы и выделить на них деньги иногда проблематично.

Ситуация в частном секторе несколько стихийная. Довольно часто компании не принимают меры до тех пор, пока не появятся проблемы.

Для того чтобы подсчитать, сколько средств следует выделить на информационную безопасность, фирма должна ответить на вопрос: сколько стоит один день простоя? Получить точный ответ у некоторых клиентов довольно трудно.

Остановить работу компании на один день относительно легко, поэтому нужно думать не о том, взломают ли ее, а когда и как это произойдет.

— Каковы перспективы рынка информационной безопасности в Беларуси?

— Думаю, в ближайшее время нас ожидает еще один рывок вперед, который затронет частные компании. Он будет связан с проектом закона «О персональных данных» и совершенствованием законодательства в этой сфере, а также с выходом Концепции информационной безопасности.

Важную роль играет ответственность. В наших кошельках лежат различные скидочные карты магазинов. Чтобы получить их, необходимо заполнить анкету. Мы указываем в ней имя, фамилию, электронную почту, номер телефона и другую информацию — это уже персональные данные. Защита этих сведений — направление, которое будет активно развиваться после принятия закона «О персональных данных».

— На что нужно обращать внимание компаниям при защите своих данных?

— Зависит от компании. Если говорить в целом, то необходимо обучить сотрудников основам безопасной работы с системой, почтой и т. д. Обычно мишенью при взломах компаний становятся рядовые сотрудники: экономисты, юристы, бухгалтеры и другие специалисты.

Классический пример — взлом через почту. Приведу одну из реальных ситуаций. Юристу пришло письмо с резюме из непонятного источника. Поскольку это не его тема, он не стал разбираться и переслал резюме в HR-отдел. Кадровик получил информацию уже из достоверного источника и открыл письмо, которое оказалось шифровальщиком. В результате важная для компании информация была потеряна.

Злоумышленники очень хорошо подходят к вопросу социальной инженерии и, если возьмутся за компанию, проанализируют ее от а до я. Поэтому необходимо обучать своих сотрудников, разрабатывать инструкции по работе с персональным компьютером, интернетом и входящими файлами.

Нужно быть внимательным с тем, что вы выбрасываете в мусорную корзину. Зачастую в урне возле офиса можно найти много интересной информации о лицах, которые подписывают документы, бланки с оттисками печати, а также другие данные, которые облегчат злоумышленникам задачу. ▮

Интервью для газеты «Белорусы и рынок»

kaspersky.ru/business

Твоя сеть.
Твои правила.

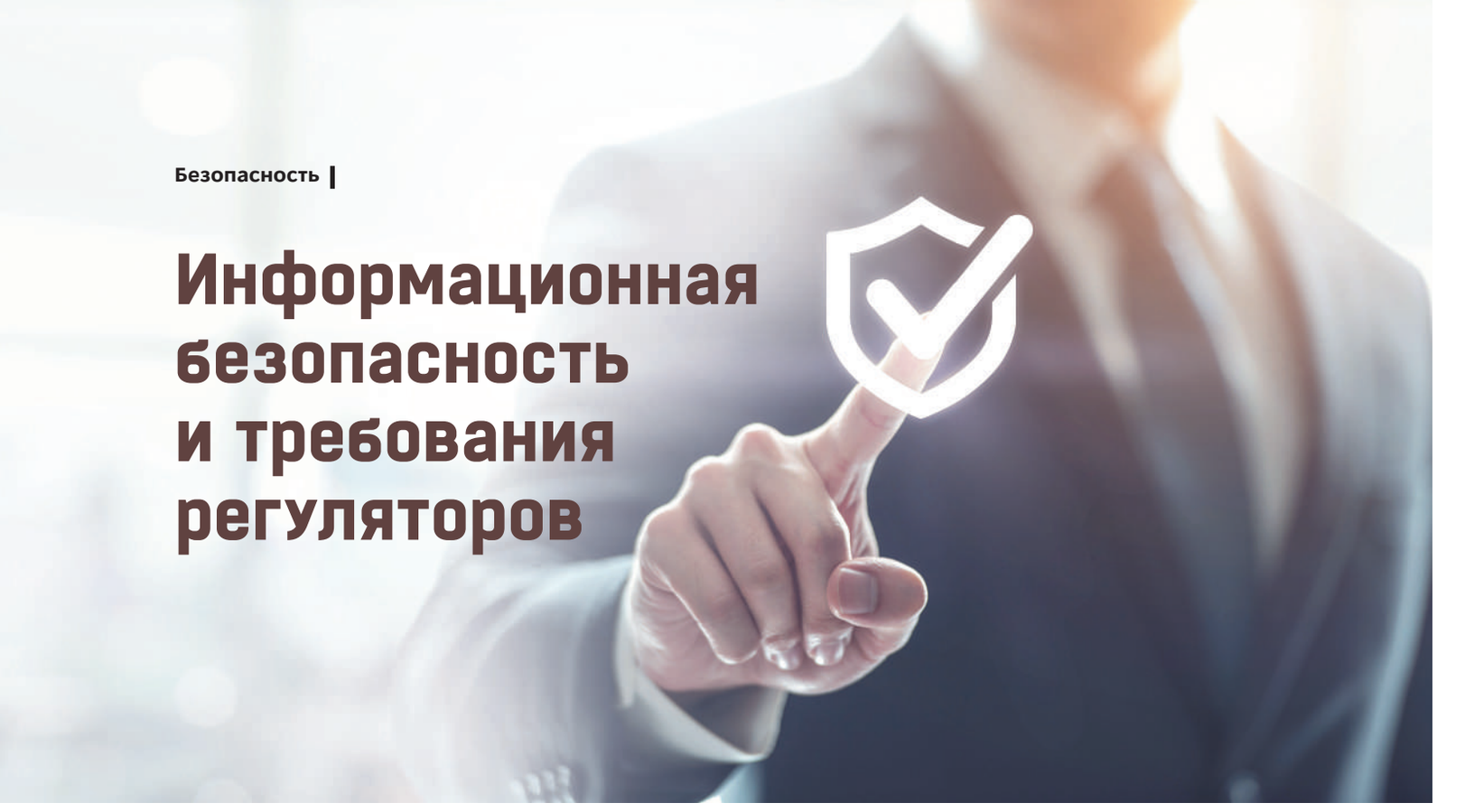
Гибкая защита — для растущего бизнеса.
Kaspersky Endpoint Security для бизнеса Универсальный защитит виртуальные и физические рабочие места в любом их соотношении и поддержит ваши планы по развитию корпоративной IT-инфраструктуры.

Kaspersky®
Endpoint Security
для бизнеса
Универсальный

kaspersky

Получить консультацию по продуктам Лаборатории Касперского вы можете у эксперта Softline:
Виталий Шавель,
+375 (17) 336-55-95 доб.4440
Vitaliy.Shavel@softline.com

Информационная безопасность и требования регуляторов



Специалист по информационной безопасности Softline Дмитрий Сугако рассказал об особенностях обеспечения информационной безопасности в Беларуси и ключевых направлениях Softline в этой области.

— Кто такие регуляторы и почему так важно соответствовать их требованиям в сфере ИТ-безопасности?

— Регулятором является государственный орган, который контролирует деятельность по обеспечению защиты информации от утечки и несанкционированных действий. Речь идет о данных, составляющих государственную тайну, или сведениях, охраняемых в соответствии с законодательством. У нас в стране функцию регулятора выполняет оперативно-аналитический центр при президенте Республики Беларусь (ОАЦ).

Если взглянуть на предъявляемые требования, то они вполне логичны. Для обеспечения защиты вышеупомянутой информации важно обеспечить выполнение ряда правовых, организационных и технических мер. Это касается и защиты персональных данных.

— Как сейчас обстоят дела с выполнением требований? Какие иллюзии существуют у компаний на этот счет?

— Ситуация не самая лучшая, но процесс идет. В некоторых компаниях система защиты уже построена и даже настроена максимально приближенно к требованиям, но используется несертифицированное оборудование, ПО и т.д. В других – не отражены требования к настройке в локальных нормативно-правовых актах организации.

Многие ИБ-специалисты и руководители считают, что соблюдение требований – это формальность, а основная защита заключается в использовании программно-аппаратных решений. На самом деле регламентирующие документы важны для создания действительно надежной системы информационной безопасности. К примеру, если злоумышленник получит конфиденциальные данные через сотрудника компании, то в этом случае программное решение не сработает.

Чтобы качественно защитить корпоративный периметр, нужен комплексный подход, который подразумевает использование не только программных средств защиты, но и разработку документов по информационной безопасности и совершенствование ЛНПА организации. Это процесс не одного дня, месяца и даже года.

— Что такое комплексные системы защиты? Какую защиту они обеспечивают? Почему и за счет чего окупаются существенные расходы на закупку таких систем?

— Главная задача комплексного подхода – оптимизация всей системы в совокупности, а не улучшение отдельных ее частей. Комплексные системы включают целый ряд средств, направ-

ленных на защиту информации от различного рода атак (вирусных, хакерских и т.д.), обеспечение сохранности данных при физической утрате и поломках информационных носителей, создание безопасного доступа к хранимым ресурсам, восстановление информационной системы в случае повреждений.

Надо понимать, что система защиты – это не только совокупность программных средств, но и разработанные, внедренные локальные нормативно-правовые акты организации. Стоимость таких систем не должна превышать стоимости той информации, которая обрабатывается в инфраструктуре компании.

Одним из компонентов комплексного подхода является поддержание здорового климата в коллективе. Довольный сотрудник с меньшей долей вероятности сознательно нанесет ущерб компании, в которой он трудится. На безопасность влияет и осведомленность сотрудников организации о популярных методах атак. Даже если у специалиста нет намерений совершить что-либо во вред, в силу своей неосведомленности он легко может попасть на удочку злоумышленников. Работа с коллективом является одним из важных аспектов комплексного обеспечения информационной безопасности организации.

— Как оценить вероятные потери?

— Потери будут в большей степени финансовые – от попадания информации не в те руки. Результатом может стать, к примеру, проигранный конкурс на поставку какого-либо продукта или банальный шантаж собственника информации. Злоумышленники могут продать информацию заинтересованным лицам, конкурентам.

Другой вариант – вывод из строя оборудования информационной системы, что влечет за собой простои в работе. Угрозу представляют не только люди (свои или чужие), но также и природные явления, технологические факторы (сбои в электропитании, охлаждении и т.д.).

Существует два основных метода оценки рисков: количественный и качественный. Невозможно однозначно сказать, какой из них лучше - у обоих есть как достоинства, так и недостатки.

Количественный метод заключается в том, чтобы представить в денежном эквиваленте вероятные потери от реализации угроз. Звучит несложно! Неправда ли? Но для такого подсчета нам необходимо: оценить актив, определить процент ущерба, который может быть причинен активу в результате реализации угрозы. И это еще не все. Имея вышеназванные входные данные, мы можем оценить ущерб от одиночной атаки, но атаки могут совершаться неоднократно. На основании статистики компании, если такая имеется, или же мировой статистики, можем предположить, что реализация данной угрозы происходит пять раз в год. После этого умножаем значение единичной потери на количество предполагаемых ее реализаций и в результате имеем значение вероятных потерь в год.

Качественный метод заключается в формировании экспертной группы из компетентных специалистов, которые создают матрицу с указанием вероятности реализации риска (например, крайне вероятно, вероятно, маловероятно и т.д.) и ущерба, который он наносит (например, низкий, средний, высокий, крайне высокий). Затем матрица заполняется экспертами, используя метод «мозгового штурма», или любым другим способом. На следующем этапе создается другая матрица, в которой отражаются решения, направленные на минимизацию возможности реализации рисков. Напротив каждого из решений проставляются соответствующие баллы. По результатам заполнения матрица анализируется и выбирается оптимальное решение.

— Как видим, методы весьма относительны. Но как тогда быть?

— Есть ряд международных стандартов, касающихся защиты информации. Например, ISO/IEC 27001 (ISO 27001), в котором собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента ИБ для демонстрации способности организации защищать свои информационные ресурсы. Этот стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности.

— Это международные стандарты. А действуют ли они у нас? Каким требованиям должны следовать белорусские компании?

— Да, они действует и у нас. Следовать международным стандартам должны все компании, имеющие международные связи (требование со стороны заказчика, иностранного предприятия).

Кроме того, в нашем локальном законодательстве есть ряд своих уточняющих документов, регламентирующих требования к системам защиты. Например, приказ ОАЦ №62. Для выполнения требований данного приказа существует группа стандартов СТБ 34 серии (требования к документации, средствам защиты, алгоритмам шифрования и т.д.).

Если говорить об информационной безопасности в целом, то такими регламентирующими документами будут выступать Конституция Республики Беларусь, концепция информационной безопасности РБ, закон об информации, информатизации и защите информации, а также другие законы Республики Беларусь, которые косвенно задают общий вектор направления информационной безопасности.

— Какие существуют стратегии работы с рисками?

— Существует четыре основных стратегии при работе с рисками: принятие, снижение, перенаправление, отказ от риска. Перенаправление (страхование активов) и принятие (то есть, смириться с фактом риска и его последствиями) не пользуются особой популярностью у нас в стране. Политика регулятора заключается либо в минимизации рисков с помощью сертифицированных решений, либо в отказе от риска, то есть ликвидации источника угрозы.

Чтобы понимать, какие требования должна выполнять та или иная компания, она должна определить класс своей системы (механизм описан в СТБ 34.101.30), а потом найти в приказе №62 соответствующие требования к ней.

— Как проверяется выполнение требований? Существуют ли штрафы за несоответствие?

— Для того чтобы официально подтвердить факт выполнения требований, необходимо пройти аттестацию системы защиты. Аттестат должен быть у всех компаний, обрабатывающих информацию, распространение которой ограничено. В противном случае это будет считаться нарушением законодательства. Аттестат – документ, который выдается на пять лет и подтверждает, что система ИБ способна защищать свои информационные ресурсы, то есть соответствует требованиям ОАЦ. Кроме того, наличие аттестата требуется при организации взаимодействия с другими аттестованными информационными системами. Провести аттестацию могут только компании, которые имеют на это разрешение (лицензию ОАЦ).

Для подтверждения соответствия требованиям ISO 27001 необходимо отдельно пройти аудиторскую проверку. На практике ваше обеспечение ИБ может соответствовать всем требованиям ISO, но это не означает, что ваша компания соответствует требованиям ОАЦ и наоборот, хотя во многом требования дублируются.

По поводу штрафов. При несоответствии требованиям регулятор дает предупреждение и предписание об устранении недостатков в определенные сроки. Невыполнение условий грозит вплоть до приостановки деятельности организации.

— Соответствие требованиям гарантирует компании высокий уровень защищенности?

— Наличие аттестата косвенно говорит о степени защищенности. Документ показывает, что система защиты отвечает требованиям регулятора. На общий уровень защищенности компании влияет совокупность факторов: уровень системы защиты (программно-аппаратный комплекс, лицензионное и сертифицированное ПО), работа с персоналом, аттестация и многое другое. Идеальной безопасности не существует, но использование различных инструментов в комплексе позволяет добиться максимального уровня ИБ.

— Как Softline может помочь обеспечить соответствие необходимым требованиям информационной безопасности?

— Чтобы поддерживать соответствие системы информационной безопасности соответствующим стандартам и требованиям, необходимо регулярно проводить аудит. Сегодня это наиболее эффективный способ получения независимой оценки уровня защищенности компании. Softline предлагает проведение аудита для упорядочения существующих мер защиты или расследования произошедших инцидентов (например, утечки информации).

Аудит позволяет собрать необходимую информацию о событиях с критической степенью риска; о подозрительных сайтах и приложениях, из-за которых возникают угрозы безопасности; о компьютерах в локальной сети, которые уже стали жертвой вирусной атаки. Кроме того, после проведения аудита мы предоставляем заказчикам рекомендации по совершенствованию системы защиты, отдельное описание мер по ликвидации обнаруженных проблем.

У нас есть необходимые лицензии для проектирования, создания и аттестации систем защиты информации. Мы всегда готовы помочь с внедрением сертифицированных инструментов ИБ, проведением аудита, регламентацией бизнес-процессов, прохождением аттестации и проверкой на соответствие требованиям регулятора. ▮

Компания Softline помогла ЕРИП

обеспечить процесс управления инцидентами информационной безопасности

Отрасль: Финансы
Задача:
- мониторинг событий информационной безопасности;
- предотвращение репутационных рисков и финансового ущерба.

Решение: MaxPatrol SIEM
Результат: Детальный мониторинг состояния ИТ-инфраструктуры и оперативное выявление инцидентов

О клиенте

Автоматизированные информационные системы ОАО «Небанковская кредитно-финансовая организация «ЕРИП» имеют общереспубликанский статус и затрагивают широкий спектр общественных отношений в Республике Беларусь.

Задача

Покупка SIEM-системы была обусловлена необходимостью мониторинга и корреляции событий информационной безопасности. Кроме того, необходимо было обеспечить выполнение требований Оперативно-аналитического центра при Президенте Республики Беларусь. По результатам открытого конкурса партнером проекта была выбрана компания Softline, специалисты которой предложили наиболее эффективное решение – MaxPatrol SIEM компании Positive Technologies.

Решение

Max Patrol SIEM поддерживает большое количество источников, постоянно обновляется и имеет одну из крупнейших в мире базу знаний об уязвимостях. Система одновременно анализирует и выявляет даже самые нетипичные атаки, контролирует текущее состояние ИТ-инфраструктуры.

Главным преимуществом решения является то, что в отличие от других поставщиков, компания Positive Technologies самостоятельно разрабатывает коннекторы для целевых систем, если их нет в базе. Кроме того, для обслуживания данной SIEM-системы необходим всего один офицер безопасности, в отличие от других решений данной категории.

Внедрение осуществлялось в несколько этапов. Предпроектный аудит позволил экспертам Softline оценить актуальное состояние информационных систем ЕРИП, их продуктивность и отказоустойчивость. После чего было произведено развертывание системы и ее запуск в эксплуатацию.

На базе MaxPatrol SIEM произведена интеграция с системами ЕРИП по сбору, корреляции и управлению событиями безопасности. Проект был реализован специалистами Softline в кратчайшие сроки – менее чем за 3 месяца.

Помимо установки нового решения Softline провела обучение ИБ-специалистов компании и предоставила техническую поддержку.

> «ЕРИП предоставляет пользователям мгновенный сервис оплаты, поэтому для нас особенно важно поддерживать бесперебойную работу информационных систем и оперативно реагировать на атаки. Внедрение SIEM-системы позволило нам создать собственный центр мониторинга информационной безопасности для своевременного выявления инцидентов».
>
> Таран Дмитрий, заместитель начальника службы безопасности ОАО «Небанковская кредитно-финансовая организация «ЕРИП»

Результат

Внедрив продукт MaxPatrol SIEM, ОАО «Небанковская кредитно-финансовая организация «ЕРИП» получило возможность централизованно собирать со всех своих систем данные о событиях информационной безопасности. Благодаря этому организация сможет своевременно реагировать на возникающие риски и обеспечит безопасность работы всех своих сервисов. ▮

ETHIC:

External Threats & Human Intelligence Center

За последнее десятилетие количество преступлений, совершаемых с использованием информационных и телекоммуникационных технологий, растет по экспоненте. Причем следует понимать, что в современном мире кибератака — это не обязательно взлом компьютерной системы. Это сочетание технических методов, социальной инженерии и многого другого.

Недостатки традиционной модели обеспечения ИБ

По мере перемещения в сеть общественных отношений и бизнес-процессов растет и количество векторов атак на организацию или ее клиентов

И тут становится видно, что традиционная модель обеспечения безопасности, на которую все полагались в последние десятилетия, уже не так эффективна, как хотелось бы.

На чем базируется традиционная модель? На выстраивании защищенного периметра, сегментировании внутренней сети, применении политик безопасности, а также на мониторинге происходящего внутри периметра и попыток проникновения извне. Все эти методы актуальны и сейчас, но их уже недостаточно. Дело в том, что ни одна организация не находится в вакууме. Она осуществляет внешние контакты с клиентами, партнерами или поставщиками, использует системы дистанционного банковского обслуживания, продвигает бренд в интернете. Ее сотрудники общаются в соцсетях, размещают объявления о поиске работы и т.д. Это означает, что внутренние процессы, протекающие в компании, так или иначе проявляются за ее пределами — в глобальном информационном пространстве. Так что, если вы хотите выстроить комплексную систему безопасности, вы должны отслеживать все, что происходит не только внутри организации, но и снаружи.

Это можно сравнить с обороной средневекового замка. У него могут быть высокие и прочные стены, но если вы будете прятаться за ними, не высылая дозоры разведчиков, то обнаружите армию со стенобитными орудиями лишь тогда, когда она уже перейдет к осаде. Если же вы будете мыслить масштабнее, то сможете предотвратить значительное количество угроз еще на этапе их подготовки или, по крайней мере, как следует подготовитесь к нападению.
Именно поэтому наша компания решила предложить своим клиентам новую концепцию обеспечения безопасности, основанную на выявлении потенциально опасных действий и событий за пределами «защищенного периметра» в глобальных информационных и телекоммуникационных сетях, что позволяет своевременно реагировать на возможные атаки, не допуская наступления негативных последствий или минимизируя их. Причем речь идет не только об угрозах информационной безопасности. Выявляемые действия могут затрагивать экономическую или собственную безопасность, тем более что сейчас эти направления достаточно тесно переплетены.

ETHIC — комплексный контроль и выявление цифровых угроз

Чтобы преодолеть недостатки традиционной системы обеспечения ИБ, мы запустили облачный сервис ETHIC: External Threats & Human Intelligence Center — комплексный контроль и выявление цифровых угроз бизнесу.
Главное преимущество сервиса заключается в том, что мы берем на себя всю трудоемкую работу по поиску, классификации и анализу угроз, а в ряде случаев и по немедленному реагированию на них. Это значительно экономит время и ресурсы заказчика, а все выявляемые сведения верифицируются командой опытных аналитиков. Мы максимально автоматизировали данный процесс, разработав для этого собственное программное решение.
Если вы хотите выстроить комплексную систему безопасности, необходимо отслеживать все, что происходит не только внутри организации, но и снаружи.
Все события и угрозы отражаются в личном кабинете заказчика в простой и понятной форме. Имеется возможность ранжировать их по уровню опасности, помечать события как отработанные и пр.
Вторым преимуществом является модульность сервиса, обеспечивающая его гибкость, ведь перечень угроз может значительно варьироваться в зависимости от направления деятельности компании. Поэтому мы разделили сервис на десять модулей — заказчик сам выбирает объем услуг, который ему нужен. Например, модули «Услуги» и «Утечки» предназначены для выявления объявлений о нелегальных услугах, имеющих непосредственное отношение к заказчику, а также его информационных активов, намеренно или случайно опубликованных в интернете. С этой целью мы анализируем контент, размещенный в социальных сетях, мессенджерах, на хакерских площадках, в даркнете и в других источниках.

Какую информацию мы выявляем?

Информация, которую мы выявляем, крайне разнообразна. Это могут быть, например, объявления о вербовке сотрудников компании для их вовлечения в криминальные схемы, предложения «пробить» какие-либо данные с использованием корпоративных ресурсов, объявления о продаже банковских карт или дампов, скомпрометированные учетные записи и многое другое. Причем мы не ограничиваемся выявлением информации, мы проводим комплекс мероприятий, направленных на установление лиц, причастных к противоправной активности, что значительно упрощает для заказчика как проведение внутренних расследований, так и подготовку материалов для обращения в правоохранительные органы.
Примерно так же дело обстоит с фишингом. Ежечасно мы сканируем более 3 тыс. доменных зон на предмет регистрации новых доменных имен, имеющих сходство с охраняемым брендом заказчика. И, если обычно реагирование на фишинг осуществляется по факту возникновения инцидента (обнаружение работающего фишингового ресурса), то использование ETHIC позволяет выявлять потенциально фишинговые доменные имена до наступления негативных последствий и отслеживать все происходящие с ними метаморфозы — от изменения DNS-записей до появления ассоциированного с ними веб-ресурса. Как только такой домен начинает представлять реальную угрозу, мы немедленно принимаем необходимые меры.
Функционирование на базе нашей компании центра мониторинга и реагирования на инциденты информационной безопасности (Infosecurity CERT) позволяет обмениваться информацией о выявленных фишинговых доменах как с регистраторами, так и с международным сообществом центров реагирования на инциденты ИБ, в кратчайшие сроки добиваться блокировки

подобных доменных имен в белорусской и зарубежных доменных зонах. По нашему опыту, среднее время, требуемое для блокировки веб-ресурса, составляет около трех рабочих дней. Модули «Негатив» и «Бренд» позволяют выявлять негативные и компрометирующие публикации, касающиеся деятельности заказчика, а также обнаруживать и пресекать случаи неправомерного использования бренда в социальных сетях и мессенджерах. Причем сценарии использования этих модулей могут быть весьма разнообразными: от мониторинга PR-атак на компанию до выявления коррупционных схем или случаев злоупотреблений со стороны сотрудников.

Важным элементом сервиса является и модуль «Юридические лица». Мы отслеживаем тысячи объявлений о продаже как фирм однодневок, так и компаний, имеющих долгую и хорошую репутацию, необходимые лицензии и коды ОКВЭД, не замеченные ранее в участии в сомнительных схемах (то есть успешно проходящих традиционную комплаенс-проверку).

Просто и доступно

Нередко о каком-нибудь инструменте говорят: «В умелых руках он способен творить чудеса». Сервис ETHIC отличается тем, что способен творить чудеса не только в умелых руках — обо всем уже позаботились наши сотрудники. Работа с продуктом предельно проста, но при этом он обеспечивает вас всей необходимой информацией о том, что творится за стенами вашей компании, но имеет к ней отношение. Поэтому возможности ETHIC смогут в полной мере оценить как специалисты по информационной безопасности, мыслящие в технической плоскости, так и сотрудники экономической или собственной безопасности, для которых важен глубокий анализ не только технических, но и социальных аспектов поведения злоумышленников. Кроме того, сервис ETHIC может быть задействован и для повышения эффективности работы на HR- и PR-направлениях.

Мир быстро меняется. Безопасность современной компании не может находиться в статике, она должна постоянно развиваться, отвечая веяниям времени. Немало организаций погорело на том, что, внедрив однажды хорошую и дорогую ИБ-систему, они надеялись решить проблему раз и навсегда.

Угрозы эволюционируют, и методы противодействия развиваются вместе с ними. Когда мы разрабатывали сервис ETHIC, нашей целью было создать решение, которое дополнит имеющиеся в компании защитные механизмы и значительно расширит возможности выявления и предупреждения угроз без дополнительной нагрузки на сотрудников и инфраструктуру. И у нас это получилось. ▮

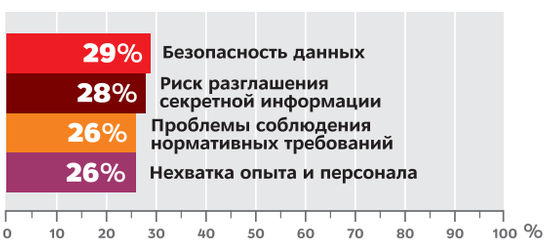
Автор статьи:
заместитель генерального директора
компании Infosecurity Softline
Игорь Сергиенко

66% специалистов по ИБ считают, что технологии защиты облаков не работают

Эксперты компании Check Point представили отчет о безопасности облачных хранилищ данных 2019

Проблема обеспечения безопасности данных – одна из главных причин, почему компании не доверяют облачным технологиям (57% компаний указали ее как основную). По результатам исследования, проведенного компанией Check Point, 66% ИБ-специалистов считают, что **традиционные инструменты безопасности не обеспечивают достаточную защиту** в облаке или не защищают совсем.

Безопасность данных является крупнейшим барьером для внедрения публичных облачных систем, по мнению почти трети (29%) респондентов. На втором месте стоит риск разглашения секретной информации (28%), на третьем — проблемы соблюдения нормативных требований (26%), а также нехватка опыта и квалифицированного персонала для обеспечения безопасности (26%).



Облачные провайдеры усиливают меры безопасности для защиты своих платформ, но ответственность за защиту данных и приложений на этих платформах лежит на самих заказчиках. Несмотря на то, что более 54% организаций заявили, что их облачные хранилища не взламывали, четверть респондентов не смогли точно ответить на этот вопрос, а еще 15% подтвердили, что их облака страдали от каких-либо инцидентов безопасности.

По словам аналитиков Check Point, в публичном облаке есть четыре особо уязвимых места: несанкционированный доступ в облако (42%), небезопасные интерфейсы (42%), неправильная настройка облачной платформы (40%), хищение аккаунта (39%).

Проблемы безопасности при работе с облаком

67% респондентов посчитали главной проблемой **несоответствие облачной инфраструктуры нормативным требованиям**.

31% назвали причинами отсутствия безопасности **несогласованные политики безопасности в облаке и на компьютерах компаний**, а также **нехватку квалифицированных сотрудников службы безопасности**.

«Выводы в отчете свидетельствуют о том, что специалистам по информационной безопасности необходимо срочно пересмотреть стратегии защиты и заменить устаревшие решения. Преступники стремятся использовать облачные уязвимости организаций — уже 15% респондентов сообщают о полобных инцидентах. Компаниям необходимо обеспечить полную прозрачность во всех своих общедоступных облачных средах, которая будет поддерживаться автоматизацией политик, соблюдением нормативных требований, защитой привилегированных пользователей и анализом угроз, чтобы сделать облачные хранилища более безопасными и управляемыми».

Зохар Алон, глава подразделения, выпускающего линейку решений для облаков в компании Check Point Software Technologies

Три причины эффективности точечного фишинга

Сегодня практически и дня не проходит без того, чтобы кто-то не сообщил 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 серьезную озабоченность – сегодня это одна из наиболее часто эксплуатируемых угроз. Способы фишинга развиваются и меняются, постоянно совершенствуясь и подстраиваясь под формальную переписку целевого аккаунта. И если все сделано правильно, то сложно сразу определить, что такое письмо содержит угрозу. 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 серьезном 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 используемые адреса выглядели надежными и убедительными. Около 53% этих атак подделывают Microsoft и Apple, а остальные имитируют такие имена, как UPS, Chase и Amazon. Далее разрабатываются специальные шаблоны электронной почты, чтобы фишинговую корреспонденцию можно было принять за письмо от имени какой-нибудь большой и известной компании. Это повышает вероятность доверительного отношения адресата. В тексте письма может содержаться предупреждение о нарушении безопасности или запрос на подтверждение какой-либо информации. В любом случае, главная цель – заставить получателя нажать на ссылку, подтвердить свои данные для входа в учетную запись или сообщить другие персональные данные.

Ссылки в таких письмах могут выглядеть формально правильными, однако, нажав на них, жертва попадает на фишинговый веб-сайт, который используется для кражи учетных данных. Получив учетные данные пользователя, легко можно 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, является то, что учетные данные Office 365 – это самый короткий путь к ИТ-инфраструктуре любой компании. Став обладателями учетных данных пользователя для доступа к облачным приложениям, злоумышленники 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 млрд. Но это только верхушка айсберга, потому что большая часть осталась неучтенной из-за нежелания компаний рассказывать о подобных проблемах.

Почему потери от этого вида мошенничества так высоки, если они составляют всего 6% от общего количества 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 млн, 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.

Основные типы точечных фишинговых атак

Иллюзия шантажа и запугивания

Каждая десятая фишинг-атака нацелена на шантаж или запугивание жертвы при помощи якобы существующих компрометирующих материалов. Злоумышленники часто начинают рассылать свои требования, получив комбинацию адреса электронной почты и пароля в результате одной из атак. Эти учетные данные собираются в darknet, а затем используются в качестве возможного доказательства того, что у злоумышленника есть личная информация о жертве. Установив «достоверность» учетных данных, злоумышленники начинают предъявлять требования о выкупе. Обычно речь идет о каком-нибудь видео, фотографии или информации о просмотре неблагонадежных веб-страниц. Преступник редко обладает серьезной 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.

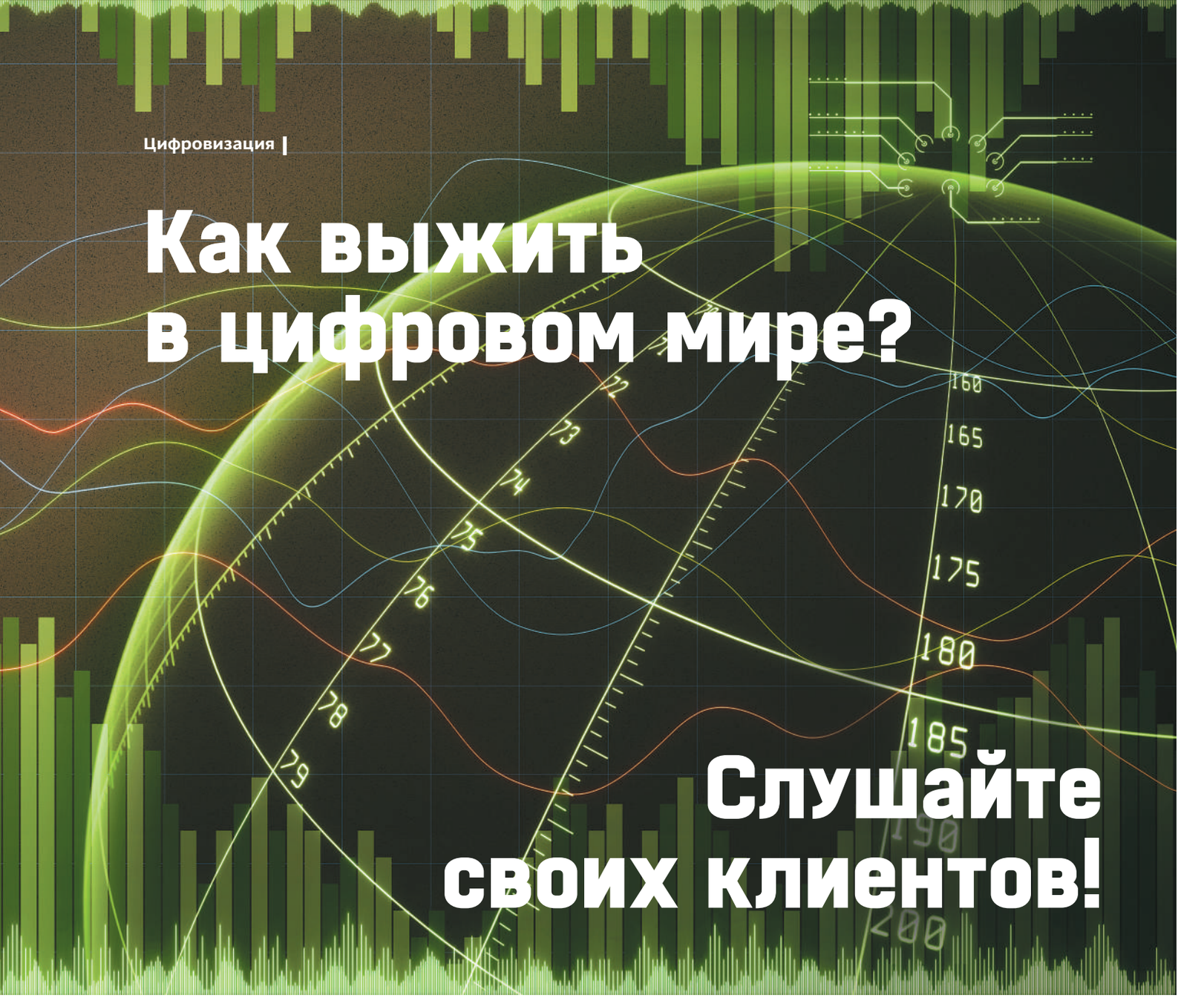
Атаки тщательно продуманы и направлены, наблюдение за предполагаемой жертвой занимает несколько месяцев. Фишинговые сообщения составлены как реальные письма и рассылаются штучно.

Очень часто для начала атаки выбираются такие почтовые сервисы, как Gmail, из-за чего отправляющий домен имеет высокую репутацию. Поэтому эти письма не блокируются при отсутствии явно вредоносных ссылок или вложений, как в случае атаки BEC.

По результатам отчета Trend Micro Research Midyear Security Roundup Evasive за первое полугодие 2019 количество BEC-атак, по сравнению со второй половиной 2018, возросло на 52%, мошеннических рассылок – в 4 раза, фишинговых атак на облачные сервисы Office 365, включая Outlook — на 76%.

Увеличение фишинговых атак связано с распространенностью сервиса в корпоративной среде и сложностями в организации защиты. Общемировая статистика показывает, что количество переходов на фишинговые URL заметно сократилось, как следствие повышения осведомленности пользователей. Понимание собственных рисков и знания о мошеннических схемах — работающий метод противодействия преступникам. ■

Trend Micro – японская компания-разработчик программного обеспечения, лидер в области безопасности гибридного облака, сетевой защиты, безопасности малого бизнеса и защиты конечных точек. Компания предлагает надежные и экономичные решения по обеспечению безопасности контента, антивирусы, защиту от шпионского ПО, антиспам, защиту от фишинга, средства фильтрации контента, решения для предотвращения утечки информации.



Как выжить в цифровом мире?

Слушайте своих клиентов!

Собственники бизнеса и менеджеры высшего звена часто настолько сосредоточены на результатах, что теряют из виду ожидания своих клиентов. Руководители компаний не только не концентрируются на поставке клиентам того, чего хотят последние, но даже не знают точно, удовлетворены ли заказчики тем, что получают сегодня.

Цифровая трансформация — это не реконструкция сайта или внедрение нового документооборота, как и не новый способ продать клиентам товар или мотивировать их воспользоваться вашими услугами. Для любых компаний и организаций, которые что-то продают, главный смысл трансформации состоит в том, чтобы предложить заказчикам то, в чем они действительно нуждаются.

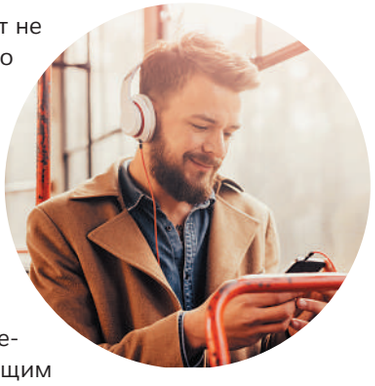
Да, цифровизация решает много задач, а именно — позволяет работать удобнее, тратить меньше и повышать маржинальность. Но в центре настоящего, качественного цифрового скачка, совершенного компаниями, которых теперь считают иконами цифровой эпохи – Uber, Alibaba, Airbnb, Netflix – лежит именно понимание настоящих желаний клиентов и готовность отвечать им. Именно такую трансформацию можно считать истинной. Только она поможет вам осуществить революцию на рынках товаров и услуг. Только она поставит вашу компанию на первое место. Дайте людям то, что они хотят, и мир будет у ваших ног.

Путешествия и туризм

Когда-то для того, чтобы совершить туристическую или деловую поездку, вы шли в агентство путешествий, рассказывали менеджеру ваши пожелания, листали каталоги гостиниц, долго решали, купить ли пакетный тур или лучше билет и гостиницу отдельно, советовались с друзьями и записывали в блокнот телефоны проверенных частников, готовых сдать жилье. И где эти агентства путешествий сейчас? Где авиакассы?

Booking.com, Airbnb, агрегаторы авиабилетов предложили клиентам именно то, что им было нужно – свободу, удобство, максимальную дружелюбность и открытость туристической инфраструктуры всего мира. Индустрия туризма уже никогда не будет прежней, потому что ранее она не отвечала потребностям клиентов в полной мере. Эти перемены стали возможными благодаря технологиям, но вдохновили их именно желания людей.

Медиаиндустрия

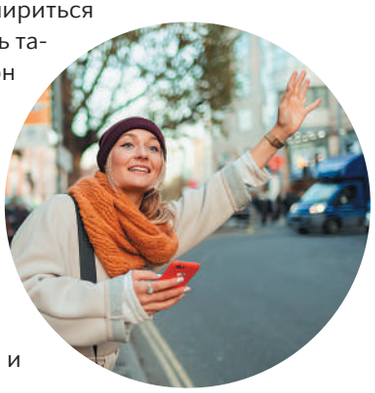


В фантастическом фильме «Люди в черном» (1997) есть момент, который не может не отозваться в душе любого меломана со стажем. Один персонаж знакомит другого с новейшими инопланетными разработками, которые вскоре будут внедрены на Земле, и, кроме всего прочего, показывает маленький диск. «Ну вот, – без радости говорит второй. – Значит, опять придется покупать Белый альбом Beatles!» Так и есть, музыкальная индустрия хорошо заработала на нас, продавая одну и ту же музыку снова и снова на новых носителях. А еще нам приходилось покупать альбомы, чтобы послушать одну или две песни.

Возможность слушать музыку в любом месте, получать именно те песни, которые нужны, не покупать дорогостоящий проигрыватель – все это нам дала технологическая индустрия, породившая MP3, iTunes и тому подобное, в корне изменившая ценообразование, доступ, доставку и потребление музыки. Вдохновляющим фактором здесь стало опять же желание клиентов. А роскошные музыкальные магазины и звукозаписывающие лейблы оказались неспособны угадать и удовлетворить эти потребности.

Точно так же произошло практически во всей медийной индустрии. Помните видеопрокаты и видеомагазины? Они были когда-то точками притяжения в мегаполисах, местом встречи. Но туда нужно было идти, довольствоваться лишь ограниченным ассортиментом, мириться с определенным ценообразованием. Этими слабыми сторонами воспользовались такие сервисы, как Netflix. Захватив неудовлетворенный потребительский рынок, он дал клиентам именно то, что они хотели, и быстро разрушил целую отрасль.

Вам шашечки или ехать?



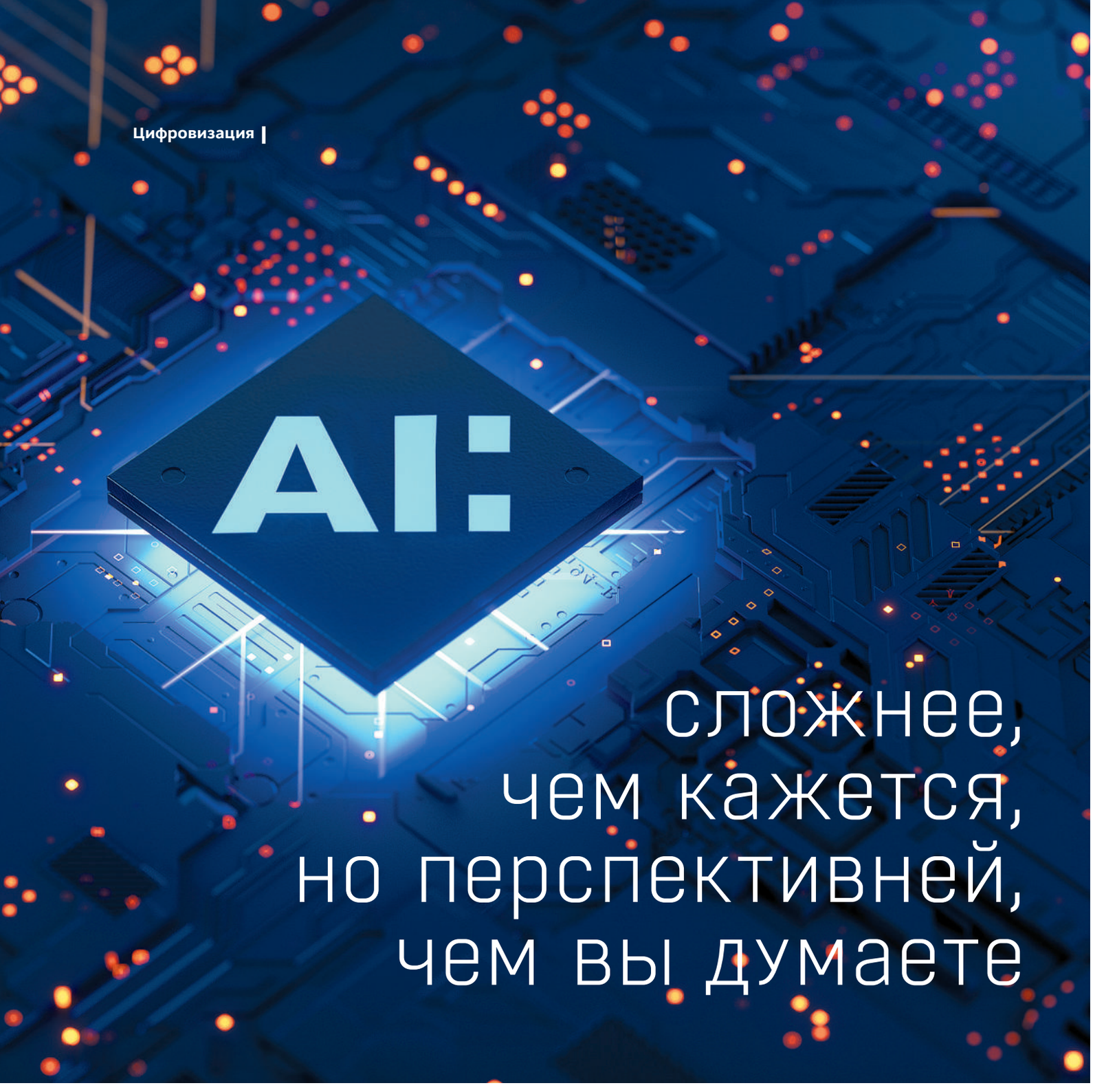
Традиционные крупные таксопарки в большинстве городов мира тоже приказали долго жить. Бизнесу такси нравилось иметь монополию на клиентов, но он потерял ее, как только технологии позволили любому владельцу автомобиля стать сертифицированным и застрахованным водителем, моментально доступным через приложение на смартфоне.

Благодаря Uber и последователям эта индустрия тоже никогда не будет прежней, и перемены на 100% вдохновлены желанием клиента.

На первом месте заказчик

А вы можете представить себе сценарий того, как ваш бизнес разрушается конкурентами, которые выслушивают ваших клиентов и удовлетворяют их потребности лучше, чем это делаете вы? Приложите усилия, чтобы узнать, чего хотят заказчики. Есть масса возможностей и инструментов для выяснения интересов, желаний, поведения существующих потребителей и всей целевой аудитории.

Клиенты, которых вы только собираетесь охватить, заслуживают еще более пристального внимания. Если вы не знаете, что им нужно, то едва ли убедите, что сможете решить их задачи. Вам следует вести себя так, чтобы было видно, что вы заняты проблемами клиента, а не вашего бизнеса. При этом ведите себя искренне и действительно интересуйтесь желаниями людей. Иначе никакой цифровой трансформации не получится. ▮



AI: сложнее, чем кажется, но перспективней, чем вы думаете

Искусственный интеллект (ИИ; англ. Artificial intelligence, AI) уже много лет будоражит воображение, но реальные перспективы по преобразованию бизнеса с его помощью появились относительно недавно. Знаете ли вы, что до сих пор 85% проектов в области искусственного интеллекта не приносят бизнесу обещанных результатов (по данным Pactera Technologies за 2019 г.). Это, однако, не мешает большинству экспертов и игроков рынка оценивать потенциал ИИ оптимистично, ведь риски высоки, но и выгоды могут быть огромными.

Часто проекты AI оказываются непредсказуемыми: вы можете достигнуть намеченных целей, можете вернуться в исходную точку ни с чем, а можете найти сокровища там, где не ожидали. Давайте поговорим о том, как можно не только управлять рисками в проектах ИИ, но и получать максимум выгоды.

Разрабатывайте несколько проектов

Итак, все проекты AI – рискованные. Лучшие из них приносят огромную отдачу от инвестиций, и нетрудно найти этому множество подтверждений. Но и потерпеть неудачу легко. Идея может потребовать больше денег и сил, чем в итоге принесет пользы. Хорошая программа ИИ – это структурированное портфолио проектов, которое позволит исследовать ряд вариантов, прежде чем выбирать лучшие.

Достигать одних и тех же бизнес-целей можно разными способами, а оценка успеха этих способов в ключевых точках, выполненная по одним и тем же метрикам, даст возможность перенести усилия и ресурсы на более перспективные варианты. Если один проект показывает двойную окупаемость инвестиций, а другой – пятикратную, нетрудно сделать правильный выбор.

Впрочем, провал тоже может быть полезен. Из неперспективных проектов по-прежнему извлекайте ценные уроки для начинаний, которые только планируете развивать.

Анализируйте на полпути

Как и в любой новаторской отрасли, первый намек на успех часто окрыляет и заставляет продолжать не самую перспективную работу. Это может происходить, например, из-за экспертов в предметной области (энергетиков, маркетологов или инженеров), которые четко понимают свою узкую цель и знают, какие данные влияют на результат, но не видят полную бизнес-перспективу.

Зачастую бывает выгодней сделать шаг назад и продолжить путь в другом направлении. Могут обнаружиться полезные источники данных, о которых вы раньше всерьез не думали, потому что они не соответствуют начальным моделям. Или исследование ожидаемой корреляции (например, позитивного влияния изменения частоты рассылок на продажи) способно съесть все ресурсы, в то время как на практике другие переменные могут оказывать более весомое влияние на бизнес.

Конечно, любые решения должны быть основаны на бизнес-целях, а не на стремлении к техническому совершенству. Вы можете снизить частоту ошибок модели с 2% до 1%, но не старайтесь это сделать делать, если и 2% приемлемы.

Как действовать грамотно? Вам поможет постоянный анализ, идентификация потенциальных ловушек и исследование новых возможностей. Не бойтесь отказываться от проектов и переходить на более перспективные маршруты.

Уделите самое большое внимание качеству данных

Машинное обучение оказалось чрезвычайно успешным в решении задач классификации, распознавания, ранжирования, диагностики. Однако для его эффективного применения необходимы большие объемы подготовленных данных, получить которые в реальной жизни – большая проблема.

Имеются сведения, что большинство исследователей данных тратят только 20% своего времени на анализ и 80% – на поиск, очистку и реорганизацию огромных объемов информации. Очевидно, что это неэффективная стратегия.

Связаться с различными отделами для получения сведений, дождаться, определить, содержится ли в них нужная информация, решить проблемы с качеством – все это требует много времени и усилий. А чтобы хранилища не превратились в свалки, наборы данных необходимо систематизировать и классифицировать. Компромиссы же ведут к некачественному обучению и плохо работающим на практике моделям.

Решением может стать продуманная политика управления информацией в масштабе организации и использование современных облачных инструментов для автоматизации утомительных процессов, связанных с поиском и очисткой файлов.

Впрочем, для ряда задач данных для обучения заведомо нет. Если вы хотите применить ИИ для предсказания выхода из строя многомиллионной газовой турбины, вряд ли вы найдете много информации по отказам такого оборудования. В таких случаях применять обучаемые модели, очевидно, нет смысла.

Сейчас мы затронули лишь вершину айсберга. Как и в любой новой и сложной технологии, ее успешное применение требует учитывать огромное число факторов и нюансов. ▮

Почему Kubernetes так важен для вашего бизнеса

Что такое Kubernetes?

Контейнеры захватили ИТ-индустрию и в рекордные сроки стали очень популярными. Сегодня многие ИТ-лидеры, такие как Amazon, VMware, Microsoft, IBM, поддерживают Kubernetes – лидирующую на рынке платформу для запуска и оркестровки контейнеров с открытым исходным кодом, систему для развертывания, масштабирования и управления приложениями. Kubernetes упрощает управление инфраструктурой и делает ее более гибкой: приложения можно легко перемещать между различными облаками и внутренними средами. Платформа требует меньших затрат на ИТ-персонал.

Как это работает?

Чтобы объяснить, как это работает, вначале нужно понять суть виртуализации и контейнеризации. Традиционная виртуализация позволяет разделить физические серверы на несколько виртуальных машин для эффективного совместного использования оборудования. Контейнерная технология обеспечивает еще более эффективный способ виртуализации физического оборудования, позволяя запускать приложения в полностью стандартизованном контейнере, в изолированной среде.

Kubernetes облегчает управление большим количеством контейнеров. Представьте себе гигантский склад. Все товары аккуратно упакованы в коробки и изолированы друг от друга. При огромном масштабе сотрудники не могут эффективно отслеживать нужные коробки и вручную доставлять их по месту требования в определенное время. Чтобы автоматически отслеживать, планировать и организовывать все эти контейнеры нужно решение для оркестрации. Для этого и создан Kubernetes. Он автоматизирует управление контейнерами. Контейнеры делают приложения более гибкими и экономически эффективными. Если сравнивать со складом, то Kubernetes делает для контейнерных ИТ-сред то, что автономные мобильные роботы делают для современных фабрик.

Одним словом, Kubernetes позволяет разработчикам более быстро и надежно доставлять приложения для пользователей и поддерживать ИТ-системы онлайн в режиме 24/7.

Какие задачи решает Kubernetes

Компании могут использовать Kubernetes для полного аутсорсинга ЦОД, мобильных и веб-приложений, поддержки SaaS, облачного веб-хостинга или высокопроизводительных вычислений. Kubernetes обеспечивает **отказоустойчивость** важных систем для бизнеса и поддерживает работоспособность даже при выходе из строя отдельных приложений.

Kubernetes решает проблему непрерывного **обновления систем**. Проблема заключается в том, что при обновлении какого-либо ИТ-решения важно обеспечить его корректную работу после переноса со среды разработки на продуктовую платформу. Контейнеры объединяют все компоненты ПО в один изолированный от внешней среды пакет, что позволяет быстро и надежно разворачивать приложения на любой инфраструктуре.

Kubernetes может использоваться для **масштабирования веб-хостинга**. Мобильные приложения и сайты со сложным кодом могут быть развернуты с использованием Kubernetes на обычном оборудовании для снижения затрат на подготовку веб-сервера к хостам публичного облака.

Разработчики ценят Kubernetes за то, что платформа ориентирована на приложения, а не инфраструктуру, а также поддерживает Docker-контейнеры. Кроме того, Kubernetes удобен для работы не только с одним дата-центром, но и с несколькими, распределенными по разным офисам.

Система способна сама себя восстанавливать в случае сбоев. ИТ-отдел может не беспокоиться, на какой физической машине запущен тот или иной контейнер, и куда его перенести, чтобы запустить новый сервис.

Как Kubernetes помогает бизнесу

Автоматизирует процессы. Все операции проходят в Kubernetes автоматически. Бизнес экономит на аппаратных решениях и человеческих ресурсах. Чтобы обслуживать и настраивать систему необходимо максимум 1-2 человека. Компании могут арендовать кластеры Kubernetes в облаке, если хотят снять с себя работу по администрированию и заниматься только разработкой.
Повышает гибкость мультиоблаков. Kubernetes значительно упрощает запуск любого приложения в публичном облаке или на объединенной платформе из публичного и частного облаков. Система позволяет эффективно распределять рабочие нагрузки в нужном облаке, избегать привязки к поставщику и тем самым повышает рентабельность инвестиций в ИТ.
Снижает затраты. Kubernetes помогает бизнесу сократить расходы на ИТ-инфраструктуру. Приложения объединяются с минимальными ресурсами, а бизнес при этом получает максимальную выгоду от облачных и программно-аппаратных вложений. Приложения, которые необходимо расширить, можно размещать в модулях, где есть место для роста.
Мгновенно масштабирует приложения. Kubernetes автоматизирует горизонтальное масштабирование приложений путем добавления и удаления контейнеров, а также автоматического увеличения или уменьшения размера кластера в зависимости от актуальных показателей нагрузки. Вертикальное масштабирование обеспечивает эффективное распределение ресурсов, доступных в кластере. За счет масштабирования кластера система становится еще более производительной и отказоустойчивой.

VMware Essential PKS

Сегодня одно из популярных решений для применения Kubernetes – контейнерная служба VMware PKS (Pivotal Container Service). Кроме оркестрации контейнеров, платформа PKS позволяет разворачивать большое количество контейнеров в рамках одного развертывания и имеет расширенные функции по их управлению.
Мировой лидер в области виртуализации предлагает несколько инструментов, отвечающих всем потребностям в контейнерных разработках:

- **VMware Essential PKS** – для компаний с собственной экспертизой проектирования своей ИТ-системы или тех, кто планирует ее создать. Исходный код Kubernetes позволяет работать с решением при поддержке экспертов VMware.
- **VMware Enterprise PKS** – для компаний, которые работают с контейнерными проектами «под ключ». Обычно такие организации уже работают с продуктами VMware.
- **VMware Cloud PKS** – для компаний, которые планируют создать высокодоступные кластеры Kubernetes, чтобы ИТ-отдел не разбирался в настройках самостоятельно. Кластеры при этом полностью настроены и сконфигурированы в соответствии с задачами, постоянно доступны и оперативно масштабируются.

Одно из преимуществ платформы PKS в том, что она совместима с различными облачными средами: Azure Cloud Provider Interface, VMware vSphere, Google Cloud Platform, Amazon EC2.

Работа с Kubernetes

С помощью Kubernetes можно легко мигрировать с одной инфраструктуры на другую, например, с физической на облачную или гибридную с оркестрацией контейнеров on-premise и в облаке. Но перед переходом необходимо продумать конфигурацию и поработать над архитектурой. Поскольку это технология с открытым исходным кодом, то у нее нет официальной поддержки. Значит, для развертывания и управления системой вам нужна помощь как собственных инженеров, так и партнеров, которые понимают, как функционируют уровни абстракции и всегда в курсе последних изменений в мире экосистемы инструментов Kubernetes. Компания Softline может сделать современные технологии доступными даже малому бизнесу.

Для получения дополнительной информации
вы можете обратиться к **Игорю Волокитину**,
product manager infrastructure and virtualization solutions Softline
по телефону **+375(29)172-89-64** или e-mail **Igor.Volokitin@softline.com.**

PARITETBANK

Модернизация ИТ-инфраструктуры ОАО «Паритетбанк»

Отрасль: Финансы
Задача: Повышение управляемости инфраструктурой, централизованное управление рабочими столами, создание защищенной ИТ-среды
Решение: Безопасное и масштабируемое решение VMware Horizon
Результат: Автоматизация управления инфраструктурой, снижение стоимости обслуживания рабочих мест, гибкое управление информационными ресурсами

О клиенте

«Паритетбанк» уже более 20 лет оказывает широкий перечень финансовых услуг физическим лицам и организациям. Сегодня банк активно развивается и работает с клиентами в 26 отделениях по всей Беларуси. Основным фокусом на ближайшее время является создание современных простых решений для людей и бизнеса.

Задача

ЦБУ «Паритетбанка» расположены в 16 городах Беларуси. В связи с территориальной удаленностью офисов управлять рабочими местами становилось все сложнее. Руководство банка приняло решение о модернизации ИТ-инфраструктуры. Необходимо было снизить затраты на обслуживание рабочих мест и при этом улучшить защиту корпоративных данных. Было принято решение о внедрении технологий виртуализации рабочих столов.
По результатам открытого конкурса партнером проекта стала компания Softline, которая имеет необходимые компетенции и опыт в области виртуализации. Эксперты Softline предложили «Паритетбанку» внедрить технологию VDI и провести виртуализацию рабочих мест с помощью решения VMware Horizon.

Решение

Проанализировав ИТ-инфраструктуру предприятия, компания Softline совместно со специалистами банка разработала план внедрения.

После обновления существующих аппаратных и программных компонентов инженеры Softline приступили к развертыванию платформы виртуализации рабочих столов и системы мониторинга. Были установлены комплексы продуктов VMware Horizon и VMware vRealize Operations. Следующим этапом проводилось создание «золотого» образа рабочей станции и интеграция в него пользовательского ПО, необходимого для работы с текущими банковскими сервисами. Новая цифровая платформа позволила сотрудникам безопасно пользоваться внутренними системами банка с тонких клиентов и ПК через единую рабочую среду. С помощью удобной панели мониторинга ИТ-отдел получил возможность контролировать всю виртуальную инфраструктуру, оперативно реагировать на сбои и устранять их, а также настраивать единые политики безопасности виртуальных рабочих столов.

Доступ к системе предоставляется через ПК, на которых установлен клиент Horizon, либо через тонкие клиенты, которые гораздо дешевле компьютеров и имеют более длительный срок службы. Так как вычислительные мощности рабочего стола сосредоточены на сервере, то масштабирование происходит быстро и экономно. Создание новых рабочих мест происходит за считанные минуты.

Основные преимущества использования технологии VDI:

- соответствие высоким стандартам безопасности;
- мгновенное создание новых рабочих мест;
- экономическая выгода за счет использования тонких клиентов;
- экономия электроэнергии;
- регулярное резервное копирование;
- улучшенный контроль за сотрудниками банка;
- гибкое рабочее место и гарантия непрерывности работы.

Результат

«Паритетбанк» перешел на современную виртуальную ИТ-платформу, повысил уровень безопасности и управляемости инфраструктурой, снизил затраты на обслуживание. Специалисты банка получили единое пространство для совместной работы. Теперь они могут безопасно работать с любого устройства и в любом месте. Новая виртуальная инфраструктура была развернута для 200 виртуальных рабочих столов.

«Благодаря технологиям виртуализации VMware мы можем с легкостью запускать новые банковские сервисы и услуги. Единое цифровое пространство позволило специалистам стать более мобильными: они имеют постоянный доступ к внутренним системам банка, быстрее обслуживают клиентов, продуктивнее работают. Кроме того, мы значительно повысили безопасность ИТ-системы и снизили затраты на обслуживание локальных компьютеров и электроэнергию», - отметил начальник управления ИТ-инфраструктуры и телекоммуникаций Владимир Дорошко. ▮

HPE за БЕЗОПАСНОСТЬ!

Новые уровни безопасности для эры сложных сред и серьезных угроз

Длинный перечень различных сертификатов – знак того, что предлагаемые компанией HPE продукты соответствуют самым строгим стандартам безопасности и нормативным требованиям. Каким образом удается этого достичь?

Hewlett Packard Enterprise

Автор: Джон Фрюэ,
старший аналитик
Moor Insights & Strategy

Обсуждая вопросы безопасности, многие говорят исключительно о программном обеспечении. Однако, если предприятия заинтересованы в реальной безопасности ИТ, начинать следует с более низкого уровня — **уровня оборудования.** Проблемы безопасности на аппаратном уровне могут представлять для организаций большую проблему. Поскольку по умолчанию предполагается, что оборудование полностью безопасно, в случае внедрения вредоносного кода на уровне оборудования атака может оставаться незамеченной в течение недель, месяцев или лет.

Silicon Root of Trust

В серверах HPE ProLiant Gen10 встроена технология «Silicon Root of Trust», которая работает на уровне микросхем материнской платы, которая позволяет проверять прошивку контроллера управления iLO на наличие вредоносного кода.

Защита сети с Aruba 360 Secure Fabric — ClearPass+IntroSpect

Решение HPE/Aruba ClearPass Policy Manager, защищающее сеть и обеспечивающее контроль доступа к ней, выявляет устройства, помогает соблюдать политики. Программный продукт IntroSpect, последнее приобретение компании HPE, интегрируется в эти средства и с помощью расширенного мониторинга и средств анализа отслеживает поведение пользователей, устройств и систем, намного более оперативно выявляя и устраняя аномалии. IntroSpect контролирует взаимодействие между машинами и выявляет подозрительные действия, которые, возможно, связаны с оборудованием.

И это далеко не все. Нужны подробности?
По всем вопросам вас проконсультирует **Александр Мигаль**,
специалист по продажам отдела консалтинга Softline
+375 (17) 336-55-95 доб.4421 | Alexander.Migal@softline.com

Защита конечных устройств сотрудников с помощью решений Cisco

Современный бизнес сложно представить без мобильных технологий. Согласно данным компании Advanis, корпоративную почту с мобильных устройств проверяют 75% офисных сотрудников. По сведениям IDC, 56% руководителей заявляют, что мобильная стратегия чрезвычайно важна для достижения поставленных целей, а также для нормального развития и модернизации бизнес-процессов.

Мобильность сотрудников — требование текущего дня, а потому на подразделения ИТ возлагается довольно сложная задача — обеспечить пользователям безопасный доступ к корпоративным ресурсам с любого устройства, в любой момент времени и из любой точки.

Компания Cisco предлагает набор решений, которые обеспечат грамотное планирование и реализацию перехода к использованию мобильных технологий, а также гарантируют безопасность конфиденциальных сведений.

Cisco Identity Services Engine (Cisco ISE)

Решение обеспечивает мониторинг пользователей и устройств, позволяя поддерживать и контролировать мобильный доступ к корпоративным ресурсам. Продукт позволяет определять политики информационной безопасности и управлять ими в масштабе всей организации.

Функционал:

- политика контроля доступа, учитывающая контекст, позволяет обеспечить поддержку «любых устройств»;
- решение различает корпоративные и личные пользовательские устройства;
- средства контроля доступа и шифрования, реализованные на уровне сети, помогают автоматизировать процессы обеспечения информационной безопасности;
- позволяет разрабатывать политики, учитывающие пользователей и их местоположение, используемые устройства и приложения.

Благодаря Cisco ISE есть возможность разграничить доступ по множеству критериев:

- кто должен иметь доступ,
- с каких устройств,
- в какое время суток,
- через какие сетевые устройства,
- какой уровень доступа необходим.

Все это определяет контекст доступа в сеть.

Применение Identity Services Engine (ISE) позволяет создавать доверенную среду в масштабе всей организации на базе единой централизованной политики ИБ для любых типов пользователей, устройств и подключений.

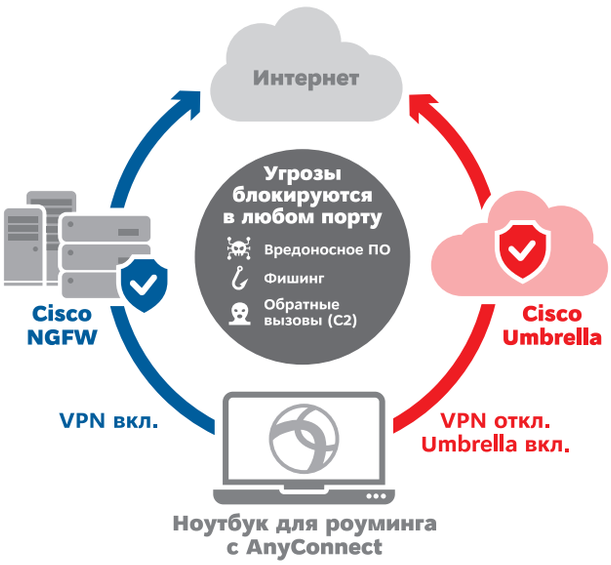
- Пользователи смогут получить привычный набор сетевых сервисов вне зависимости от места и способа подключения к сети.
- Управленцы получают возможность добиться разделения полномочий и обязанностей ИТ-подразделений и подразделений информационной безопасности. За счет этого повысится отклик ИТ-инфраструктуры предприятия на новые требования бизнеса, снизятся операционные затраты и автоматизируются ресурсоемкие ИТ-процессы.
- Топ-менеджмент может получить значительную выгоду от внедрения систем контроля доступа. Следствием внедрения этих систем является переход на новые модели ведения бизнеса, такие как: Mobility (безопасная мобильность рабочего места сотрудника) и BYOD (использование персональных устройств для работы с корпоративными данными).

Мобильные пользователи являются одной из основных проблем информационной безопасности. Решение ISE позволяет контролировать доступ, политики, учитывать контекстную информацию. С помощью этого продукта пользователи получают привычный набор сетевых сервисов вне зависимости от места и способа подключения к сети. Но этим не исчерпываются все сложности, ведь теперь необходимо обеспечить безопасность соединения как для пользователя, так и для ресурсов компании.

Cisco AnyConnect

Решение Cisco AnyConnect упрощает реализацию безопасного доступа с различных устройств. Cisco AnyConnect — это облегченный клиент безопасности, который устанавливается на мобильные устройства на платформах IOS, Android, Mac, Windows. Решение настраивается пользователем с учетом индивидуальных бизнес-потребностей. Cisco AnyConnect обладает следующим функционалом:

- возможности VPN для ПК и мобильных платформ, включая VPN для отдельного приложения на мобильных платформах, VPN телефона Cisco и VPN-клиенты IKEv2 сторонних производителей;
- сбор основной контекстной информации с оконечных устройств;
- запрашивающее устройство IEEE 802.1X Windows;
- облачная система защиты веб-трафика Cisco Cloud Web Security для платформ Windows и ОС Mac X;
- регулятор Cisco AMP для оконечных устройств. (AMP для оконечных устройств лицензируется отдельно);



- подключение к VPN на многофункциональном устройстве обеспечения безопасности Cisco ASA без использования клиента (через браузер);
- агент соблюдения нормативных требований и оценки состояния VPN вместе с многофункциональным устройством обеспечения безопасности Cisco ASA;
- агент соблюдения унифицированных требований и оценки состояния вместе с платформой Cisco Identity Services Engine;
- модуль контроля состояния сети.

Как и все продукты Cisco, AnyConnect обладает гибкой системой лицензирования, позволяющей не переплачивать за неиспользуемый функционал. Доступны как срочные (на 1, 3 или 5 лет), так и бессрочные лицензии. Кроме того, AnyConnect можно масштабировать в зависимости от конкретных потребностей.

Cisco Umbrella

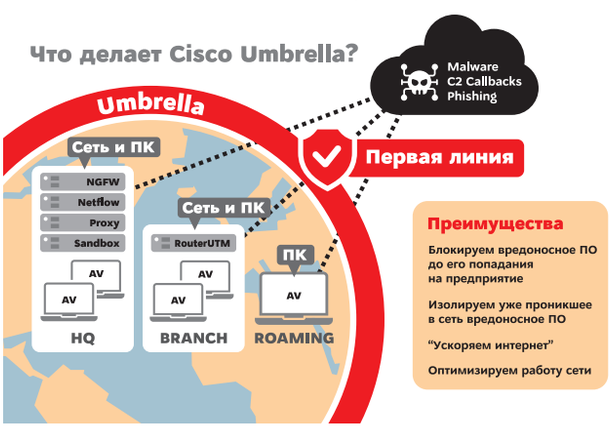
Специалисты компании Cisco провели ряд исследований и выяснили, что к 2020 году 92% глобального трафика ЦОД будет приходиться на облака. Согласно исследованию компании Gartner, в скором времени примерно 25% корпоративного трафика будет проходить мимо периметральной безопасности.

Возникает вопрос: если есть VPN, то почему трафик идет мимо периметра? Ответ достаточно простой — VPN это лишние действия, меньше скорость, не так удобно. По статистике 82% удаленных и мобильных пользователей предпочитают VPN не включать.

Для решения этой проблемы компания Cisco ввела в эксплуатацию новый облачный продукт Cisco Umbrella, представляющий собой интернет-шлюз (secure internet gateway, SIG).

Продукт Cisco Umbrella не так давно поступил на белорусский рынок, однако он уже используется более чем в 160 странах.

Шлюз интернет-безопасности Cisco Umbrella представляет собой облачную платформу, которая играет роль первой линии защиты пользователей как в корпоративной сети, так и за ее пределами. Umbrella преграждает путь имеющимся и новым угрозам по всем портам и протоколам, блокирует доступ к опасным доменам, адресам (URL и IP) и файлам еще до установки соединения или загрузки файла. Так как большинство угроз направлено на оконечные точки, важно закрыть все порты и протоколы, чтобы сеть безопасности покрывала весь трафик.



Основной функционал Cisco Umbrella предназначен для защиты мобильных устройств сотрудников, вне зависимости от их нахождения внутри или вне корпоративной сети. На практике решение проверяет все DNS-запросы.

Шлюз Umbrella позволяет идентифицировать и заранее предотвращать угрозы с помощью средств Cisco Security, в числе которых:

- модели машинного обучения, позволяющие выявить известные и появляющиеся угрозы, блокировать подключения к вредоносным сайтам на уровнях DNS и IP;
- интеллектуальные средства Cisco Talos для блокирования вредоносных URL на уровне HTTP/S;
- технология Cisco Advanced Malware Protection (AMP) для обнаружения вредоносных файлов и блокирования их в облаке.

Предусмотрена интеграция Umbrella с другими системами, включая устройства защиты, платформы анализа данных, а также средства собственной разработки, позволяющие расширить защиту устройств и площадок за пределы периметра.

В последние годы ИТ-специалисты пытались контролировать наплыв смартфонов, планшетов, ридеров электронных книг и других мобильных устройств в рабочей среде. Теперь стало очевидно, что при правильном подходе ИТ-отдел может гораздо шире использовать возможности мобильных технологий, при этом минимизируя связанные с этим риски.

ОТКРОЙТЕ БЕЗГРАНИЧНЫЕ ВОЗМОЖНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ЛЮБЫХ БИЗНЕС-ЗАДАЧ

softlinecloud.by

Эволюция проектирования с Dynamo

О том, как платформа Dynamo расширяет функционал Revit и оптимизирует работу проектировщиков, рассказала ведущий архитектор и тренер по Revit в Softline Елена Хацкевич.

Dynamo

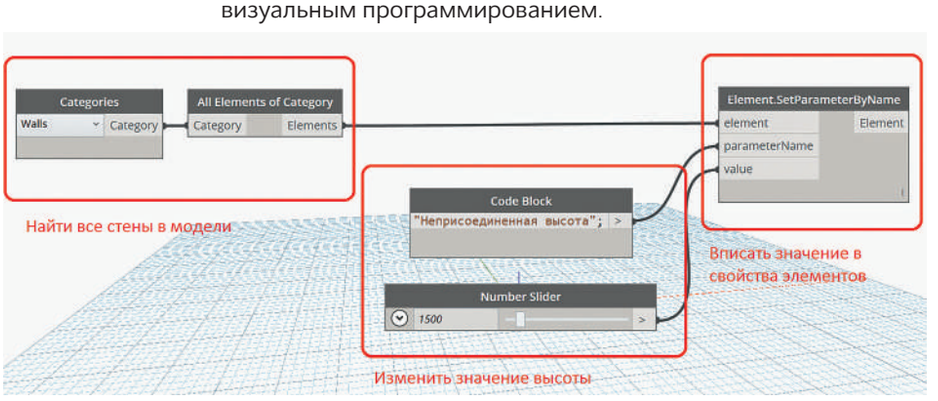
– Что представляет собой Dynamo?

– Dynamo – это платформа, которая расширяет стандартный функционал Revit и позволяет производить любые расчеты нажатием одной кнопки.

Любой инженер, проектирующий жилые здания в Autodesk Revit, знает, что не существует готовых решений, которые бы учитывали все тонкости процесса расчета параметров жилого комплекса. Dynamo была создана для расширения базового функционала Revit и экономии времени проектировщиков.

Dynamo является Open Sourse-проектом – платформой для графического или визуального программирования с открытым исходным кодом, но для работы с продуктом не обязательно знать язык программирования. В данном случае мы имеем дело с визуальным языком, где код не пишется напрямую, а генерируется с помощью графических элементов (блоков). Блоки (ноды) расставляются в необходимом порядке, после чего между ними настраиваются связи.

Вместо сложного кода в Dynamo используются простые блоки, написанные человеческим языком. Из блоков собираются правила, по которым будет работать Revit. Такой подход и называется визуальным программированием.

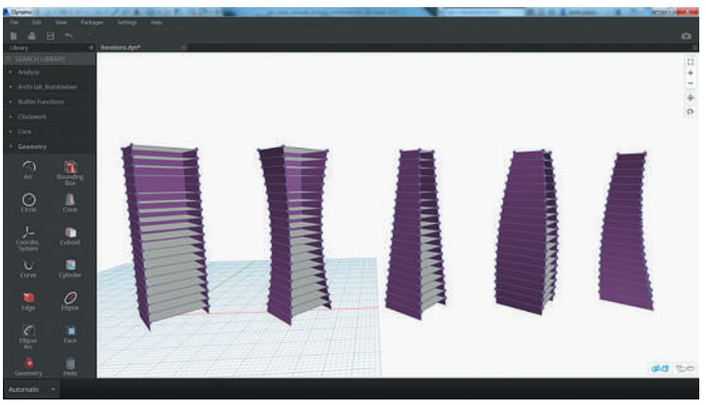


В Dynamo есть огромная библиотека готовых нодов для разных задач. С их помощью можно запрограммировать весь необходимый функционал и дальше работать с ним в Revit или Civil. Например, создавать любую геометрию в Revit, вытягивать данные для дальнейшего использования в спецификациях.

– Какие основные области применения и возможности Dynamo?

– Проектировщики могут использовать Dynamo на всех стадиях проектирования: при создании концептуальных форм; при разработке конструкций по заданной архитекторами геометрии здания; для формирования спецификаций.

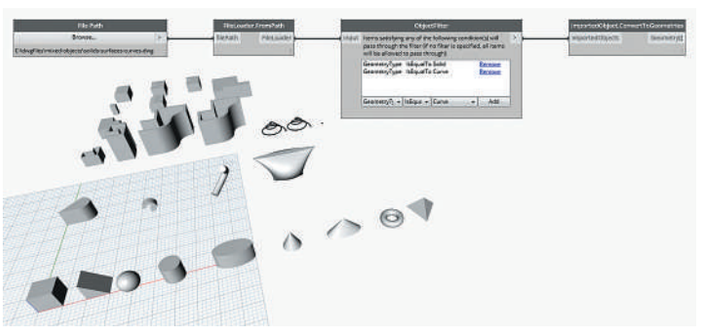
Важное преимущество программы в том, что пользователь или проектировщик могут получать необходимую информацию из Revit и передавать ее обратно. Есть возможность создавать новые элементы по необходимым параметрам: построить стену по заданным линиям, расставить колонны с заданным шагом.



С помощью Dynamo можно быстро создать теплотехнический расчет, расчет отделки помещений, расстановку светильников, подключить инженерное оборудование, оптимизировать путь инженерных сетей, рассчитать несущие конструкции. Кроме того, инженеры могут оформлять здесь необходимую документацию, формировать сметы.

Dynamo легко можно дорабатывать под свои задачи. Это отличная возможность писать Revit «под себя».

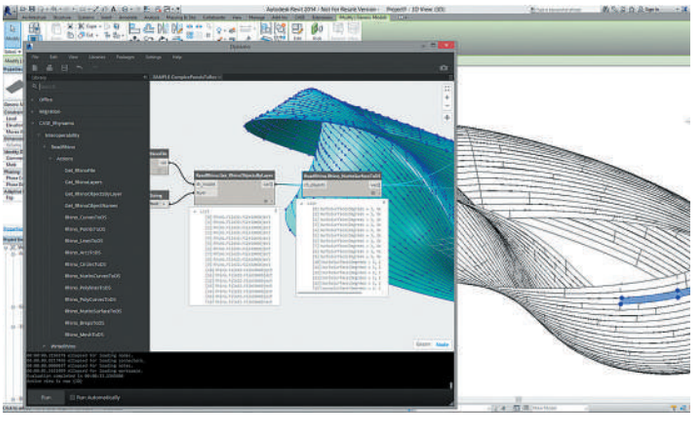
– Почему Dynamo сегодня настолько популярный и ценный продукт?



– Далеко не все инструменты в Revit являются достаточно гибкими. Иногда инженерам необходим дополнительный функционал для проектирования того или иного объекта. Dynamo не просто расширяет базовый функционал в Revit. Этот продукт представляет собой своего рода мост, через который многие архитекторы переходят от обычного проектирования к программированию, получая новые возможности для производственного процесса.

Визуальное программирование с Dynamo – это наглядная иллюстрация эволюции проектирования: большинство операций можно заложить в алгоритмы, что в несколько раз ускорит рабочие процессы.

В Softline мы изучаем способы применения Dynamo для разных сфер бизнеса и уже сейчас можем сказать, что продукт снижает время подготовки документации, повышает качество создания информационных моделей, точность расчета объемов работ.



– Как получить/установить модуль Dynamo?

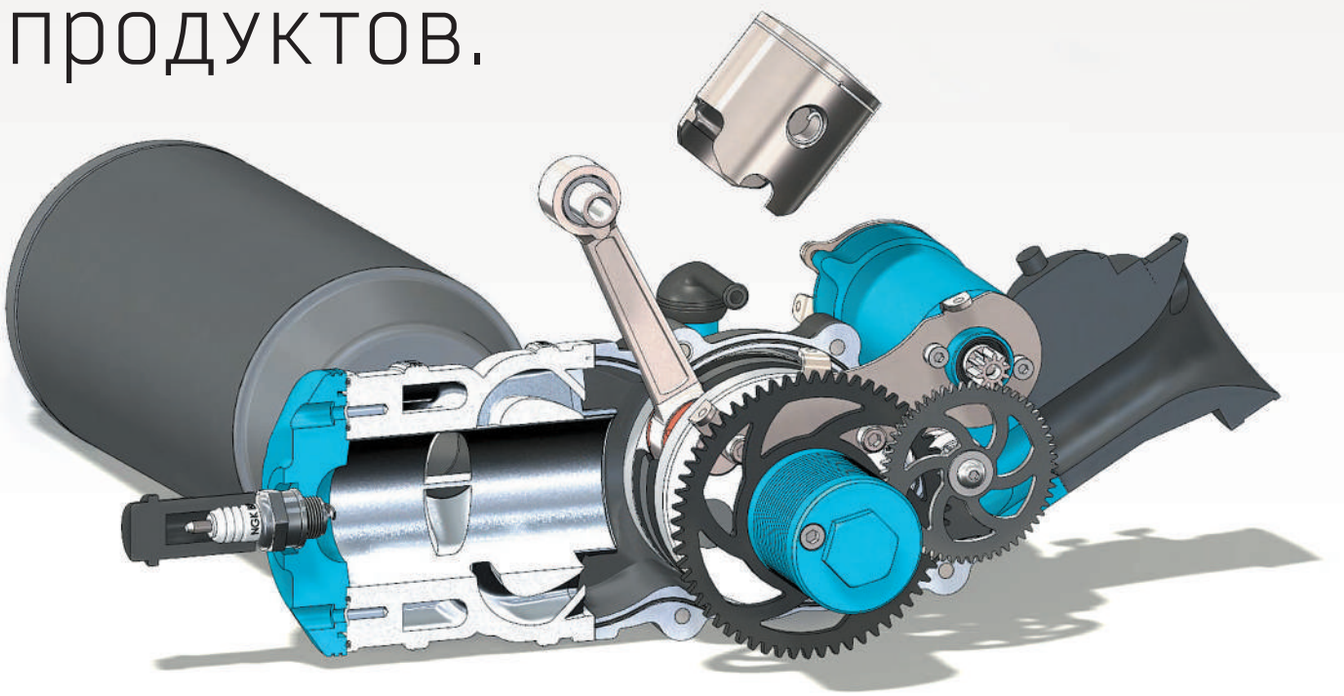
– Главное преимущество платформы в том, что плагин не нужно загружать дополнительно. Он устанавливается вместе с программой Revit. Достаточно перейти на вкладку Dynamo и можно начать использование.

– Где можно обучиться работе с Dynamo?

– На базе авторизованного учебного центра Softline планируется проведение курса по данному продукту с привлечением иностранного спикера-практика по Dynamo. На текущий момент группа находится в процессе формирования. ▮

Елена Хацкевич,
ведущий архитектор
и тренер по Revit в Softline
Тел: +375 (29) 606-53-52
Elena.Khatskevich@softline.com

SOLIDWORKS Sell: облачная 3D технология персонализации продуктов.

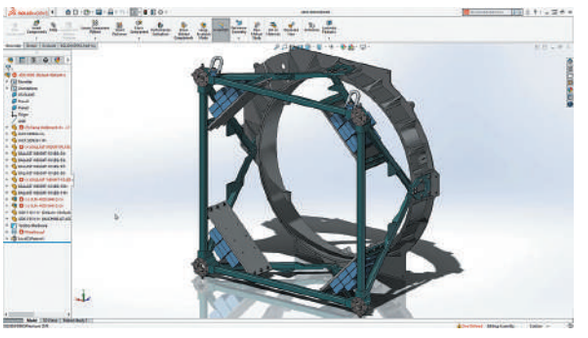


Технология, позволяющая использовать инженерные данные в продажах и продвижении продукции компании.

Владимир Фонов, менеджер по направлению «Машиностроение»

Что из себя представляет?

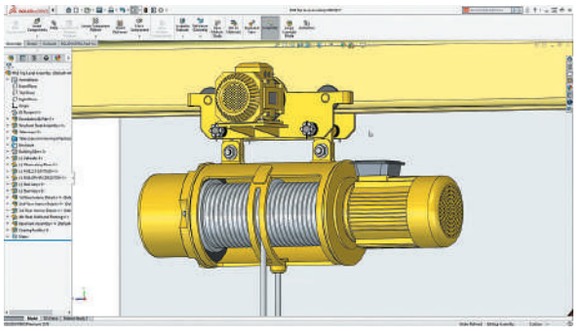
SOLIDWORKS Sell – это решение, которое позволяет инженерам поделиться данными 3D моделей с руководством для принятия решений, с отделом маркетинга для продвижения продукции, с отделом продаж для демонстрации продуктов покупателям. Или же сразу разместить модель в интернет магазине для заказчиков. Важнее 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

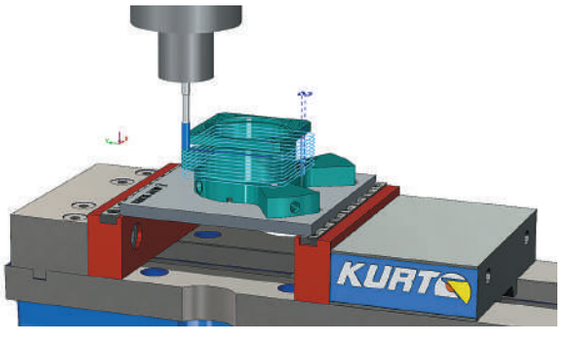


Попав на страничку с изделием в SOLIDWORKS Sell пользователь имеет ряд преимуществ перед обычным конфигуратором:

- 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.

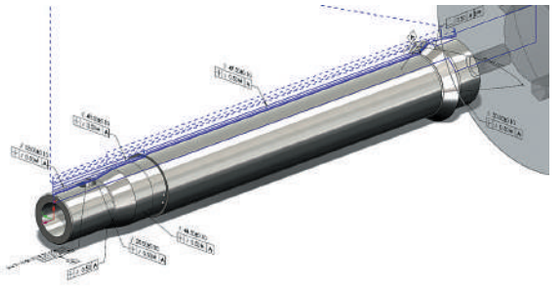
Преимущества



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:

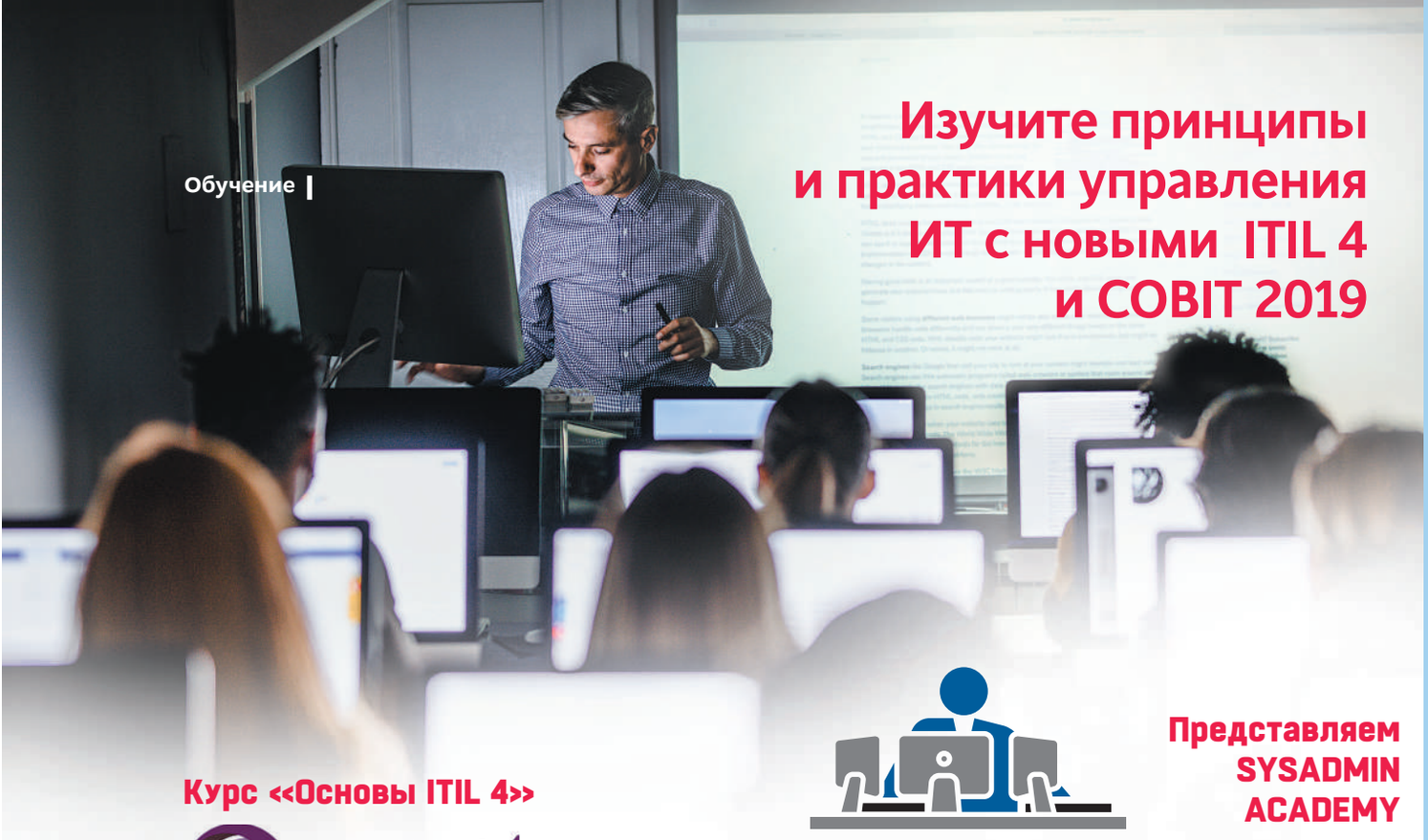
- Customize
- Digital Catalog
- eCommerce

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:
Владимир Фонов, менеджер по направлению «Машиностроение»
Тел: +375(17)336-55-95 (доб. 4527) | M +375(29)571-57-61
Vladimir.Fonov@softlinegroup.com



Изучите принципы и практики управления ИТ с новыми ITIL 4 и COBIT 2019

Курс «Основы ITIL 4»

ITIL® 4 FOUNDATION

Курс формирует общий словарь, основные принципы и понятия ИТ-сервис-менеджмента. Его программа поможет освоить последующие более специализированные и продвинутые тренинги ITIL 4.
Обучение проводится по авторской методике и позволяет подготовиться к официальному экзамену ITIL 4 Foundation. Ряд практик универсален и применим даже за рамками ИТ-области, в области бизнеса, организаций любого масштаба и повышает личную эффективность.

Курс «Основы COBIT 2019»

COBIT 2019

Обучение по новой версии методологии COBIT 2019 поможет организациям наладить взаимопонимание и соответствие между ИТ и бизнесом, понять пользу и принципы построения системы руководства и управления по модели COBIT 2019, синхронизировать словарь терминов, понимать принципы адаптации, управления производительностью и проведения оценки/аудита.
Данный трехдневный курс ориентирован на руководителей ИТ-подразделений, также будет полезен ИТ-сотрудникам любого уровня и руководителям бизнес единиц.

Представляем SYSADMIN ACADEMY

Хотите освоить профессию системного администратора или только начали работу и нужны уверенные знания и навыки?
Профессиональный сисадмин должен хорошо знать работу клиентских и серверных операционных систем (Windows 10, Windows Server 2016), уметь настроить сеть предприятия (подключение, роутеры, маршрутизаторы), а также оперативно устранять неисправности в их работе и обеспечивать безопасность.
Учебный центр Softline предлагает новую комплексной программу обучения, состоящую из четырех частей и включающую получение практических знаний по основам локальный сетей Cisco, а также установке и настройке Windows и Windows Server.

- Часть 1 «Системный администратор. Elementary»
- Часть 2 «Системный администратор. Pre-Intermediate»
- Часть 3 «Системный администратор. Intermediate»
- Часть 4 «Системный администратор. Advanced»

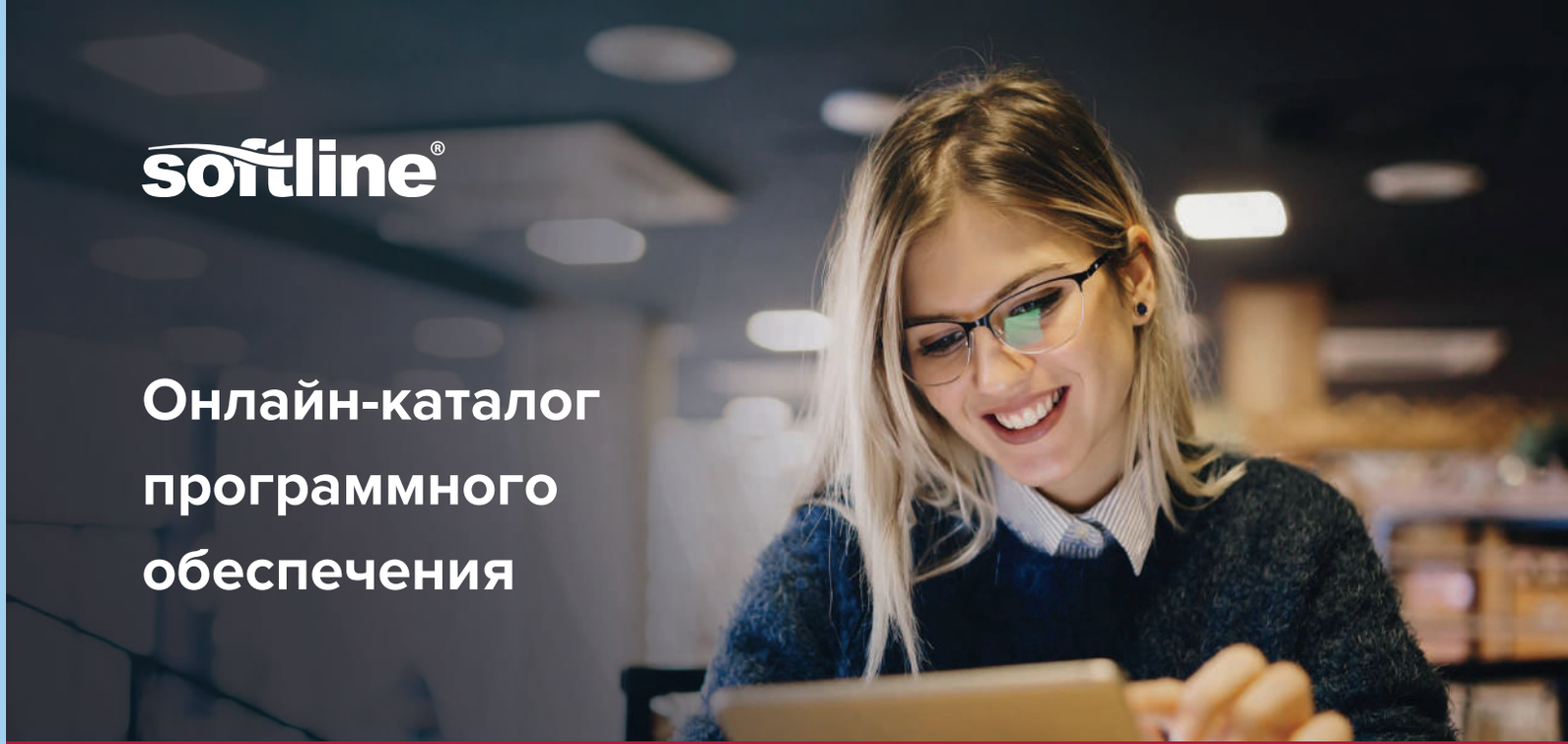
Каждая часть программы длится 5 недель. Обучение проходит 2 раза в неделю по будним дням с 18:00 до 21:00.

cisco Networking Academy

Блок обучения по сетям проводится в сотрудничестве с сетевой академией Cisco по программе CCNA R&S. Обучение насыщенно практическими работами, слушатели выполняют домашние задания и сдают экзамены, по результатам которых могут получить скидку 50% на экзамен Cisco CCNA. По окончании слушателям выдается сертификат компании Cisco.

Хотите записаться на курсы?

Заходите на наш сайт **http://edu.softline.by**, знакомьтесь с расписанием и программами обучения, нажимайте «Записаться» для оформления заявки, и наши специалисты свяжутся с вами для оформления документов.



softline®

Онлайн-каталог программного обеспечения

Для малого и среднего бизнеса

Преимущества:

- Более 5 000 позиций оборудования и программного обеспечения
- Получение счета и шаблона договора на ваш электронный адрес
- Автоматическая отправка бухгалтерских документов заказной почтой
- Выставление электронных счет-фактур на портале МНС
- Оперативная доставка электронных лицензий
- Работаем по всей Беларуси
- Поставка эксклюзивного программного обеспечения

Microsoft · Adobe · embarcadero · kaspersky · AUTODESK · VEEAM

ATLASSIAN · ABBYY · DevExpress · Acronis · COREL · eset · Dr.WEB

store.softline.by

+375 (17) 336-55-10

Код	Название курса	Дни/часы
Microsoft		
Курсы Windows Server 2012		
20410	Установка и конфигурирование Windows Server 2012 R2	5 /40
20411	Администрирование Windows Server 2012 R2	5 /40
C20410+20411	Администрирование и настройка Windows Server 2012 R2	5 /40
20412	Дополнительные службы Windows Server 2012 R2	5 /40
20413	Проектирование и реализация серверной инфраструктуры	5 /40
20414	Реализация продвинутой серверной инфраструктуры	5 /40
10991	Основные технологии устранения неисправностей в Windows Server 2016	5 /40
10969	Службы Active Directory в Windows Server	5 /40
Курсы Windows Server 2016		
20740	Установка, организация хранилища и работа в Windows Server 2016	5 /40
20741	Настройка сети в Windows Server 2016	5 /40
20742	Службы проверки подлинности (Active Directory) в Windows Server 2016	5 /40
20743	Обновление навыков до MCSA: Windows Server 2016	5 /40
20744	Обеспечение безопасности Windows Server 2016	5 /40
10961	Автоматизация администрирования с использованием Windows PowerShell	5 /40
10962	Расширенная автоматизация администрирования с помощью Windows PowerShell	3 /24
MS-PKI	Развертывание инфраструктуры открытого ключа в среде Windows Server 2016	3 /24
Курсы Windows 10		
MD-100T	Установка, настройка, поддержка и безопасность Windows 10	5 /40
MD-101T	Управление современными устройствами	5 /40
10982	Поддержка и устранение неисправностей Windows 10	5 /40
20695	Развертывание корпоративных приложений и устройств с Windows	5 /40
Курсы SQL Server 2014		
20461	Создание запросов к Microsoft SQL Server	5 /40
20462	Администрирование баз данных Microsoft SQL Server	5 /40
Курсы SQL Server 2016		
20761	Создание запросов данных при помощи Transact-SQL	5 /40
20762	Разработка баз данных SQL	5 /40
20764	Администрирование инфраструктуры баз данных SQL	5 /40
10987	Настройка производительности и оптимизация баз данных SQL	3 /24
10988	Управление операциями бизнес-аналитики SQL	3 /24
10990	Анализ данных при помощи SQL Server Reporting Services	3 /24
Курсы Exchange Server 2016		
20345-1	Администрирование Microsoft Exchange Server 2016	5 /40
20345-2	Проектирование и развертывание Microsoft Exchange Server 2016	5 /40
Курсы Microsoft SharePoint 2016		
20339-1	Планирование и администрирование SharePoint 2016	5 /40
20339-2	Расширенные технологии SharePoint 2016	5 /40
Курсы Visual Studio		
20480	Программирование на HTML5 с использованием JavaScript и CSS3	5 /40
20483	Программирование на C#	5 /40
Курсы Systems Center Configuration Manager		
20703-1	Администрирование System Center Configuration Manager	5 /40
20703-2	Интеграция MDM и облачных сервисов с System Center Configuration Manager	3 /24
10748	Планирование и развертывание System Center 2012 Configuration Manager	3 /24
Курсы по виртуализации серверов		
MS-RDS	Установка и конфигурирование служб удаленных рабочих столов	2 /16
20694	Виртуализация корпоративных рабочих столов и приложений	5 /40
10324	Внедрение и управление инфраструктурой виртуализации рабочих станций Microsoft	5 /40
10215	Внедрение и сопровождение платформы виртуализации на базе Microsoft Server	5 /40

Код	Название курса	Дни/часы
Курсы Microsoft Project		
55054	Освоение Microsoft Project 2013	3 /24
55056	Управление проектами с Microsoft Project 2013	5 /40
55180	Введение в Microsoft Project 2016: начало работы	2 /16
55201	Управление проектами с Microsoft Project 2016	5 /40
Курсы Microsoft Office		
VBA-Excel	Программирование на VBA для Microsoft Excel	4 /32
BI-Excel-Adv	Бизнес-аналитика средствами Microsoft Excel, Power BI и Power BI Desktop	4 /32
O365	Использование Office 365	3 /24
Cisco		
Курсы Cisco по маршрутизации и коммутации		
ICND1	Использование сетевого оборудования Cisco. Часть I	5 /40
ICND2	Использование сетевого оборудования Cisco. Часть II	5 /40
ROUTE	IP-маршрутизация на базе оборудования Cisco	5 /40
SWITCH	Внедрение коммутируемых сетей Cisco	5 /40
TSHOOT	Поиск и устранение неисправностей в IP-сетях Cisco	5 /40
Курсы Cisco по безопасности		
IINS	Применение системы сетевой безопасности на базе Cisco IOS	5 /40
SISAS	Внедрение решений Cisco для безопасного доступа	5 /40
SENSS	Развертывание решений Cisco по обеспечению безопасности границ сети	5 /40
SIMOS	Внедрение решений Cisco для безопасной мобильности	5 /40
SITCS	Развертывание решений Cisco по контролю за угрозами (v1.5) NEW	5 /40
SASAC	Реализация базовой сетевой защиты с использованием Cisco ASA	5 /40
SASAA	Реализация повышенной сетевой защиты с использованием Cisco ASA	5 /40
SISE	Внедрение и настройка Cisco Identity Services Engine	5 /40
SWSA	Защита доступа в интернет с использованием Cisco Web Security Appliance (SWSA) v3.0	2 /16
Курсы Cisco по беспроводным сетям		
WIFUND	Основы внедрения беспроводных сетей Cisco	5 /40
WIDESIGN	Проектирование корпоративных беспроводных сетей Cisco	5 /40
WIDEPLOY	Развертывание корпоративных беспроводных сетей Cisco	5 /40
WITSHOOT	Устранение неисправностей корпоративных беспроводных сетей Cisco	5 /40
WISECURE	Обеспечение безопасности корпоративных беспроводных сетей Cisco	5 /40
WDBWL	Развертывание базовых беспроводных сетей Cisco LAN	3 /24
WDAWL	Развертывание сложных беспроводных сетей Cisco LAN	2 /16
Курсы Cisco Design		
DESGN	Дизайн распределенных сетей Cisco	5 /40
ARCH	Проектирование сетей Cisco	5 /40
Курсы Cisco Service Provider		
QOS	Реализация QoS в сетях Cisco	5 /40
MPLS	Реализация мультипротокольной коммутации с использованием меток в сетях Cisco	5 /40
BGP	Настройка BGP на маршрутизаторах Cisco	5 /40
IP6FD	Основы протокола IPv6, дизайн и построение сетей на его основе	5 /40
Oracle		
12cDBA	Администрирование Oracle Database 12c	5 /40
12cSQL1	Oracle Database 12c: основы SQL 1	3 /24
12cSQL2	Oracle Database 12c: основы SQL 2	2 /16
12cPLSQL	Oracle Database 12c: основы PL/SQL	2 /16
12cDPU	Oracle Database 12c: разработка программных модулей на PL/SQL	3 /24
12cAPLS	Oracle Database 12c: передовые методы PL/SQL	3 /24
12cTSQL	Oracle Database 12c: настройка SQL-операторов баз данных	3 /24
12cASQL	Oracle Database 12c: аналитические функции SQL в хранилищах данных	2 /16
12cBAR	Oracle Database 12c: резервирование и восстановление	5 /40

Код	Название курса	Дни/часы
WLS-AE	Основы администрирования сервера приложений Oracle Weblogic	5 /40
Oracle BI	Oracle BI Server: создание, организация совместного использования аналитических web-витрин и отчетов во всех стандартных форматах	5 /40
Linux		
RH7-124	Системное администрирование Red Hat Linux 7. Часть 1	5 /40
RH7-134	Системное администрирование Red Hat Linux 7. Часть 2	5 /40
RH7-254	Системное администрирование Red Hat Linux 7. Часть 3	5 /40
SL-105	Администрирование SUSE Linux	5 /40
SL-106	Углубленный курс по администрированию SUSE Linux	5 /40
SL-107	Администрирование SUSE Linux Enterprise Server 12	5 /40
VMware		
VSICM 6.7	VMware vSphere: установка, настройка, управление [V6.7]	5 /40
VSOS 6.7	VMware vSphere: оптимизация и масштабирование [V6.7]	5 /40
VSRM 6.1	VMware Site Recovery Manager: Install, Configure, Manage [V6.1]	2 /16
NSXICM 6.4	VMware NSX: установка, настройка, управление [V6.4]	5 /40
VHICM 7.7	VMware Horizon 7: установка, настройка, управление [V7.7]	5 /40
vSANDM	VMware vSAN 6.7: развертывание и управление	3 /24
vSANTW	VMware vSAN v6.x: устранение неполадок	2 /16
VROICM7	VMware vRealize Operations: установка, настройка и использование [V7]	5 /40
VRAICM 7.3	VMware vRealize Automation: установка, настройка, управление [V7.3]	5 /40
“Лаборатория Касперского”		
KL 002.11.1	Kaspersky Endpoint Security and Management. Базовый курс	3 /24
KL 302.10	Kaspersky Endpoint Security and Management. Масштабирование	1 /8
KL 008.104	Kaspersky Endpoint Security and Management. Шифрование	1 /8
KL 009.11	Kaspersky Endpoint Security and Management. Управление системами	1 /8
Управление проектами		
PMBOK	Практика управления проектами на основе стандарта PMBOK	3 /24
PM-Risk	Прикладное управление рисками проекта	2 /16
IT-Project	Управление ИТ-проектами	3 /24
PM-Scrum	Впереди изменений, или Scrum в действии	2 /16
PM-Agile	Гибкое управление проектами разработки ПО	2 /16
ИТ-сервис менеджмент		
ITIL 4	NEW! Основы ITIL 4	3 /24
OSA	ITIL OSA - операционная поддержка и анализ (Operational Support And Analysis)	4 /32
RCV	ITIL RCV - релизы, контроль и валидация (Release, Control & Validation)	4 /32
SOA	ITIL SOA - предложение услуг и подготовка соглашений (Service Offerings and Agreements)	4 /32
COBIT 2019	NEW! Основы COBIT 2019	3 /24
Информационная безопасность		
ОИБ	Основы информационной безопасности	3 /24
ISMS	Разработка, внедрение и аудит системы менеджмента информационной безопасности в соответствии с требованиями ISO/IEC 27001:2013 (СТБ ISO/IEC 27001-2016)	5 /40
ISA	Аудит информационной безопасности	4 /32
CyberSecurity	Обеспечение кибербезопасности и защита информации в организации	5 /40
ISRM	Оценка и управление рисками информационной безопасности в организации	2 /16
ISRM-Bank	Оценка и управление рисками нарушения информационной безопасности банка	3 /24
САИС	Создание автоматизированных систем в защищенном исполнении	3 /24
КТ	Защита коммерческой тайны и организация конфиденциального делопроизводства	2 /16
CS	Безопасность облачных вычислений (Cloud Security)	3 /24

Полный каталог курсов и подробные программы обучения вы можете найти на нашем сайте **http://edu.softline.by**
Получить дополнительную информацию по курсам можно
по телефону **+375 (17) 336-55-41** или e-mail **edu.by@softline.com**

Учебный центр Softline – то, что нужно для развития!

Учебный центр Softline – это:

- более 1000 курсов различной тематики и уровня сложности;
- авторизации от ведущих производителей программного обеспечения;
- комфортные и современно оборудованные учебные классы;
- высококвалифицированные тренеры с богатым практическим опытом работы;
- широкий перечень курсов в дистанционном формате, которые можно пройти, присоединившись к занятию, проводимому в классе очно;
- международные сертификаты для IT-специалистов и пользователей в авторизованных центрах тестирования.

85% клиентов обращаются к нам повторно

Лучший выбор авторизованных курсов

Мы обучили более 5 000 слушателей

Учебный центр Softline – лидер в сфере IT-образования, обладающий широкой сетью из более чем 35 представительств, расположенных в Беларуси, России и других странах, что позволяет сделать качественное обучение доступным большому числу IT-специалистов.

Все курсы в нашем Учебном центре проводят сертифицированные тренеры, имеющие многолетний практический опыт и основательную педагогическую подготовку.

Расписание курсов смотрите на сайте edu.softline.by

softline®

Курсы

- Microsoft
- Cisco
- VMware
- Citrix
- Oracle
- Red Hat Linux
- Kaspersky Lab
- ITSM / ITIL
- Управление проектами
- Autodesk
- Veeam
- Symantec
- Check Point
- Информационная безопасность
- 1С:Предприятие 8

Сертификация

kaspersky

PEARSON VUE AUTHORISED CENTRE

Контакты

г. Минск, 220062
пр-т Победителей,
д. 110, этаж 5
+375 (17) 336-55-41
edu.by@softline.com

ГЛОБАЛЬНЫЙ ПОСТАВЩИК ИТ-РЕШЕНИЙ И СЕРВИСОВ

- Облачные решения
- Кибербезопасность
- Инфраструктура
- Бизнес-решения
- Техническая поддержка
- САПР и ГИС
- Учебный центр

+375 (17) 336-55-95 | www.softline.by