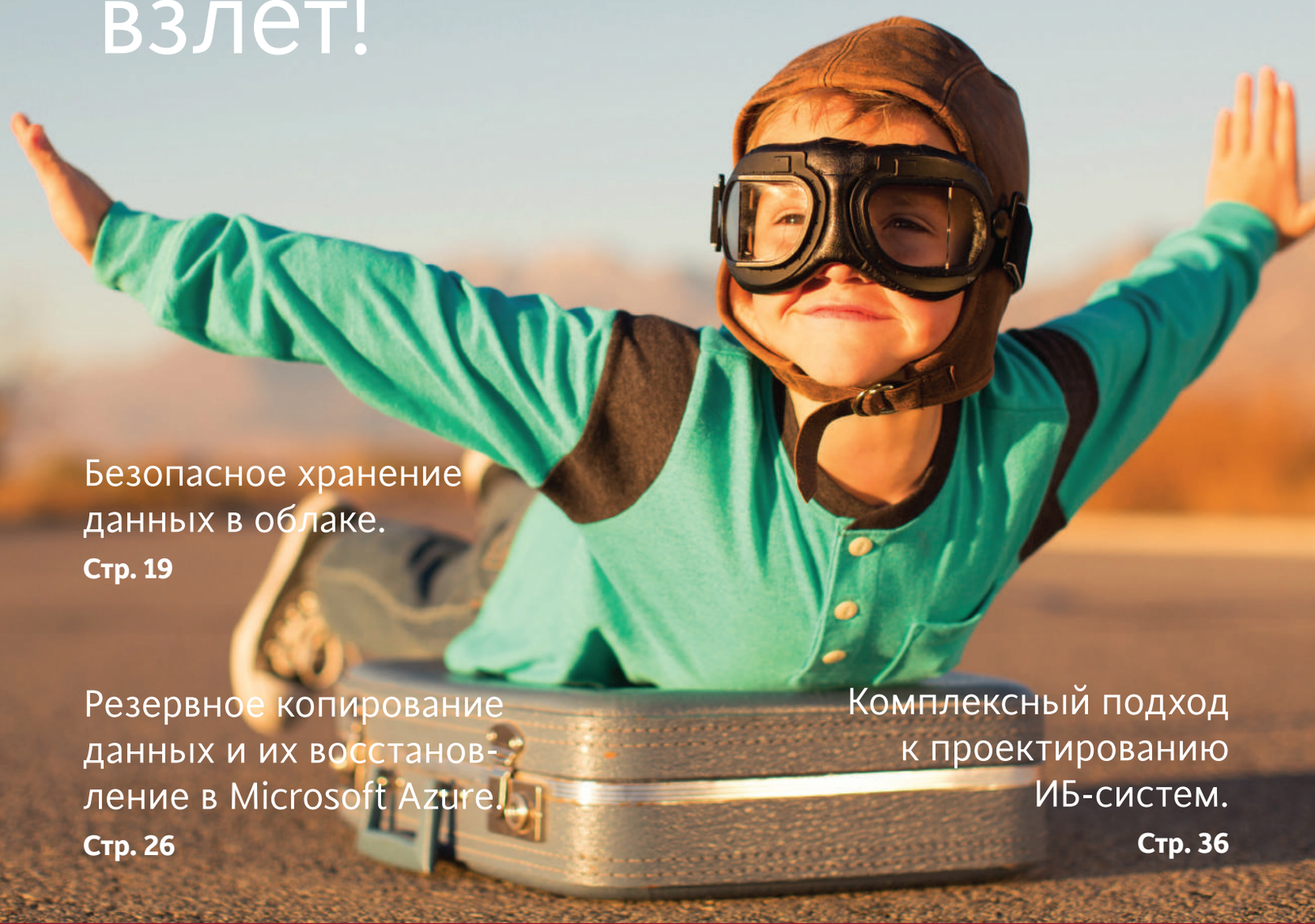
softline direct

КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1 (32)
2018 BY

Настройтесь на безопасный взлет!



Безопасное хранение данных в облаке.
Стр. 19

Резервное копирование данных и их восстановление в Microsoft Azure.
Стр. 26

Комплексный подход к проектированию ИБ-систем.
Стр. 36

+375 (17) 388-95-95

www.softline.by


G O D
SAVE THE
CLOUD
www.softlinecloud.by

Уважаемые коллеги!

Мы рады представить вам новый выпуск каталога Softline-direct.

В условиях бурного развития цифровой экономики нам важно слышать и понимать клиентов, помогая им успевать за высокими темпами перемен. Известно, что любое изменение в инфраструктуре и процессах работы компании предоставляет новые возможности и для злоумышленников.

Каждый год Softline осуществляет сотни проектов по проверке защищенности отдельных систем, веб- или мобильных приложений. Наши специалисты выполняют комплексный аудит информационной безопасности крупнейших ИТ-систем международного уровня. Мы хорошо знаем схемы мошенничества в разных отраслях бизнеса и можем гарантировать клиентам качество и приемлемую стоимость внедрения решений для обеспечения информационной безопасности.

Отдельная рубрика нового выпуска посвящена кибербезопасности, как одному из приоритетных направлений деятельности Softline, и решениям, которые мы считаем наиболее актуальными в текущем году.

Мы поговорим на тему использования облачных технологий в контексте законодательства и расскажем, почему это безопасно как с технической, так и с юридической точки зрения. Руководитель департамента Microsoft Максим Павловский расскажет о соблюдении требований по работе с персональными данными при переходе в облако.

Стратегия развития компании Softline направлена на повышение эффективности бизнеса своих клиентов с промощью передовых информационных технологий. Непрерывность бизнес-процессов и экономию времени на осуществление послеаварийного восстановления обеспечит новое решение Veeam Availability Orchestrator, о котором вы узнаете в разделе «Резервное копирование». Также мы расскажем о корпоративной платформе для осуществления безопасного доступа к любому приложению с любого устройства – Workspace ONE.

Сегодня решение задач автоматизации производства невозможно представить без средств компьютерного моделирования и инженерной графики. Мы расскажем о мощных функциональных возможностях программ для 3D-моделирования Autodesk и 3D-принтерах MakerBot, которые помогут вам создать более совершенные проекты с меньшими затратами.

Многолетний опыт и высокий уровень профессионализма команды Softline позволяет нам решать задачи любой сложности, делать невозможное возможным. Мы рады предложить вам наилучшие условия по организации ИТ-инфраструктуры вашей компании.

С пожеланиями успеха и процветания,

Андрей Овсейко, генеральный директор компании Softline Беларусь

Каталог ИТ-решений и сервисов для бизнеса

Softline direct

МАЙ

2018-1(32)-BY

Учредитель: ООО «СофтЛайн Директ»

Главный редактор: Людмила Васильевна Пешкун

Выпускающий редактор: Яна Ламзина

Редактор: Инна Савончик

Дизайн и верстка: Константин Косачев

Адрес редакции: 220040, г. Минск, ул. Богдановича, д. 155, офис 1201

Распространяется бесплатно.

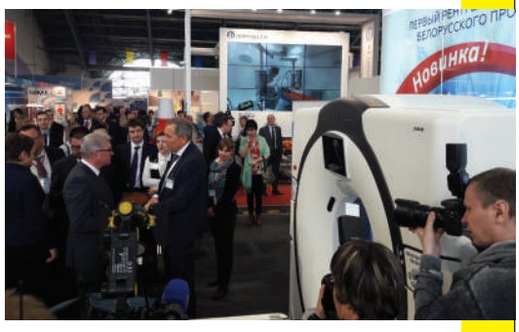
Тираж: 3000 экз.

Подписано в печать 31.05.2018. Отпечатано в типографии ООО «ТриАпринт», Минская обл., Минский р-н, а.г. Острошицкий Городок, ул. Ленина, 1 Свидетельство №2/87 от 19.07.2016 Заказ № р795

Зарегистрировано в Министерстве информации РБ. Свидетельство о регистрации № 1396 от 24.12.10

Контактная информация: marketing@softline.by

СОДЕРЖАНИЕ



САПР

Интервью номера

Результаты и дальнейшие планы географической экспансии Softline. В проработке – развитие бизнеса в Восточной Европе, а также усиление позиций в Латинской Америке и в Юго-Восточной Азии. В перспективе – Африка. **Стр. 6**

Инновационные технологии в серверах HPE ProLiant поколения Gen10

Цель разработки семейства Gen 10 – обеспечение максимальной защищенности решений и абсолютной безопасности инфраструктур заказчиков. Благодаря чипам собственного производства компании HPE iLO удалось обеспечить безопасность на всех этапах жизненного цикла сервера. **Стр. 48**

Аддитивные технологии в учебных лабораториях

Создавая специализированные лаборатории, учреждения среднего, средне-специального и высшего образования не только делают учебный процесс наглядным и запоминающимся, но и повышают свой престиж, давая своим студентам знания, соответствующие запросам современного мира. **Стр. 56**

Softline в соцсетях SoftlineBelarus @softline_belarus Softline Belarus

Облачные решения

Резервное копирование

Цифровизация

Безопасность

Аппаратные решения

Обучение

ПОРТРЕТ КОМПАНИИ

Наша миссия

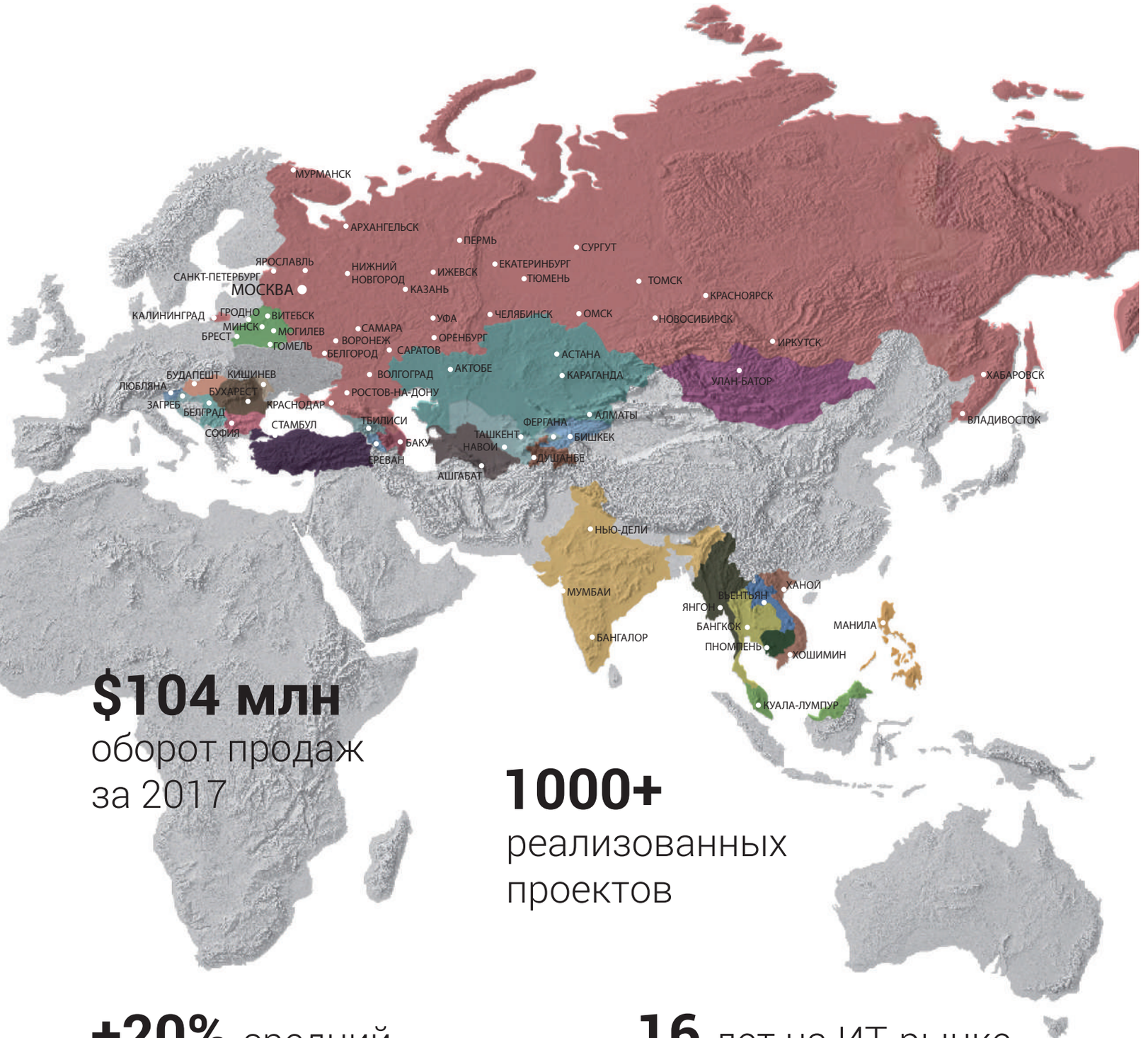
Мы осуществляем цифровую трансформацию бизнеса наших клиентов на основе передовых информационных технологий и средств кибербезопасности.

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



$104 млн
оборот продаж
за 2017

1000+
реализованных
проектов

+20% средний
ежегодный рост продаж

16 лет на ИТ-рынке
Беларуси

Генеральный директор
Softline International
Игорь Петляков

В середине 2000 годов группа компаний Softline начала географическую диверсификацию бизнеса. Сначала ее представительства появились в странах ближнего зарубежья, потом пришло время дальнего. В настоящее время офисы Softline находятся в полусотне городов 29 зарубежных стран. Генеральный директор Softline International Игорь Петляков рассказал о том, почему было принято решение о начале географической экспансии, по какому принципу выбираются страны для открытия офисов, как происходит выход на новые рынки и о том, не мешает ли международному бизнесу политическая обстановка.

— Когда формально стартовал интернациональный проект? В 2004 году в списке иностранных офисов фигурировали Минск, Алма-Ата и Ташкент, в 2006 — офисы появились в 10 странах, а в 2008 — в 13.

— Развитие бизнеса в странах дальнего зарубежья началось с открытия офисов в Турции и Вьетнаме в 2008 году. К тому моменту компания уже несколько лет успешно работала на территории ближнего зарубежья. Было очевидно, что российский опыт можно перенести на рынки других стран, поэтому идея начать работать с дальним зарубежьем стала естественным шагом развития бизнеса Softline.

Результаты и дальнейшие планы **географической экспансии Softline**

SOFTLINE ЗА ПОСЛЕДНИЕ ТРИ ГОДА ПРЕДПРИНЯЛА НЕСКОЛЬКО ПОГЛОЩЕНИЙ НА КЛЮЧЕВЫХ ДЛЯ СЕБЯ РЫНКАХ — В РОССИИ И ЛАТИНСКОЙ АМЕРИКЕ.

Немного раньше, в 2007 году, у Игоря Боровикова, основателя группы компаний Softline и председателя совета ее директоров, возникла идея выйти на IPO. Инвесторы верят в компании с мощным и диверсифицированным бизнесом. Уже на тот момент стало ясно, что Softline, у которой есть бизнес в России, странах ближнего и дальнего зарубежья, вполне соответствует этим критериям.

Сейчас ситуация подходящая: Softline за последние три года предприняла несколько поглощений на ключевых для себя рынках — в России и Латинской Америке. В капитал компании вошли крупные инвесторы, Softline открыла историю публичного долга, разместив на Московской бирже свои облигации.

— Какие признаки отличают страны, потенциально перспективные для бизнеса? Как осуществляется выход на рынок: через создание новой структуры, покупку местной компании?

— Мы стараемся выбирать крупные и средние страны с большим потенциалом роста экономики, в которых ниже уровень конкуренции на ИТ-рынке, и где ниже уровень развития информационных технологий, чем в России.

Помимо этого, мы советуемся с вендорами. Их сведения удачно обогащают ту картину ситуации, которая складывается у нас. В ходе диалога также становится понятно, готовы ли вендоры поддерживать нас на новом рынке. Фактор поддержки часто является определяющим.

Что касается стратегии выхода, на первом этапе международного развития мы предпочитали учреждать локальные «дочки» и формировать команды. Но в ряде случаев более рациональным вариантом выглядит покупка уже готовой компании. Например, так мы поступили в Бразилии, приобретя компанию Compusoftware. На данный момент поглощение компаний – приоритетная стратегия роста. Покупка действующего бизнеса помогает понять ситуацию на рынке изнутри.

— У компании весьма широкое предложение продуктов и услуг, вряд ли в каждой стране найдется полный штат специалистов по всем тематикам. Как устроено ведение проектов, осуществление их поддержки?

— Широта предложения обусловлена тем, что, с учетом общей тенденции падения маржинальности продаж ПО, невозможно быть прибыльной компанией, не предоставляя услуги и не делая комплексные ИТ-проекты. Менеджеры проектов работают «на местах». Все, что касается технической и технологической составляющей этих проектов, организуется удаленно. Например, из России, Беларуси, Индии. В Индии достаточно большой офис, там работает около 150 человек.

— В развитых странах — свои мощные интеграторы и провайдеры сервисов, сложное трудовое законодательство. В развивающихся — неочевидные законы и предпочтение «своим» компаниям. Как в Softline справляются с такими особенностями?

— Разумеется, особенности есть везде. Мы стараемся о них узнавать заранее. Ранее, когда выход на новые рынки осуществлялся через создание представительств, все страновые особенности нивелировались благодаря опыту местных менеджеров, из которых мы формировали команды. В рамках стратегии расширения, связанной с покупкой компаний, вопрос местных особенностей перестал быть актуальным. Мы сохраняем команды приобретаемых компаний. Для этих команд то, что мы воспринимаем как особенности, — привычная бизнес-среда.

В плане предпочтений мы также не заметили какого-либо противодействия. Во-первых, даже в составе группы Softline локальные компании продолжают восприниматься как «свои». Во-вторых, на рынках, которые по уровню развития немного отстают от российского, заказчикам важно получить экспертизу более глубокую, чем та, которую могут предоставить наши локальные конкуренты.

— Повлияла ли на зарубежный бизнес нынешняя международная обстановка?

— Мы учитываем страновые риски и не работаем там, где они высоки. Кроме того, как я уже говорил, купленную нами компанию, как правило, продолжают воспринимать как «свою». Так что каких-то особенных проблем не возникает.

— Какую долю в обороте компании занимает международный бизнес?

— Softline объявляет консолидированные финансовые результаты по группе компаний в целом, поэтому мы не разглашаем показатели бизнеса в дальнем зарубежье или в конкретной стране. Кроме того, ценность международного бизнеса состоит не только в его обороте. Благодаря нему Softline — глобальная компания, ее выручка диверсифицирована по ключевым регионам. Ну и, как я говорил, диверсификация важна с точки зрения инвесторов. Они видят, как глобальный статус Softline снижает риски, связанные с рынком конкретных стран. Число инвесторов у Softline растет. Думаю, это лучше всего говорит о том, насколько международная составляющая бизнеса важна для компании в целом.

— Есть планы по дальнейшему проникновению по планете, или перспективные страны уже освоены?

— В проработке – развитие бизнеса в Восточной Европе, а также усиление позиций в Латинской Америке и в Юго-Восточной Азии. В перспективе – Африка.

Источник: Computerworld Россия

В ПРОРАБОТКЕ – РАЗВИТИЕ БИЗНЕСА В ВОСТОЧНОЙ ЕВРОПЕ, А ТАКЖЕ УСИЛЕНИЕ ПОЗИЦИЙ В ЛАТИНСКОЙ АМЕРИКЕ И В ЮГО-ВОСТОЧНОЙ АЗИИ. В ПЕРСПЕКТИВЕ – АФРИКА.

МЫ СТАРАЕМСЯ ВЫБИРАТЬ КРУПНЫЕ И СРЕДНИЕ СТРАНЫ С БОЛЬШИМ ПОТЕНЦИАЛОМ РОСТА ЭКОНОМИКИ, В КОТОРЫХ НИЖЕ УРОВЕНЬ КОНКУРЕНЦИИ НА ИТ-РЫНКЕ, И ГДЕ НИЖЕ УРОВЕНЬ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЧЕМ В РОССИИ.

Клиенты Softline посетили Microsoft Technology Center

Microsoft Technology Center (MTC) – единственный в странах СНГ и один из самых масштабных проектов компании. Специализированная площадка с инновационным оборудованием позволяет демонстрировать и тестировать передовые технологии, проводить презентации для партнеров и заказчиков, семинары для ИТ-специалистов и брифинги для журналистов. Основная задача центра – предоставление заказчикам и партнерам возможности познакомиться с современными ИТ-технологиями: от инструментов в области корпоративной мобильности до сложнейших решений по построению современных ЦОДов.

В ходе экскурсии по центру было представлено расширение для платформы Microsoft Azure — Azure Stack. Расширение обеспечивает гибкость и высокую скорость внедрения инноваций облачной среды в локальной среде. С помощью Azure Stack клиенты могут предоставлять службы Azure из собственного центра обработки данных, поддерживать баланс между гибкостью и контролем и обеспечивать по-настоящему согласованные гибридные облачные развертывания.

На стенде AddReality, платформы для создания и управления интерактивным контентом на экранах, были продемонстрированы возможности когнитивных сервисов Microsoft (Azure Cognitive Services).

«Дополнительный уровень защиты для многих отраслей – API распознавания лиц. Функция работает следующим образом: клиент подходит к видеокамере, расположенной под экраном, и система автоматически считывает его возраст, пол, эмоции. И если фотография клиента занесена в базу, то система распознает даже его ФИО, а также показывает всю историю пребывания и действий клиента в данной организации», — рассказывает руководитель департамента Microsoft Softline Максим Павловский.

Эксперты Microsoft отметили возможности умных зеркал, которые позволяют примерять любую одежду в магазине, а также, не переодеваясь, менять ее цвета с помощью простого движения руки.

В отдельном шоу-руме, оснащенном множеством мониторов, всевозможной аппаратурой, был показан один день из жизни цифровой организации. На сцене располагались три зоны – для «руководителя», «маркетолога» и «коммерческого директора». В ходе презентации «коллеги» демонстрировали, как Microsoft 365 и его отдельные решения (Microsoft Teams, Outlook, SharePoint, OneNote и др.) помогают эффективно решать ежедневные задачи, оперативно принимать решения, организовывать взаимодействия сотрудников, обрабатывать полученную информацию, сокращать затраты и повышать производительность компании.

Возможности еще одного решения Microsoft – Skype for Business – были продемонстрированы с помощью современных видеокамер для конференций Polycom. Одна из поворотных камер системы фокусировалась на объекте (ориентируясь на голос) и выводила на экран самого спикера, другая – держала общий вид, транслировала презентацию на второй экран. Эксперты центра показали, как прямо с рабочего ноутбука или телефона можно звонить или подключаться к проходящей в переговорной комнате конференции.

Особым вниманием слушателей была отмечена презентация о цифровой безопасности компании. На примере конкретной организации спикер наглядно показал, как злоумышленники могут похитить данные, и что необходимо предпринять для их защиты, а также подробно рассказал о решениях для защиты локальных и персональных компьютеров: Windows 10 Enterprise, Windows Server, EMS (Enterprise Mobility + Security), Azure Active Directory Premium и др.

С помощью Microsoft Surface Hub, так называемого «стенда для коллективной работы», эксперт Microsoft моментально отправлял все созданные им данные слушателям на e-mail.

Отдельные темы семинара были посвящены машинному обучению, большим данным и аналитике нового поколения – инструменту Power BI. Клиенты узнали, как получать и использовать информацию в интересах бизнеса, как использовать данные в применении к различным сегментам рынка, как подключаться к сотням источников информации, упрощать ее обработку, создавать отчеты и совместно работать с ними.

Спикер компании Softline поделился успешным внедрением интернета вещей для «Криогенмаш», крупнейшей компании в России по производству технологий и оборудования для разделения воздуха, снабжения техническими газами и разработке комплексных решений по переработке попутного, природного газа и СПГ. Заказчику потребовалось решение, которое бы позволяло специалистам удаленно проводить мониторинг параметров криогенной воздухоразделительной установки и сохранять архив данных для последующей обработки. Разработанный специалистами Softline IoT-сервис, интегрированный с облаком Azure, помог компании получить доступ с любого устройства и из любой точки мира к данным, снимаемым с датчиков воздухоразделительной установки.

В течение семинара архитекторы Технологического центра Microsoft и эксперты Softline поделились своим опытом, помогли клиентам Softline увидеть и разработать собственную стратегию для решения задач, повышения производительности и эффективности бизнеса.

Компания Softline подтвердила самый высокий статус партнерства VMware

Начиная с 2016 года компания Softline успешно подтверждает наивысший статус партнерства мирового лидера виртуализации компании VMware – VMware Solution Provider Premier Partner.

Ежегодное подтверждение статуса характеризует Softline как надежного партнера в реализации проектов по виртуализации инфраструктуры любой сложности для организаций всех отраслей и размеров бизнеса.

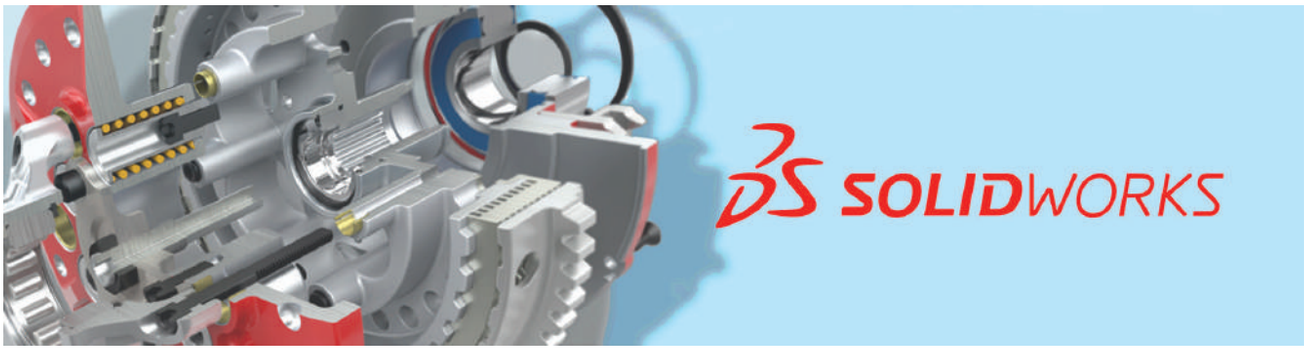
Мы постоянно наращиваем свою экспертизу, получая новые технологические компетенции VMware, а наши специалисты повышают свои технические знания в инновационных решениях вендора, что гарантирует профессиональный подход к задачам клиентов и высокое качество поддержки на всех этапах проекта.

Сегодня Softline предлагает своим заказчикам полный спектр услуг по виртуализации ИТ-инфраструктуры с помощью решений VMware: от обследования ИТ-среды, в результате которого заказчик получает рекомендации по дальнейшему эффективному использованию своего серверного оборудования, до авторизованного обучения ИТ-специалистов и технических консультаций по установке и настройке. Сертифицированные эксперты компании помогут разработать и внедрить наиболее эффективные, гибкие и управляемые решения виртуализации VMware, которые не только повысят качество ИТ-услуг вашей компании, но и сократят издержки на развитие ИТ-инфраструктуры в дальнейшем.

Дополнительные компетенции Adobe в области образования

Компания Softline расширила свой постоянный статус реселлера Adobe и получила дополнительные компетенции в образовательной сфере. Таким образом, мы рады предложить образовательным учреждениям уникальные приложения Adobe и гибкие варианты лицензирования.

Используя решения Adobe, образовательные учреждения смогут внедрять современные цифровые технологии для всех устройств, которыми чаще всего пользуются учащиеся; выполнять детальный анализ данных и предоставлять информацию об интересах потенциальных учащихся с помощью Marketing Cloud, и на его основе организовывать набор учеников, отслеживать эффективность набора и корректировать его для достижения наилучшего результата; оптимизировать работу административного персонала с помощью Document Cloud для сокращения временных и денежных расходов на зачисление учащихся и введение в учебный процесс; использовать инструменты Creative Cloud для дизайна уникальных брошюр, приложений, электронных писем и других цифровых материалов, которые помогут вызвать интерес у потенциальных учащихся; эффективно управлять контентом с помощью Marketing Cloud для обеспечения согласованного представления бренда учебного заведения во всех информационных средах и многое другое.



Solidworks в портфеле САПР-решений компании Softline Беларусь

В январе 2018 года Softline получила статус авторизованного партнера компании Dassault Systemes Solidworks, одного из мировых лидеров в области решений для 3D-проектирования, создания цифровых 3D-макетов и управления жизненным циклом изделий.
Это сотрудничество позволяет компании Softline предложить белорусским предприятиям тяжелой и легкой промышленности широкий спектр программных решений САПР Solidworks, включая такие известные продукты, как Solidworks 3D CAD – решение для 3D-проектирования, Solidworks Simulation – решение для проведения расчетных исследований и инженерного анализа, Solidworks PDM – решение для организации единой среды проектирования и документооборота.
Компания Softline готова оказать полный спектр услуг по внедрению данных продуктов, их сопровождению и обучению специалистов работе с ними.

Конференция «e-Health – цифровая трансформация системы здравоохранения Республики Беларусь»

В рамках масштабной конференции «e-Health – цифровая трансформация системы здравоохранения Республики Беларусь» эксперты Softline рассказали об инновационных подходах к дистанционному обучению и проведению облачных конференций.
Технический специалист Softline Александр Шинкевич и менеджер по продажам услуг на базе технологий Microsoft Евгений Андрейчук отметили преимущества Skype for Business и IP-телефонии, как одного из решений Microsoft Office 365, позволяющего интегрировать удаленный рабочий персонал, получить мгновенный доступ к экспертизе и консультации лечащего врача-клинициста, проводить широковещательные веб-трансляции до 10 000 участников.
Александр Шинкевич рассказал об особенностях виртуального класса HPE MyRoom, позволяющего пройти обучение прямо за рабочим столом. В том числе, о таких преимуществах решения, как 18 языков интерфейса, функции шифрования аудио, видео и другого содержимого, доступ к комнатам без создания учетной записи, планирование событий и множество полезных функций.

В Беларуси зарегистрировано общественное объединение «Сеть бизнес-ангелов»

В конце апреля в Беларуси было зарегистрировано общественное объединение «Сеть бизнес-ангелов». По сути — это BAN (Business Angels Network). Такие сети есть в разных странах Европы: Польше, Литве, Латвии, Эстонии, Финляндии.

Белорусская ассоциация выбрала для себя звучное и живое название Angels Band. Регистрация заняла пару месяцев. Долгий срок, по словам представителей сообщества, обусловлен тем, что формат и специфика объединения были в новинку для учредителей и регистрирующих органов.

Сейчас в сети 15 бизнес-ангелов. Среди них — Кирилл Волошин, Виталий Денисенков, Кирилл Голуб, Дмитрий Матвеев, Таня Маринич, Настя Хоменкова, Сергей Дивин, Павел Гордон и др. Еще 30 человек могут присоединиться к сообществу в ближайшее время. Руководство объединения полагает, что через год сеть может увеличиться до 100 инвесторов.

Участники объединения изучают тему ангельского инвестирования около двух лет, у некоторых уже есть первые инвестиции в стартапы. Нужные знания некоторые инвесторы получили в Business Angels Academy, которую проводит бизнес-клуб Imaguru, а также в поездках по странам с развитыми экосистемами — США, Эстонии, Израиле.

В рамках союза бизнес-ангелы смогут объединяться в синдикаты и инвестировать в проекты сообща — это нормальная мировая практика. Таким образом инвестор распределяет свой капитал, формируя портфель из 10-20 разных стартапов. Вероятность успеха в этом случае выше, чем при инвестировании всех свободных денег в один проект. Планируется, что, участвуя в синдикате, каждый инвестор суммарно будет вкладывать 20-100 тысяч долларов в течение года в ряд проектов.

Сеть бизнес-ангелов интересуют стартапы на ранних стадиях — pre-seed и seed – с готовым прототипом.

Бизнес-ангелы с большей вероятностью будут инвестировать, структурируя сделки по белорусскому законодательству, если стартап сможет войти в ПВТ. Правовой режим, в котором действуют инструменты английского права, пока распространяется только на резидентов парка.

В мае стартовал второй набор образовательной программы «Академия бизнес-ангелов». Программа состоит из десяти недель обучения в бизнес-клубе Imaguru и онлайн-занятий (информация на imaguru.by). А летом группа компаний Belbiz планирует провести конференцию об ангельском инвестировании.

Текст: Александр Литвин. Фото: Глеб Соколовский

Штрафы за пренебрежение к персональным данным пользователей

Понятие GDPR (EU General Data Protection Regulation, Общий регламент защиты персональных данных Европейского союза) уже знакомо многим белорусским компаниям, особенно в ИТ-сфере. Регламент вводит новые требования к обработке персональных данных потребителей. Компании, которые не будут им соответствовать, не смогут конкурировать на европейском рынке и подвергнутся огромным штрафам до 20 млн евро.

Регламент вступил в силу 25 мая 2018 года. Он затрагивает в том числе белорусские компании.

Это касается всех фирм и организаций, которые обрабатывают данные потребителей из ЕС: продают и запрашивают контактную информацию, анализируют пользовательское поведение пользователей или разрабатывают ПО, которое работает с персональными данными.

В таблице можно посмотреть, к каким компаниям GDPR имеет непосредственное отношение.

Для того чтобы привести в соответствие с GDPR все внутренние процессы, потребуются существенные трудозатраты. Поэтому важно следовать нижеприведенным рекомендациям.

Собирайте только те персональные данные, которые вам действительно необходимы

Это один из принципов GDPR – количество собираемых персональных данных должно быть минимально необходимым. Причем человек должен понимать, с какой целью они будут использоваться, а компания должна быть готова подтвердить, что такая цель обоснована и необходима.

Убедитесь, что у вас есть согласие на обработку данных

Есть два основных сценария.

- Согласие не нужно, если компания запрашивает данные, которые объективно нужны для исполнения договора (интернет-магазин).
- Согласие нужно, если вы хотите использовать данные клиентов в дополнительных целях — анализ поведения и т.д. Тогда вы должны запросить согласие у человека на обработку его персональных данных в соответствующих целях.

Текст согласия должен быть составлен в предельно ясной форме. Согласие можно получать и в виде галочки, однако она не должна стоять по умолчанию: нужно явное волеизъявление человека.

Проследите, чтобы GDPR соответствовала вся цепочка компаний-подрядчиков

Допустим, есть (1) фитнес-центр, который использует персональные данные своих клиентов. Работу компьютерной системы, в которой хранятся данные, и их обработку обеспечивает (2) компания-подрядчик X. Помимо этого, компьютерную систему когда-то создала (3) компания-разработчик Y, которая сейчас уже не имеет доступа к информации.

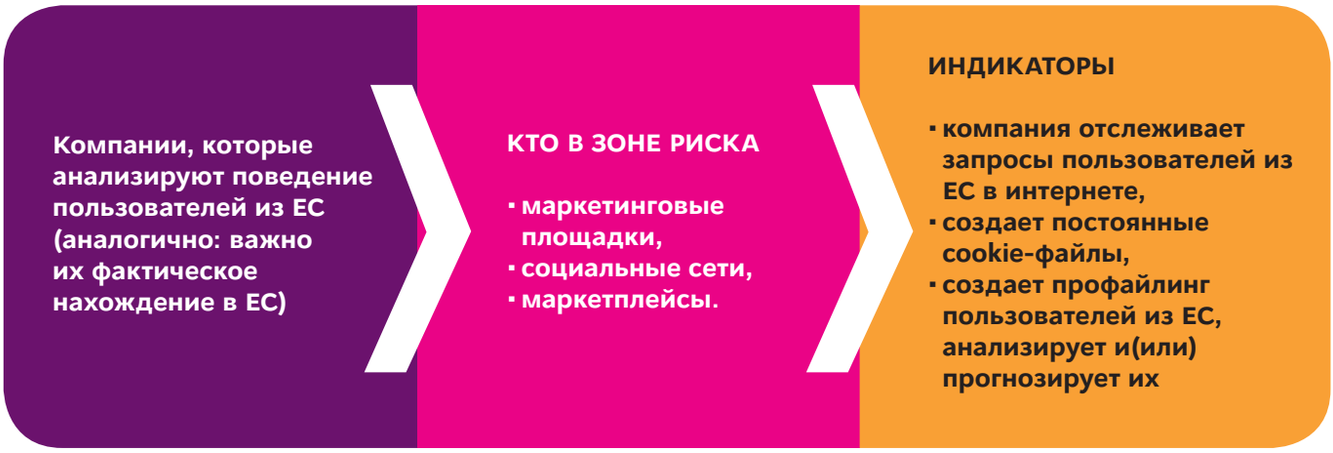
Из всех троих фитнес-центр несет наибольшую ответственность и контролирует, чтобы его деятельность соответствовала GDPR. Подрядчик X также должен им соответствовать, так как напрямую связан с обработкой. Соответствие ПО разработчика Y — формально не обязательно, но в интересах фитнес-центра, чтобы соответствовало и оно, так как это все равно снижает риски.

Документируйте весь процесс обработки персональных данных в компании

Вы должны быть готовы доказать и документально подтвердить, что соответствуете всем требованиям GDPR. Важно иметь именно документы, так как регламент напрямую указывает, что только лишь фактического соблюдения всех требований недостаточно. Прежде всего, обратите внимание, чтобы в вашей компании были следующие документы:

- политика обработки персональных данных,
- внутренние правила и процедуры работы с персональными данными,
- реестры персональных данных,
- учетные записи обработки персональных данных.

Если необходимо, назначьте представителя компании в ЕС.



По общему правилу, если иностранная компания (не резидент ЕС) обрабатывает персональные данные лиц из ЕС, она должна назначить представителя на территории ЕС. Именно он будет отвечать за соблюдение GDPR.

Исключение делается для компаний, которые:

- обрабатывают персональные данные нерегулярно;
- не имеют дело с чувствительными персональными данными;
- едва ли представляют риск для прав физических лиц в связи с использованием их персональных данных.

Если необходимо, назначьте Data protection officer (DPO, инспектор по защите персональных данных)

DPO может быть как штатным сотрудником компании, так и сторонним подрядчиком. Инспектор обязателен для компаний, ключевая деятельность которых связана:

- с обработкой персональных данных, которая требует регулярного и систематического мониторинга физических лиц в больших масштабах. Это касается крупных соцсетей, компаний, работающих с Big Data, и крупных маркетплейсов;
- масштабной обработкой чувствительных персональных данных (sensitive personal data).

Проверьте, соответствует ли ПО, которое непосредственно обрабатывает персональные данные ваших клиентов, требованиям GDPR

Прежде всего, речь идет о принципах Privacy by Design и Privacy by Default.

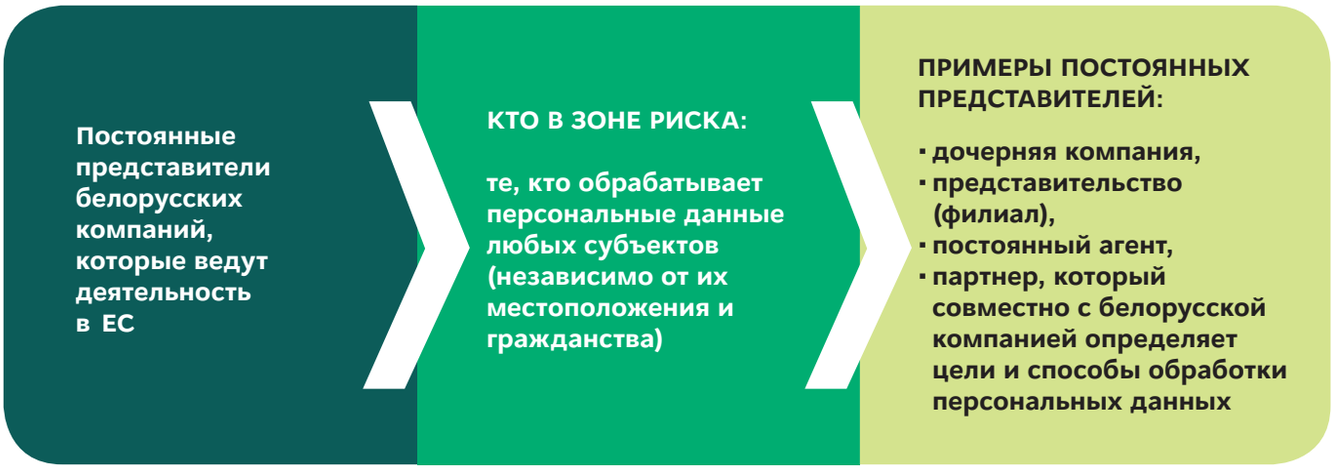
Privacy by Design означает, что приватность должна быть «встроена» в ПО еще на этапе разработки. В целом, ПО должно обеспечивать следующие меры для защиты приватности:

- псевдоминизацию или обезличивание (отдельное хранение информации, позволяющей установить личность человека, и дополнительных сведений, которые к нему относятся);
- криптографическую защиту персональных данных и другие меры защиты, которые необходимо принять с учетом рисков реальности несанкционированного доступа к персональным данным.

Privacy by Default означает, что пользователю изначально должны предлагаться максимальные настройки приватности, и это должно быть всегда по умолчанию.

Для того чтобы подтвердить соблюдение Privacy by Design и Privacy by Default, а также удостовериться в этом самим, рекомендуется проводить специальную оценку — Data Protection Impact Assessments, DPIA.

Источник: tut.by



Улучшайте сервис и оптимизируйте затраты, анализируя звонки

Для компаний, которые заботятся о своих клиентах, анализ звонков и телефонных разговоров является неотъемлемой частью улучшения качества обслуживания.

Любая компания стремится повысить эффективность работы отделов предприятия, учитывать загруженность линий, анализировать качество обслуживания клиентов и контролировать использование телефонных переговоров для личных целей сотрудников.
Выполнить эти задачи возможно при помощи анализа телефонных переговоров. Внедрение на предприятии системы учета, тарификации, анализа и контроля телефонных звонков позволяет улучшить качество обслуживания клиентов, повысить лояльность к компании и снизить количество злоупотреблений со стороны сотрудников. Эксперты сходятся во мнении, что внедренная система менеджмента звонков позволяет сократить расходы на связь приблизительно на 20%.

WinTariff

WinTariff – биллинговая система учета телефонного трафика для малого и среднего бизнеса. Программа позволяет получать, записывать и обрабатывать информацию о телефонных звонках, сохраняя все данные в собственное хранилище.
WinTariff необходим в том случае, если вы хотите получить следующие возможности:

- выяснить и оптимизировать структуру затрат на телефонную связь;
- контролировать и анализировать активность сотрудников;
- получить базу вызовов с ФИО и контактными данными клиентов для повышения лояльности к компании;
- записывать телефонные разговоры для контроля качества обслуживания;
- разделять счета за переговоры между различными пользователями и организациями, использующими одну офисную станцию, например, выписывать счета за телефонные разговоры клиентам гостиницы, контролировать затраты на звонки, совершаемые персоналом.

«Простые звонки»

«Простые звонки» – программа, которая связывает офисную или облачную АТС (или мобильный телефон) и базу клиентов из CRM-системы. В результате получается call-центр без покупки дорогостоящего ПО и оборудования.

Простые звонки помогут:

- сохранять историю и аудиозаписи разговоров со всеми клиентами в персональных карточках;
- набирать номера прямо из клиентской базы;
- узнавать, какой клиент звонит, до приема вызова;
- автоматически переводить входящие звонки на ответственных менеджеров;
- получать детализированную статистику по всем звонкам и менеджерам.

Кодовое слово: «ОПТИМИЗАЦИЯ–2018»

Вы можете приобрести новые лицензии WinTariff и «Простые звонки» со скидкой 10% по кодовому слову до 1 сентября 2018 года в интернет-магазине Allsoft.by.

Автоматизированный аудит вашей сети

allsoft.by

Точная инвентаризация ПК — это важный элемент для любой компании или организации. В рамках аудита сети вы получаете сведения о состоянии серверов, рабочих станций и оборудования, а также сведения о доступе к локальной сети и интернету.

Инвентаризация аппаратного и программного обеспечения всего компьютерного парка даже с частичной автоматизацией требует существенных затрат труда и времени. Чем больше компьютеров в компании, тем острее стоит вопрос о разумном использовании ресурсов.

С помощью специализированного программного обеспечения можно полностью автоматизировать инвентаризацию компьютерного парка, освободив тем самым время персонала для выполнения других работ и задач.

Total Network Inventory

Total Network Inventory позволяет вести полный учет программного обеспечения, установленного на компьютерах, а также осуществлять контроль аппаратной части в офисах, малых и больших корпоративных локальных сетях. Администратор может просканировать сеть удаленно и получить исчерпывающую информацию о каждом компьютере. Все дополнительные модули устанавливаются автоматически. Программа позволяет сканировать сеть как в реальном времени (онлайн), так и с помощью скрипта в момент подключения клиента к домену.

Total Network Inventory поможет:

- удаленно сканировать компьютеры и серверы на Windows, macOS, Linux, FreeBSD и ESX/ESXi;
- вести централизованный учет ПК, сетевого оборудования и ПО;
- определять структуру локальной сети;
- формировать гибкие отчеты по разным категориям данных;
- оперативно отслеживать изменения в аппаратном и программном обеспечении;
- составлять базу данных пользователей ПК;
- хранить множество паролей для различных устройств и протоколов.

Hardware Inspector

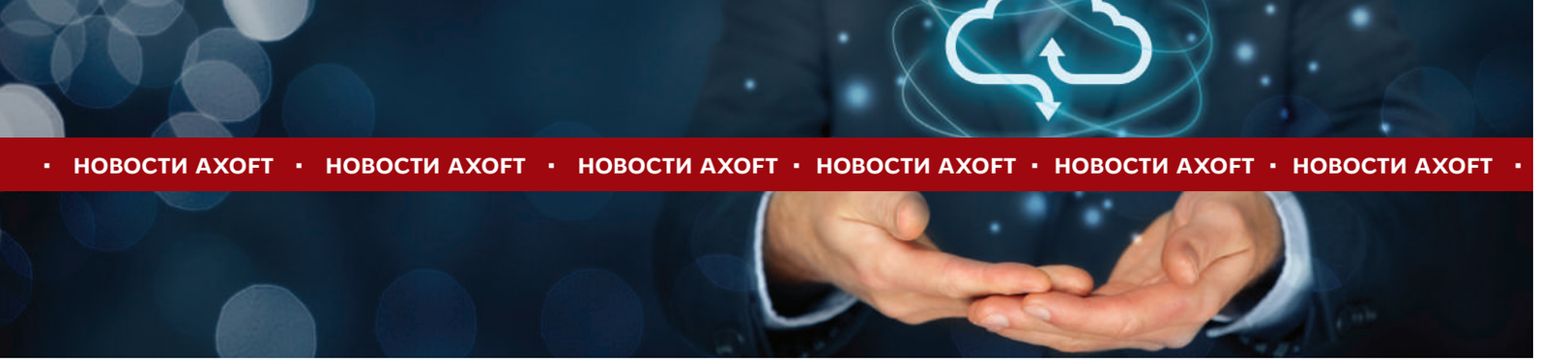
Hardware Inspector – программа, предназначенная для инвентарного учета компьютеров и другой офисной техники. Рекомендована для системных администраторов, ИТ-персонала и руководителей отделов компьютеризации. Уникальность программы Hardware Inspector заключается в возможности ведения учета как текущего состояния параметров компьютера, так и всей истории жизни каждого устройства.

Ключевые возможности Hardware Inspector:

- учет отдельных комплектующих;
- аудит лицензий программного обеспечения;
- отслеживание истории перемещения устройств, их ремонта, профилактики и инвентаризации;
- мониторинг инсталляции пользователями запрещенного ПО;
- учет заявок от пользователей;
- инвентаризация устройств с использованием штрих-кодов;
- многопользовательский режим работы.

Кодовое слово: «ОПТИМИЗАЦИЯ–2018»

Вы можете приобрести новые лицензии Total Network Inventory и Hardware Inspector со скидкой 10% по кодовому слову до 1 сентября 2018 года в интернет-магазине Allsoft.by



Axoft получил статус дистрибутора Palo Alto Networks в странах Восточной Европы и Центральной Азии

Компания Axoft получила статус дистрибутора Palo Alto Networks (PAN) в Беларуси, Казахстане, Таджикистане, Узбекистане, Кыргызстане и Армении.

В соответствии с условиями соглашения, заказчикам в Беларуси и странах СНГ доступна Next-Generation Security Platform Palo Alto Networks, которая включает межсетевой экран нового поколения NextGeneration Firewall, расширенную защиту конечных точек Traps, виртуальные брандмауэры нового поколения Aperture SaaS, обнаружение и предотвращение угроз Wildfire, а также управление безопасностью сети Panorama.

Axoft, как сервисный ИТ-дистрибутор, в настоящее время оказывает продуктовую и техническую поддержку, в том числе пресейл, располагает необходимым демооборудованием, проводит технические демонстрации и воркшопы и предлагает партнерам маркетинговую поддержку по всей линейке продуктов Palo Alto Networks на территории России. В ближайшее время данные услуги будут доступны заказчикам из Республики Беларусь.

Axoft получил декларацию соответствия ОАЦ на решение Trend Micro Deep Discovery

Компания Axoft спешит сообщить вам, что решение компании Trend Micro — платформа Deep Discovery прошла испытания в ОАЦ на соответствие требованиям технического регламента ТР 2013/027/BY.

Платформа Trend Micro Deep Discovery предназначена для защиты от угроз. Она позволяет обнаруживать, анализировать и нейтрализовать современные скрытые направленные атаки в режиме реального времени.

Модули, входящие в состав платформы Deep Discovery: Trend Micro Deep Discovery Analyzer 6.0, Trend Micro Deep Discovery Email Inspector 3.0, Trend Micro Deep Discovery Inspector 5.0. Все они успешно декларированы компанией Axoft на территории РБ и доступны к заказу.

Технический консалтинг Axoft

Придерживаясь концепции сервисного ИТ-дистрибутора, компания Axoft уже не первый год предоставляет услуги технического консалтинга партнерам на территории России и Беларуси.

Услуга позиционируется как сервис, который помогает решить сложные ИТ-задачи силами квалифицированных сотрудников Axoft, освобождая таким образом партнеров от необходимости обучать специалистов для выполнения единичного проекта, так как это дорого и отнимает большое количество времени.

Компания Axoft готова предложить полный спектр услуг по интеграции и внедрению за относительно небольшие деньги и в разумные сроки. Также существует возможность подключения специалистов Axoft к реализации тех проектов, где у партнера возникают проблемы с экспертизой, доступностью ресурсов и т.д.

Весь комплекс услуг предоставляется как на удаленной основе, из Москвы, так и локально, силами инженера по информационной безопасности в Минске. Выезд специалистов головного офиса непосредственно на объект возможен в исключительных случаях и связан с дополнительными затратами.

На текущий момент существует возможность привлечения специалистов Axoft для выполнения следующих работ и внедрения решений:

- Выполнение работ по комплексному внедрению системы контроля защищенности и соответствия стандартам (MaxPatrol 8).
- Выполнение работ по комплексному внедрению системы предотвращения атак нулевого дня и целевых атак: Kaspersky Lab (KATA), Trend Micro (Deep Discovery), Check Point (SandBlast).
- Выполнение работ по комплексному внедрению технологического мониторинга ИТ-инфраструктуры (Solarwinds).
- Выполнение работ по комплексному внедрению системы обнаружения и предотвращения атак на веб-приложения (PT WAF).
- Выполнение работ по комплексному внедрению системы сбора и управление событиями информационной безопасности (SIEM).
- Выполнение работ по комплексному внедрению решений для защиты сетей с помощью интегрированной платформы фаервола нового поколения (Check Point NGTP).
- Выполнение работ по внедрению решений Solidworks. Разработка системы под задачи предприятия.

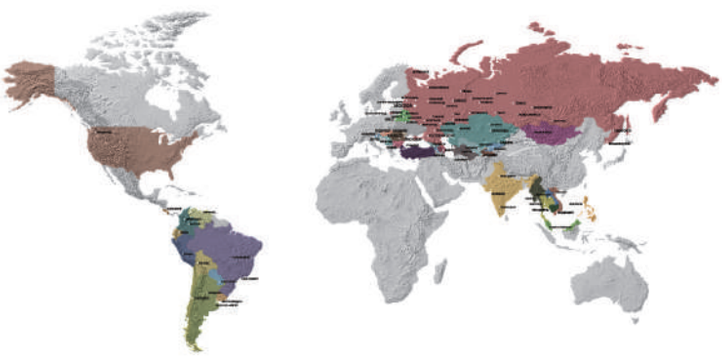
Список компетенций инженеров компании Axoft постоянно расширяется, и мы готовы оперативно подключаться к вашим новым запросам и предложениям.

Если у вас возникли вопросы или есть интересные проекты, которые требует нашей технической поддержки, то сообщите вашему курирующему менеджеру по тел. +375(17)388-95-80 или отправьте запрос на info@axoft.by.

Компания Axoft

Компания Axoft — №1 в рейтинге CRN/RE «Лучшие ИТ-дистрибуторы ПО».

Axoft — сервисный ИТ-дистрибутор, работающий в регионе CEE. С 2004 года компания помогает ИТ-производителям, системным интеграторам, реселлерам и сервис-провайдерам обеспечивать корпоративных пользователей ИТ-решениями и сервисами, которые наилучшим образом решают их бизнес-задачи.



Компания представлена в 28 городах 9 стран мира: России, Беларуси, Грузии, Армении, Азербайджане, Казахстане, Узбекистане, Таджикистане, Кыргызстане, Монголии. Преимущества работы с Axoft уже оценили около 6 тыс. компаний-участников ИТ-рынка: реселлеры программного обеспечения и системные интеграторы, разработчики программных решений, интернет-магазины и консалтинговые компании.

KERIO Acronis solarwinds INFOWATCH
paloalto SOLIDWORKS 1С·БИТРИКС POSITIVE TECHNOLOGIES
KASPERSKY TREND MICRO Check Point ABBYY
Windows Embedded EDB POSTGRES

Мы являемся официальным дистрибутором более чем 1 тыс. мировых производителей программного и программно-аппаратного обеспечения: «Лаборатории Касперского», Positive Technologies, Micro Focus (ранее Hewlett Packard Enterprise), Palo Alto Networks, Kerio и многих других. Представленные в портфеле IT-решения и сервисы разнообразны с точки зрения стоимости и функционала, отвечают потребностям крупного, среднего и малого бизнеса и государственных структур.

AXOFT

В портфеле Axoft представлены SaaS- и IaaS-решения, системы для обеспечения информационной безопасности, инфраструктурное, офисное и научное ПО, а также сопутствующие партнерские сервисы: обучение, консалтинг, маркетинговая, финансовая и техническая поддержки.

С 2009 года Axoft входит в ТОП-5 лучших ИТ-дистрибуторов программного обеспечения по версии CRN/RE и Astera. В 2017 году компания заняла первую строчку рейтинга CRN/RE.

Более подробную информацию о компании можно получить на корпоративном сайте www.axoft.by.

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Datacenter
Silver Cloud Productivity
Silver Collaboration and Content
Silver Messaging

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).

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

Безопасное хранение данных в облаке

Максим Павловский,
руководитель департамента Microsoft
в Softline

За последние 3 года я посетил десяток мероприятий, посвященных хранению данных в облаке. Если они организовывались облачными провайдерами, то выступающие объясняли, почему размещение данных в облаке безопасно как с технической, так и с юридической точки зрения. Если их организовывали различные некоммерческие ассоциации, то можно было услышать истории в стиле Сноудена: вся информация в опасности, а в облаке — вдвойне, а уж размещение там персональных данных—это просто безумие.

Что волнует ИТ-директора

В каких случаях компании поднимают вопрос безопасности персональных данных в облачных проектах?

1. Компания беспокоится, что данные в облаке будут более уязвимы, чем на собственных серверах.

2. Организация волнуется насчет проверок регулятора.

За годы продаж облаков, я слышал множество возражений против них. Одно из наиболее популярных — неочевидная безопасность.
Забавная вещь, что безопасность является одновременно и барьером для одних, и причиной для миграции в облако для других...
Во время мероприятий для потенциальных клиентов у меня было много дискуссий с ИТ-директорами средних и даже небольших организаций. Люди выражали свою озабоченность по поводу того, что облачный провайдер не сможет обеспечить им нужный уровень безопасности данных. Какие угрозы они упоминали?

- Конкуренты могут получить доступ к данным в облаке и причинить ущерб организации;
- технический персонал провайдера может оказаться коррумпированным;
- власти (например, налоговая служба) могут найти что-либо нежелательное об организации, анализируя данные в облаке;
- и отдельно от госорганизаций: ЦРУ, ФСБ, МОССАД (в зависимости от страны) могут «взломать» данные в облаке.

А что на деле?

Безопасность является одновременно и барьером для одних, и причиной для миграции в облако для других

Если речь идет о локальном сервис-провайдере облачных решений в конкретной стране, то действительно – все, что перечислено выше, может случиться. Глобальные облачные платформы, такие как Microsoft Azure, Amazon Web Services, Google Cloud Platform, смогут обеспечить необходимый уровень безопасности данных. При их использовании такие угрозы минимальны.

Мне часто задают вопрос, как это связано непосредственно с облаком? Не является ли это всеобщей угрозой для любых ИТ-систем вне зависимости от того, в облаке ли они или нет? В таких дискуссиях я обычно прошу рассказать мне, как все эти угрозы контролирует компания сейчас, в собственной инфраструктуре. Часть клиентов говорит о DLP, DMZ, SSL, CASB и других средствах безопасности, о команде профессионалов, которая следит 24 часа в сутки за всеми подозрительными активностями и т.п. Но таких организаций немного. Вторая группа признается, что они в начале пути. Ни физической защиты оборудования, ни специализированных средств безопасности (не говоря уж о сотрудниках), все конкуренты знают их ключевых специалистов, с которыми теоретически можно «договориться». И при этом ИТ-директор обеспокоен, что DLP-система у облачного провайдера недостаточно совершенна, чтобы отразить все утечки!

Выбирайте грамотно

Конечно, облачные провайдеры — это не Форт Нокс. Они должны находить баланс между безопасностью, производительностью и ценой. Это профессиональные игроки, и безопасность — составная часть их бизнеса. Команда поддержки не знает, с какой стороны и какой тип атаки им ждать. Они должны защищать свою крепость от осаждающих со всех сторон врагов. В результате, ИТ-инфраструктура облачного провайдера в среднем более безопасна, чем инфраструктура компании-клиента.

Законный вопрос

Использование облачных технологий в контексте законодательства, как правило, вызывает у клиентов два вопроса:

1) Соблюдение требований по работе с персональными данными.

Многие слышали о том, что в некоторых странах установлены особые требования к организациям, деятельность которых в той или иной степени связана с хранением и обработкой персональных данных физических лиц. Так, в Российской Федерации (РФ) действует норма, согласно которой персональные данные граждан страны должны физически храниться на ее территории. Трансграничная передача персональных данных при этом, хоть и не запрещена, но существенно ограничена. Таким образом, облачные сервисы, у которых нет серверов в РФ, фактически объявлены вне закона. Нарушение этого требования, в частности, повлекло блокировку популярной социальной сети LinkedIn на территории РФ. Здесь следует отметить, что в Беларуси, несмотря на общую схожесть законодательства двух стран, такой нормы на данный момент нет.

С другой стороны, для белорусских компаний, работающих на рынке Европейского союза, принципиальным является соответствие требованиям Общего регламента по защите данных (General Data Protection Regulation, GDPR), который устанавливает довольно строгие требования, в том числе технические, к защите персональных данных и серьезные санкции за их неисполнение (до

Облачные провайдеры — это не Форт Нокс. Они должны находить баланс между безопасностью, производительностью и ценой

€20 млн или 4% от общего глобального оборота компании). Для таких организаций перенос персональных данных в облака представляется интересным решением, поскольку крупные облачные провайдеры уже внедрили у себя необходимые технические средства защиты в соответствии со стандартами GDPR и, что не менее важно, гарантируют в этой части со своей стороны полную ответственность в случае наложения уполномоченными органами каких-либо взысканий на их клиентов.

2) Соответствие Указу Президента Республики Беларусь от 01.02.2010 N 60 (ред. от 23.01.2014) «О мерах по совершенствованию использования национального сегмента сети Интернет»:

согласно п.2 Указа № 60, деятельность по реализации товаров, выполнению работ, оказанию услуг на территории Республики Беларусь с использованием информационных сетей, систем и ресурсов, имеющих подключение к интернету, осуществляется юридическими лицами, их филиалами и представительствами, созданными в соответствии с законодательством Республики Беларусь, с местонахождением в Республике Беларусь, а также индивидуальными предпринимателями, зарегистрированными в Республике Беларусь, с использованием информационных сетей, систем и ресурсов национального сегмента сети интернет, размещенных на территории Республики Беларусь и зарегистрированных в установленном порядке. Зачастую клиентов так пугает окончание этого предложения, что они совершенно забывают о его начале, в котором установлена сфера применения данной нормы - деятельность по реализации товаров, выполнению работ, оказанию услуг с использованием информационных сетей, систем и ресурсов, имеющих подключение к интернету. Таким образом, если в облаке, серверы которого находятся за рубежом, размещен хостинг интернет-магазина, то это будет нарушением законодательства. Если же такие облачные сервисы используются для условного резервного копирования или какой-то внутренней аналитики, поводов для беспокойства быть не должно.

В облака и обратно

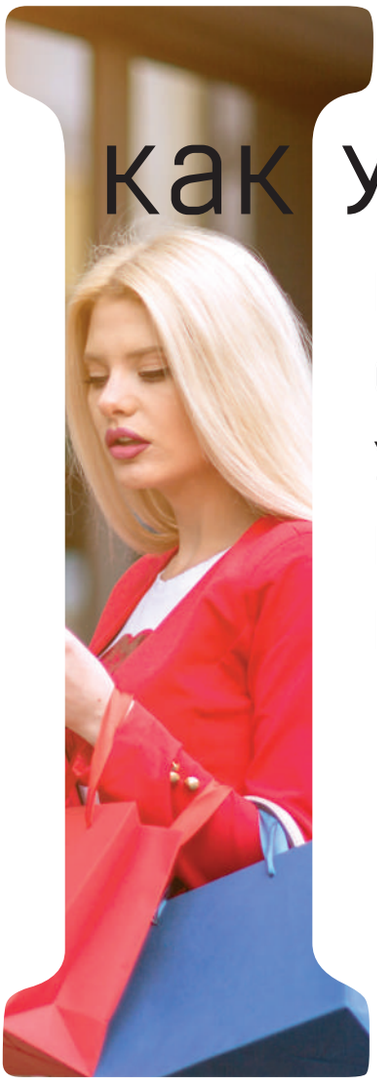
Миграции из облака и в облако технически очень похожие проекты, но с финансовой точки зрения они отличаются крайне сильно. При перемещении в облако вы оплачиваете только реально используемые ресурсы, что сокращает расходы на инфраструктуру, электроэнергию и обслуживание.

Какие преимущества дают облачные технологии?

– Безопасная, высокопроизводительная и постоянно совершенствующаяся инфраструктура.
– Надежное и отказоустойчивое хранилище.
– Рациональность использования ресурсов.
– Экономия на ресурсах ЦОД.
– Сокращение затрат на резервирование оборудования на 50-70%.

Если вы планируете запустить новый проект, для которого необходимы дополнительные ресурсы, переходите в облако! Вы сможете быстро и легко переместить рабочую нагрузку из вашего центра обработки данных, а оплату производить только за реально потребляемые вычислительные мощности.

BI как услуга: поддержим оптимальный уровень наличных в банкомате



Банковские организации были одними из первых представителей финансового сектора, которых заинтересовала бизнес-аналитика как инструмент, применимый в самых разных направлениях деятельности.

Применение BI в банковском секторе

BI в первую очередь используется банками при составлении оперативной отчетности. Руководству банка необходимо на ежедневной основе иметь представление о том, как идет бизнес и достигаются ключевые показатели. Особенно это актуально в сегменте работы с розничными клиентами, где требуется ежедневно отслеживать выполнение планов специалистами по продажам.

Предиктивная аналитика активно используется банками для определения вероятности дефолта индивидуальных и корпоративных заемщиков. Оценку кредитоспособности физических, а в некоторых случаях и юридических лиц в отношении малого и среднего бизнеса банки уже давно доверили скоринговым системам.

Предиктивная аналитика применяется для операций с пластиковыми картами, в части выявления фродовых операций, когда фрод направлен против банка или самого клиента (это могут быть попыт-

ки хищения денежных средств с карты, фиктивные переводы и многое другое). Банковской сфере присущи разного рода риски. BI помогает минимизировать не только внешние, но и внутренние операционные риски, выявляя мошеннические схемы, в которых задействован персонал, тем самым предотвращая достаточно большое количество случаев возникновения потенциальных убытков.

Банкомат как средство дистанционного обслуживания

Конкуренция на рынке банковских услуг растет очень быстро. Банки все активнее борются за каждого клиента, придумывая все новые и новые маркетинговые ходы. Физические лица зачастую являются клиентами двух-трех банков одновременно, поэтому банки стараются сделать свои предложения более персонифицированными – в этом помогает клиентская аналитика, изучение реакции на предложения, эффективности каналов продвижения. Немаловажный фактор с точки зрения конкурентной борьбы – снижение затрат и издержек. Банк, как и любая коммерческая организация, ставит цель максимизировать эффективность средств, на которых он работает. Чем активнее деньги «крутятся», тем более прибыльным становится бизнес.

Прогнозирование и оптимизация денежных средств в банкоматах — крайне актуальная тема, потому что без банкоматов невозможно представить уже ни один банк. Первым шагом к развитию дистанционных каналов обслуживания клиентов является именно банкоматная сеть. Ее требуется поддерживать, обслуживать, расширять и обновлять, а также закупать новые банкоматы.

Суммы в них храняться немаленькие. За день через один банкомат на многолюдной улице может быть совершено от 3-5 до 10 тыс. операций.

Первым шагом к развитию дистанционных каналов обслуживания является именно банкоматная сеть. Ее требуется поддерживать, расширять и обновлять, а также закупать новые банкоматы.

Тренды меняются, банкоматы остаются

Примечательно, что наблюдается тенденция снижения количества операций с наличностью, совершаемых через банкоматы.

Тем не менее нагрузка на банкоматы остается большой, поскольку банки реализуют через них различного рода сервисы, например, разнообразнейшие платежи – самая популярная операция. Люди оплачивают мобильную связь, осуществляют денежные переводы, запрашивают выписки, просматривают остатки денежных средств, пополняют счета наличными. Банки стараются максимально эффективно использовать банкоматы в качестве канала продаж и размещают в них рекламу.

Оптимизация процесса инкассации

Банкомат как точка контакта с клиентом несет в себе определенные расходы, включая стоимость устройства и его обслуживания. Операции по загрузке денежных средств выполняются бригадами инкассаторов.

Банкоматы нужно обслуживать с определенной регулярностью, но выезды важно оптимизировать и минимизировать их количество. И при этом следить, чтобы нигде внезапно не кончились деньги, поскольку длинные очереди к банкомату несут репутационные риски для банка.

Для самого банка деньги, которые лежат в банкомате, – в некоторой степени «замороженные», поскольку они не участвуют в обороте, не размещены в процессах кредитования, не находятся на остатках и никак не влияют на показатели банка в лучшую сторону, иными словами не приносят дохода.

Когда объем остатков в банкоматах минимален, это дает определенный экономический эффект. Банк должен своевременно размещать купюры в

банкомате – и исключительно столько, сколько с него могут снять.

Но есть сложность – спрос на наличные деньги непостоянен. Он зависит от того, какой день: выходной, будний, праздничный (люди снимают деньги на развлечения и покупки) или зарплатный (1, 10, 15, 25 числа). Может серьезно возрастать нагрузка на единичные банкоматы – например, на проходной крупного завода. Пик «занятости» банкомата в таком месте может приходиться лишь на два дня в месяц, а в остальное время – нагрузка минимальная. Нужно учитывать большое количество факторов, которые формируют тенденцию. Когда мы знаем тенденции, мы можем прогнозировать, что будет происходить в тот или иной момент времени.

Понимая прогноз, банк может выстраивать график пополнения банкоматов и точно определять достаточную минимальную сумму.

Личное останется личным

Конечно, банкоматная сеть находится под постоянным мониторингом. С определенной периодичностью банкомат отправляет на единый сервер информацию двух типов: о своем техническом состоянии и о тех операциях, которые были проведены. Это и данные непосредственно о работе инфраструктуры, и кэш-приемника, и наличии ошибок в ОС. Сведения о трансакциях, совершаемых с помощью банковских карт, а также информация о суммах, обслуживающем устройстве, детализация операций отражаются в процессинговых базах.

Но BI-система не работает напрямую с процессингом. Поскольку банки предъявляют очень строгие требования к безопасности информации, провайдеры BI-услуг, например, Softline, могут получать для анализа обезличенную информацию: банкоматам просто присваиваются номера, без указания их адресов. Нет также данных о конкретных клиентах, которые произвели ту или иную операцию. Все реализованные процессы остаются конфиденциальными.

BI-система не работает напрямую с процессингом

Больше эффективности – меньше затрат

Банк может реализовать аналитику самостоятельно – закупить соответствующее программное обеспечение, собственными силами настроить и запустить систему в эксплуатацию, выработать методологические подходы, нарастить компетенции. Но все это длительный и трудозатратный процесс.

В решении Power BI большая часть работы уже сделана интегратором. Система создана и апробирована в деле, методология также готова – остается только уточнить формат получаемых данных конкретного банка и в рамках тестового периода работы конкретизировать специфические моменты.

Всем известно, что важнейшая задача банков и финансовых организаций – управление рисками, которое может потребовать чрезвычайно сложного анализа множества факторов и показателей. С помощью Power BI банки получают удобную, быструю и простую систему отчетности, с помощью которой можно отслеживать и анализировать:

– продажи банковских продуктов в различных разрезах;
– кредитные риски;
– управленческую и финансовую отчетность;
– движение капиталовложений;
– динамику стоимости вложений;
– финансовые показатели по дебиторам и кредиторам;
– оперативные издержки;
– показатели по налогам и персоналу.

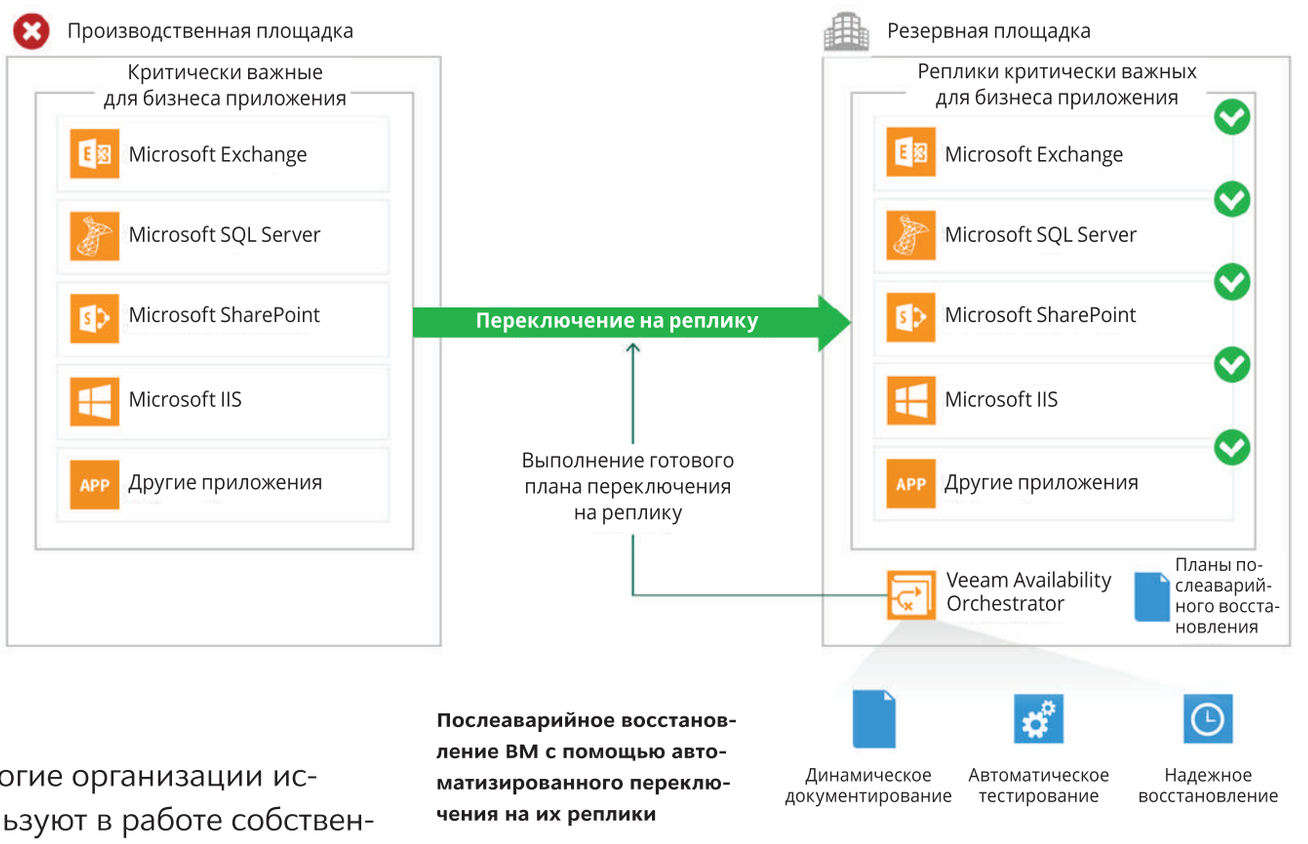
Вместе с тем вам не нужно покупать специализированное программное обеспечение и платить за него единовременно. Вы оплачиваете ежемесячную подписку, что существенно сокращает затраты на ПО и дорогостоящих специалистов. При этом от услуг вы сможете отказаться в любой момент, не потеряв инвестиций.

Воспользовавшись сервисом, банк выигрывает в стоимости и в скорости реализации.

Остались вопросы?

Обращайтесь к Максиму Павловскому, руководителю департамента Microsoft в Softline по тел. **+375(17)388-95-95** (доб. 244) или по e-mail: **Maxim.Pavlovskiy@softline.com**

Новые возможности для бизнеса с Veeam Availability Orchestrator



Послеаварийное восстановление ВМ с помощью автоматизированного переключения на их реплики

Многие организации используют в работе собственную стратегию послеаварийного восстановления данных. Вместе с тем она может подвергать риску как соответствие ИТ-системы требованиям законодательства, так и доступность данных предприятия.

Новое решение Veeam Availability Orchestrator поможет справиться с этой проблемой. Продукт позволяет автоматически создавать, документировать и тестировать планы послеаварийного восстановления, обеспечивая их соответствие требованиям законодательства и аудита.

С помощью Veeam Availability Orchestrator вы сможете:

- воспользоваться протестированной и задокументированной стратегией послеаварийного восстановления данных на предприятии;
- снизить затраты благодаря автоматическому тестированию планов послеаварийного восстановления и проверке их готовности без дорогостоящих ручных процедур;
- непрерывно предоставлять ИТ-сервисы благодаря надежному и автоматическому переключению между производственными ВМ и их репликами.

Veeam Availability Orchestrator поможет сэкономить время на осуществление послеаварийного восстановления и обеспечить непрерывность работы вашего бизнеса.

О компании

Veeam является одним из лидеров в сфере обеспечения доступности данных. В 2018 году решения компании получили высокую оценку пользователей в рейтинге Gartner «Выбор заказчиков 2018 года по отзывам коллег» в категории «ПО для резервного копирования и восстановления данных в дата-центрах».

Более подробную информацию об установке бесплатной пробной версии Veeam Availability Orchestrator и регистрации продукта вы сможете узнать у специалиста Softline **Евгения Лисовского**: **Evgeniy.Lisovskiy@softline.com** или тел. **+375(17)388-95-95, доб. 4537.**

Резервное копирование данных и их восстановление в Microsoft Azure

Veeam Recovery в Microsoft Azure поможет обеспечить непрерывность бизнес-процессов, доступность приложений и данных благодаря новому поколению послеаварийного восстановления в облако — независимо от вашего опыта работы с Azure.

Функционал Veeam Restore в Microsoft Azure встроен в Veeam Backup & Replication, а также доступен в виде отдельного продукта в Microsoft Azure Marketplace.

Veeam Recovery в Microsoft Azure позволяет использовать публичное облако в качестве резервной площадки по требованию, обеспечивая расширенные возможности восстановления данных для компаний любого масштаба без затрат на создание и поддержку собственной резервной площадки. Это решение входит в состав Veeam Backup & Replication и обеспечивает восстановление данных из резервных копий Veeam в облако Microsoft Azure. Решение может быть дополнено Veeam PN — удобным и простым продуктом для программно-определяемой настройки сети, благодаря которому не нужна сложная настройка VPN-соединения и конфигурирование сети для создания резервной площадки в облаке.

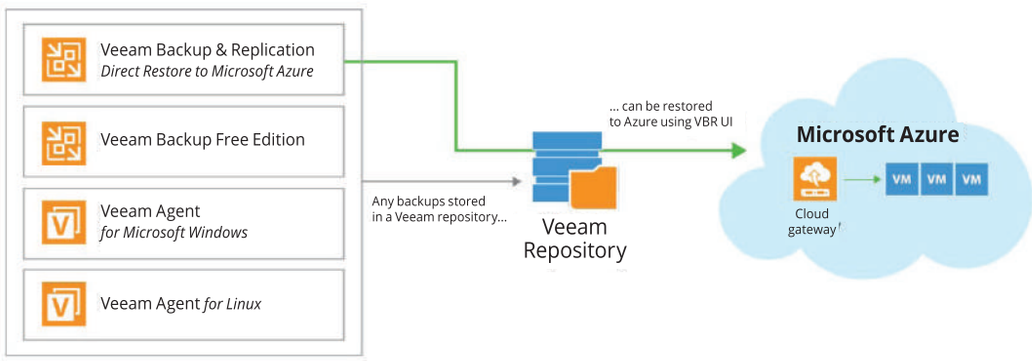
Компоненты комплексного решения

Резервное копирование любых данных на любых площадках и восстановление в Azure Veeam Restore в Microsoft Azure (входит в состав Veeam Backup & Replication) обеспечивает восстановление резервных копий Veeam в облако, оптимизируя использование ресурсов и предоставляя новые сценарии восстановления данных.

Этот компонент позволяет восстанавливать или переносить в облако данные локальных ВМ VMware и Hyper-V, физических серверов и компьютеров. Второй компонент — Veeam PN — позволяет установить соединение между локальной сетью и облаком Azure, чтобы восстановить данные и дать сотрудникам, работающим удаленно, доступ к восстановленной системе.

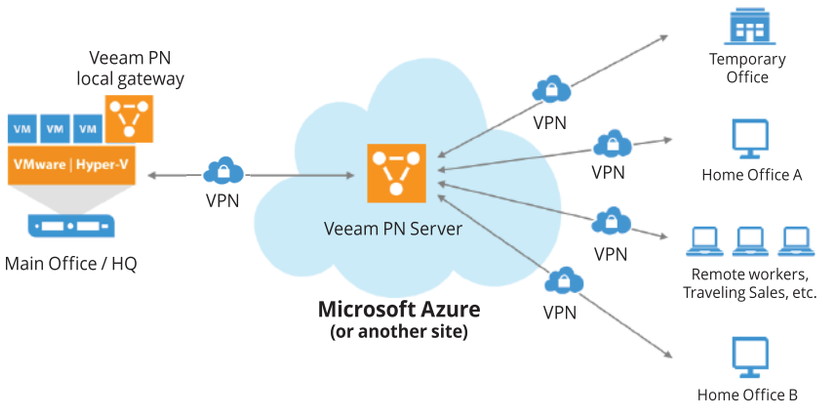
Функционал Veeam Restore в Microsoft Azure встроен в Veeam Backup & Replication, а также доступен в виде отдельного продукта в Microsoft Azure Marketplace.

Современный дата-центр больше не ограничен площадкой, где находятся физические серверы. ИТ-организации могут оптимизировать использование ресурсов, улучшить операционную масштабируемость и повысить эффективность работы, используя облако Microsoft Azure. Veeam Restore в Microsoft Azure позволяет адми-



нистраторам восстанавливать и переносить в Azure данные из физической (P2V) и виртуальной инфраструктуры (V2V). Технология не требует сложной настройки или дополнительных вложений в оборудование, благодаря чему снижаются эксплуатационные расходы.

Azure можно использовать в качестве дополнительного варианта восстановления данных для масштабирования инфраструктуры в случае необходимости.



Послеаварийное восстановление в облако по запросу Veeam PN для Microsoft Azure

Veeam PN для Microsoft Azure — это БЕСПЛАТНОЕ решение, которое упрощает и автоматизирует настройку резервной площадки в Microsoft Azure благодаря легкой программно-конфигурируемой сети (SDN). Оно помогает обеспечить непрерывную работу бизнеса и доступность данных благодаря более простому развертыванию VPN. Решение предназначено для компаний любого масштаба, включая поставщиков услуг.

- Решение нового поколения, которое совместно с Veeam Restore в Microsoft Azure предлагает восстановление данных в облако по запросу, не требуя сложного развертывания VPN. Обеспечивает непрерывную работу бизнеса и доступность данных.
- Способ создать простое и надежное сетевое соединение между ИТ-ресурсами на локальной площадке и в облаке Azure.
- Инструмент для обеспечения простого и полностью автоматизированного соединения между любыми площадками.

Veeam PN для Microsoft Azure упрощает создание соединений между удаленными пользователями и главным офисом.

Veeam PN для Microsoft Azure легко развернуть, даже не имея в штате системного администратора. Решение не требует подключения к сети вручную и сложной настройки VPN. Оно позволяет выполнить восстановление данных в облако по запросу и обеспечивает непрерывную работу бизнеса именно тогда, когда это необходимо. Решение также полезно, если нужно быстро восстановить сервер, ВМ или несколько физических серверов и портативных компьютеров. Для этого не требуется даже учетная запись Azure. Оплачивать использование Azure также не нужно до тех пор, пока не потребуется восстановление данных.

Пользователи могут не волноваться о соединении между площадками. Veeam PN для Microsoft Azure решает критически важные задачи, а его настройка обычно занимает менее пяти минут. Работая в распределенной архитектуре, находящиеся вне локальной сети устройства могут быстро установить соединение. Для этого требуется один раз описать конфигурацию в файлах.

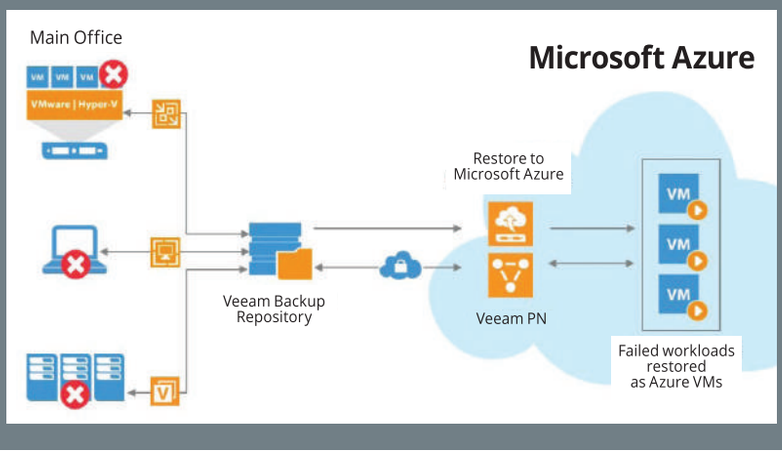
Veeam PN для Microsoft Azure можно использовать для создания гибридного сетевого соединения между любыми площадками: локальной сетью, удаленными офисами или филиалами (ROBO), домашними офисами, мобильными устройствами сотрудников, с помощью поставщиков услуг и публичного облака. Поставщики услуг могут использовать это решение для создания надежного соединения между собственным дата-центром и площадкой заказчика.

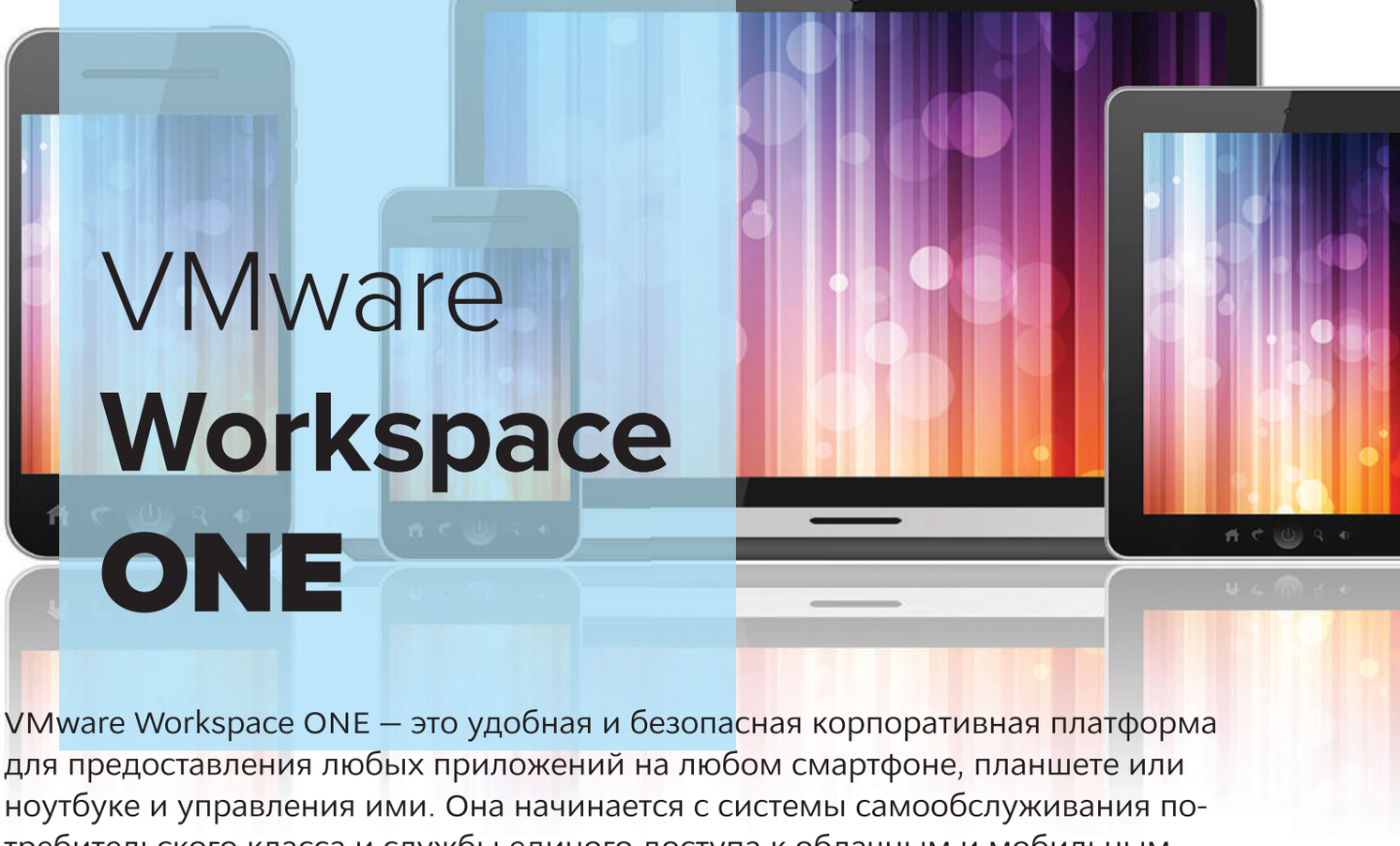
> Veeam PN для Microsoft Azure упрощает создание соединений между удаленными пользователями и главным офисом.

Три простых шага для восстановления данных в Azure

1. Зарегистрируйте учетную запись Azure и выполните предварительную настройку Veeam Backup & Replication.
2. Установите соединение с помощью Veeam PN.
3. Восстанавливайте данные прямо в Azure.

Используйте Microsoft Azure в качестве резервной площадки по требованию:





VMware Workspace ONE

VMware Workspace ONE — это удобная и безопасная корпоративная платформа для предоставления любых приложений на любом смартфоне, планшете или ноутбуке и управления ими. Она начинается с системы самообслуживания потребительского класса и службы единого доступа к облачным и мобильным приложениям, а также приложениям Windows. Платформа включает эффективно интегрированные, привлекательные для пользователей средства для совместной работы или работы с электронной почтой, календарем и файлами.

За счет интеграции VMware Identity Manager со службами Active Directory сотрудники организации могут выполнять безопасный вход в единый каталог приложений без необходимости ввода пароля.
Наконец, Workspace ONE кардинально меняет управление полным жизненным циклом устройств и приложений с помощью удобных возможностей регистрации и настройки, защиты устройств и данных, иерархии активов, удаленной поддержки и устранения неполадок.

Что представляет собой Workspace ONE?
Workspace ONE — это решение VMware, созданное для упрощения внедрения модели ориентации ИТ-услуг на потребителя. VMware Workspace ONE — удобная и безопасная корпоративная платформа для предоставления любых приложений и управления ими на любом устройстве за счет интеграции управления учетными данными, приложениями и корпоративной мобильной средой.

Для каких ключевых сценариев использования предназначен пакет Workspace ONE?
Несколько ключевых сценариев использования, для которых предназначен пакет Workspace ONE:

- Использование сотрудниками любых собственных устройств (модель BYOD) с сохранением надлежащего уровня защиты корпоративных данных.
- Унифицированный каталог корпоративных приложений с упрощенным единым входом для всех: приложений Windows, ПО как услуги, веб-приложений, а также исходных мобильных приложений.
- Комплексное управление Windows 10 и развертывание на предприятии, в том числе в режиме реального времени для предоставления приложений Windows.
- Ускоренное развертывание Office 365 благодаря объединению имеющихся локальных развертываний Active Directory и Microsoft Azure Active Directory.

Как вы обеспечиваете поддержку мобильных приложений на личных смартфонах, планшетах и ноутбуках? Должны ли сотрудники регистрировать свои личные устройства в системе управления корпоративной мобильной средой на базе Workspace ONE?
При использовании Workspace ONE сотрудникам не нужно регистрировать свои личные устройства, чтобы получить доступ к услугам. Само приложение Workspace ONE можно загрузить из Apple App Store, Google Play или Магазина Microsoft. Затем сотрудник может войти в систему и получить доступ к приложениям в соответствии с заданными для них требованиями политик.

Если у заказчика уже есть решение по управлению учетными данными, сможет ли он использовать Workspace ONE?
Да. Для некоторых приложений Workspace ONE может взаимодействовать с существующими поставщиками удостоверений, например, Ping, Okta или CA, представляя при этом общий каталог приложений для пользователей посредством Workspace ONE.

Нужно ли устанавливать какие-либо локальные компоненты в случае приобретения подписки на размещенное в облаке решение Workspace ONE?
Да. Workspace ONE необходимо подключиться к имеющемуся каталогу Active Directory в локальной среде для

подтверждения идентификационных данных пользователя. Для синхронизации VMware Identity Manager и работы консоли управления VMware AirWatch необходим один соединитель.

Что такое доступ на основе условий?
В Workspace ONE есть два типа доступа на основе условий. Первый тип предусматривает доступ на основе политик, установленных поставщиком удостоверений. При этом определенному приложению может потребоваться заданный уровень надежности проверки подлинности или ограничение на основе масштаба сети. Для второго типа используется новый компонент ComplianceCheck Conditional Access, который гарантирует совместимость устройства, передавая определенную политику, заданную в модуле политик VMware AirWatch, перед завершением проверки подлинности.

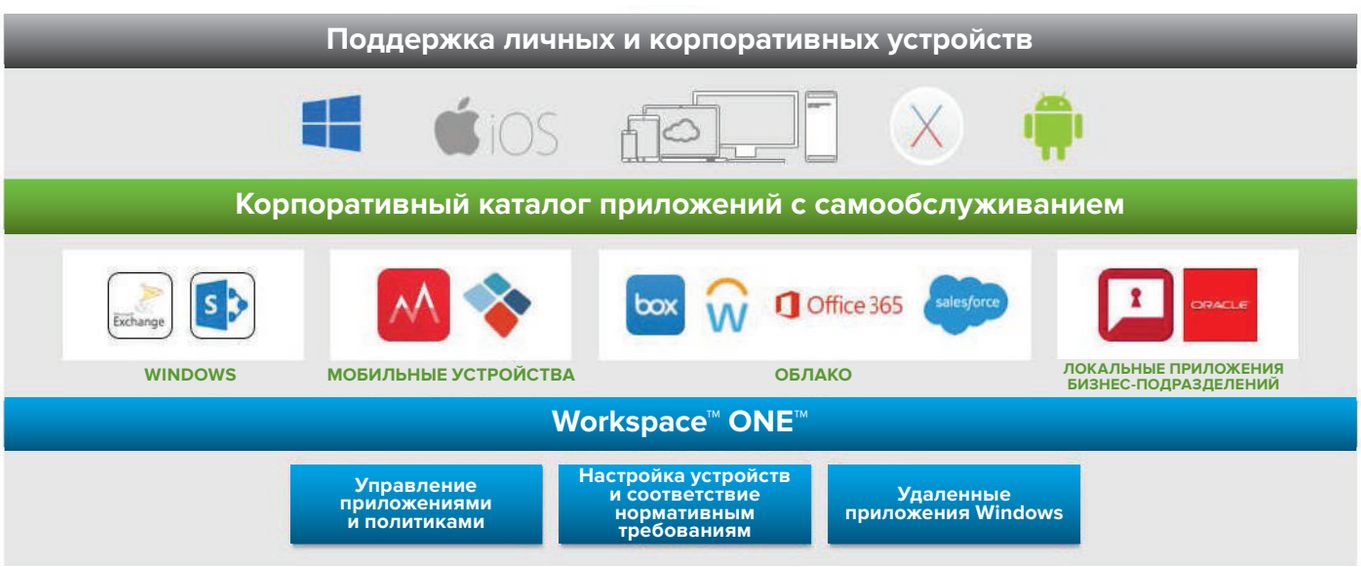
Какие операционные системы устройств поддерживает Workspace ONE?
Workspace ONE поддерживается с момента выпуска в операционных системах мобильных устройств и нескольких ОС для настольных компьютеров, в том числе iOS, Android, Mac OS, Chrome OS, ОС Windows и других.

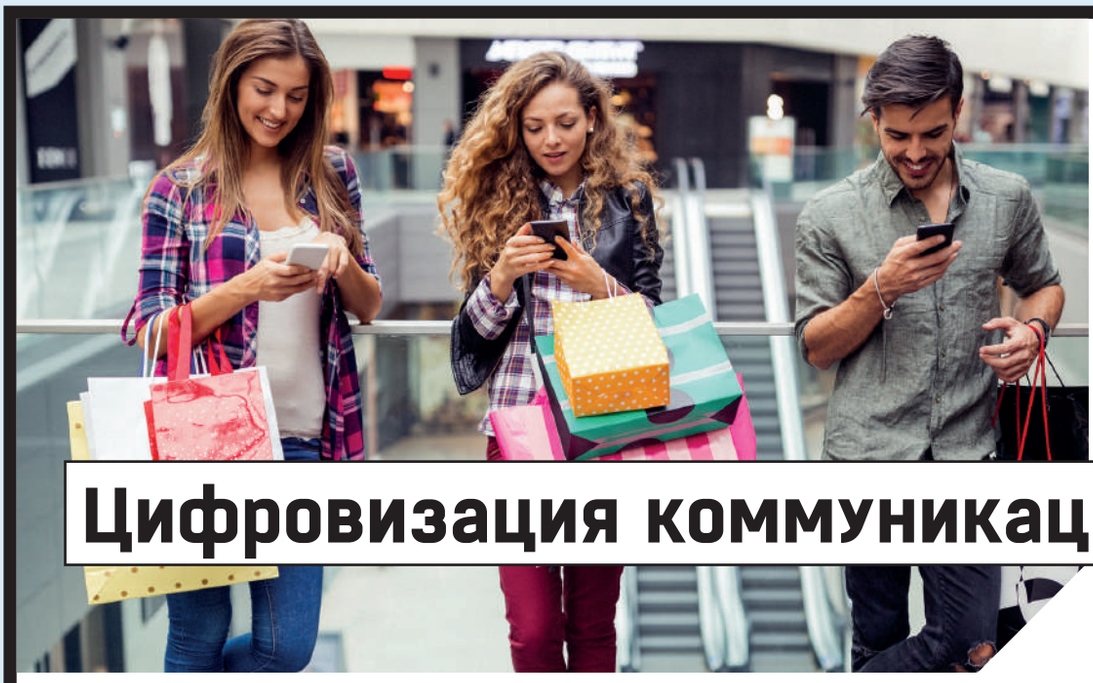
Возможности зависят от платформы. Как минимум, любое устройство с совместимым браузером HTML5 может получить доступ к каталогу приложений и средству запуска Workspace ONE через интернет для доступа к веб-приложениям и размещенным приложениям Windows с помощью Horizon или Citrix. Затем на устройстве могут предоставляться дополнительные исходные приложения Workspace ONE, которые можно установить на устройствах с ОС Windows 10, Apple iOS и Android.

Как лицензируется Workspace ONE?
Все редакции Workspace ONE лицензируются по числу пользователей и устройств и предоставляются по годовой облачной подписке или бессрочной лицензии в локальной среде.

Какую редакцию нужно приобрести, чтобы заменить устаревшие мобильные решения для защиты электронной почты, например Good или Blackberry?
Workspace ONE редакции Advanced предоставляет сотрудникам современный защищенный клиент электронной почты. У современных организаций уже есть отличные защищенные решения для электронной почты, которые поддерживаются на любимых устройствах сотрудников. В сочетании с Secure Email Gateway организации могут ограничить потерю информации из-за незащищенных вложений электронной почты.

Могу ли я приобрести Workspace ONE для большинства своих сотрудников и добавить лицензии для параллельного доступа к Horizon или лицензии на VMware AirWatch, предоставляемые по числу устройств, для остальных?
Да. Мы делаем все возможное, чтобы вы могли использовать соответствующие технологии и лицензирование для различных сценариев использования. Мы поддерживаем такой подход в сценариях, где уместнее добавить к Workspace ONE лицензии для параллельного доступа к Horizon или лицензии на VMware AirWatch, предоставляемые по числу устройств.





Цифровизация коммуникаций

Информационные технологии меняют модели коммуникации между людьми, а также между людьми и организациями (органами власти, малым и крупным бизнесом, розничной торговлей, организациями социального профиля). Устанавливать и поддерживать контакты становится все проще, мгновенно взаимодействовать друг с другом возможно на любом расстоянии. Распространение цифровых технологий происходит стремительно, причем более равномерно, чем распределение доходов.

Индивиды получают инструменты для взаимодействия напрямую, минуя посредников. Миграция в online происходит в сферах, которые раньше были доступны только offline, например, государственные услуги и образование.

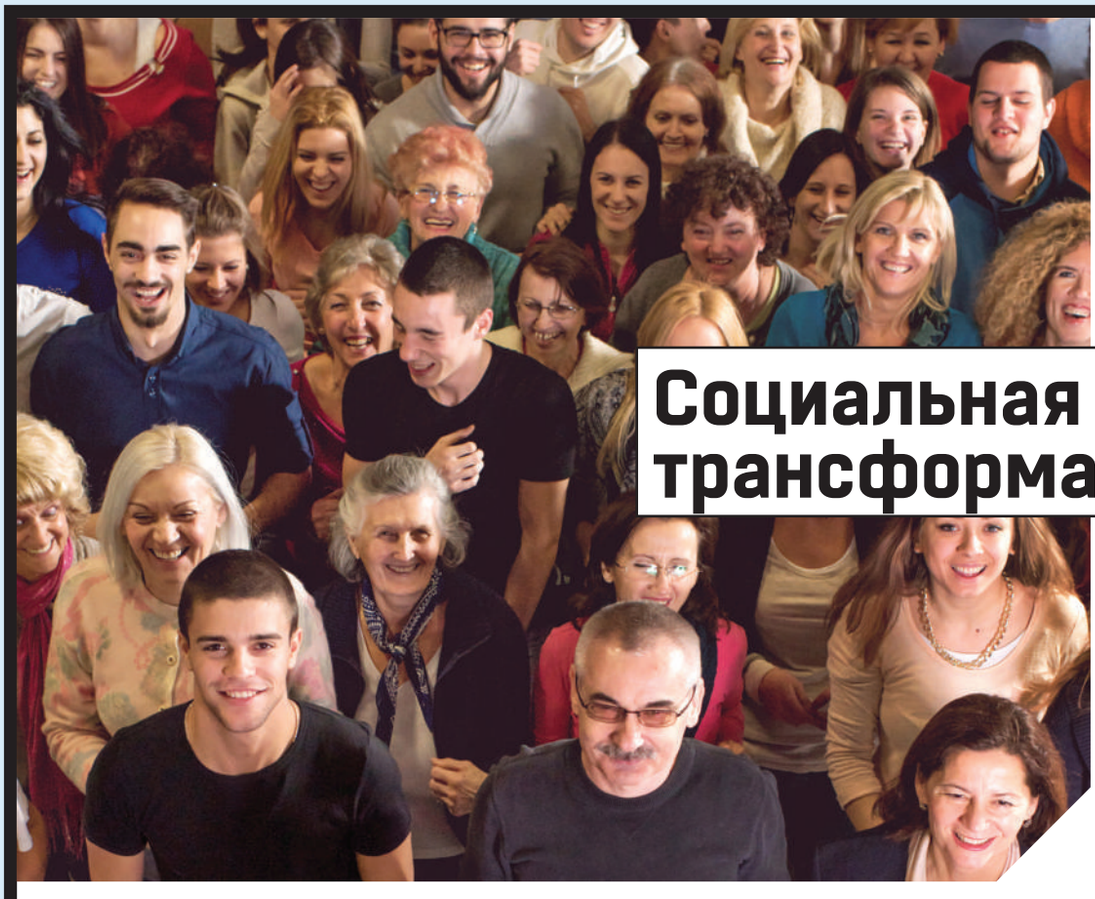
Люди во всем мире становятся зависимыми от смарт-устройств, таких как мобильные телефоны и планшетные компьютеры. С их помощью можно выполнить множество задач в любом месте и в любое время — от общения, покупки в магазине, развлечения и проверки почты до расчетов с банком, образования и GPS-навигации.

Происходит эволюция пользовательского поведения: 10 лет назад Facebook раскрыл профиль людей, изменив их жизнь. Затем Instagram и Twitter призвали делиться информацией о себе ежесекундно. Сегодня наступила эра трекинга: мы оповещаем общество, во сколько проснулись, сколько прошли, как погуляли с собакой и т.п. Практически все свободное время потребители проводят с гаджетами.

Примеры цифровизации коммуникаций:

- в Германии 37% ежедневных коммуникаций происходит через цифровые девайсы;
- почти 80% потребителей по всему миру имеют смартфоны;
- активно развивается омниканальность — возможность делать покупки в разных режимах: в торговой точке, через мобильный телефон, через компьютер с возможностью бесшовного перехода;
- одним из важнейших каналов продвижения становятся лидеры мнений в социальных сетях. 60% потребителей говорят, что прислушиваются к рекомендациям;
- компании, ориентированные на рост, стремятся создать возможности для обучения своего персонала. Объем мирового рынка online-образования в 2016 году превысил $50 млрд и по прогнозам увеличится в 5 раз к 2022 г.

Распространение цифровых технологий происходит стремительно, причем более равномерно, чем распределение доходов.



Социальная трансформация

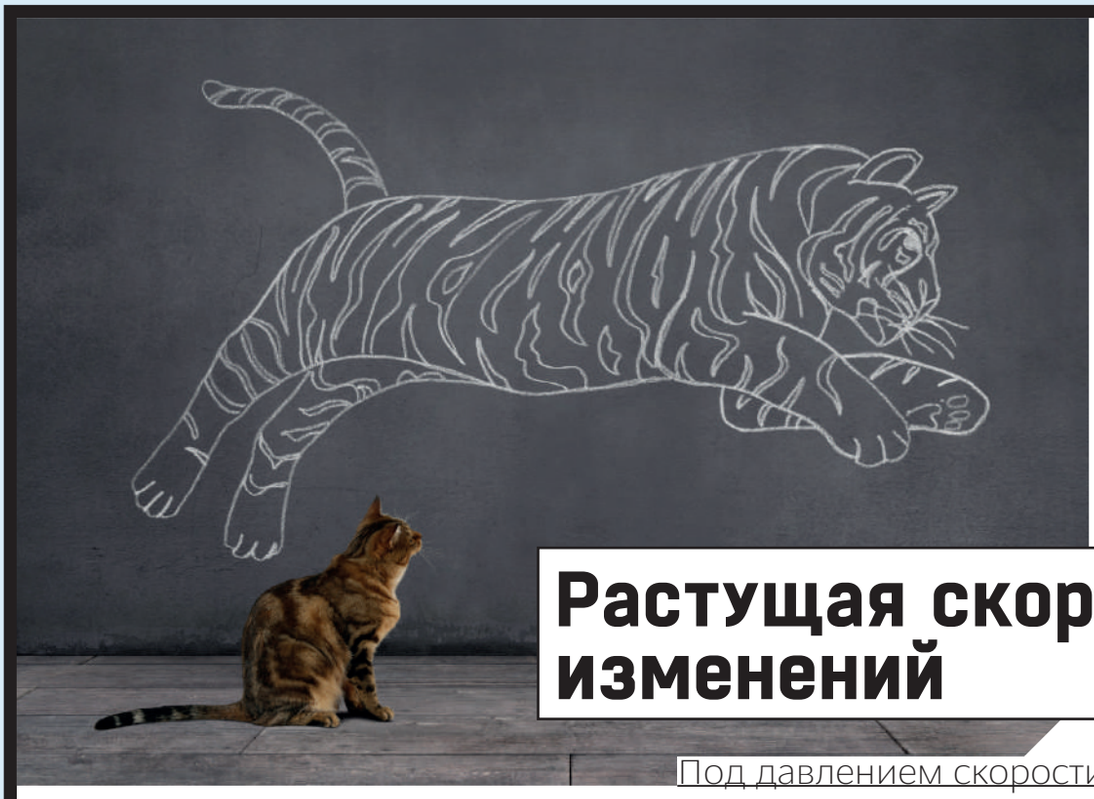
Общество находится в непрерывном движении. Основными векторами глобальных демографических сдвигов являются: устойчивое снижение рождаемости и смертности населения по мере экономического развития и урбанизации; рост населения Земли; повышение средней продолжительности жизни и ускоренная миграция населения из менее развитых в более развитые страны.

Изменяется отношение к старению, происходит сдвиг гендерных ролей и понятия семьи. Доля людей старшего возраста увеличивается. Привычки потребления пожилых людей отличаются от привычек более молодых. Повышение доступности обучения и нарастающее участие женщин в бизнесе глубоко влияют на изменение в социальной инфраструктуре. Изменяется роль женщины в обществе, развивается гендерное равенство, поколебавшее положение мужчины в качестве первого кормильца в семье. Одним из основных фактов, определяющих общество будущего является смена поколений. На смену поколения X придут поколения Y и Z, имеющие другой набор ценностей.

Примеры социальной трансформации:

- население планеты увеличится на 15% к 2030 году;
- средний возраст молодых людей при рождении первого ребенка увеличился с 26 лет в 1995 до 29 лет в 2015 и продолжит увеличиваться;
- на одну женщину к 2020 г. в среднем будет приходиться 2,47 ребенка по сравнению с 3 детьми в 1995 г.;
- в Великобритании число мужчин, уходящих в декрет, увеличилось в 10 раз по сравнению с 10 последними годами;
- две трети людей в возрасте от 14 до 34 лет говорят, что пол больше не определяет стиль жизни или поведение, как это было когда-то.

На смену поколению X придут поколения Y и Z, имеющие другой набор ценностей.



Растущая скорость изменений

Под давлением скорости развития инноваций компании вынуждены менять существующие бизнес-модели, вырабатывать новые подходы к продуктам и услугам.

Инновационные технологии, существенно изменяющие привычные действия в самых разных сферах, от промышленного производства до организации быта, захватывают потребителей нарастающими темпами. Под давлением скорости развития инноваций компании вынуждены менять существующие бизнес-модели, вырабатывать новые подходы к продуктам и услугам, процессам и поддержке бизнес-операций. Скорость вывода новых продуктов на рынок постоянно увеличивается. Бизнесу приходится оперировать в условиях неопределенности и постоянных изменений. Развиваются новые бизнес-модели, основанные на принципах «экономики совместного потребления» и электронных платформах.

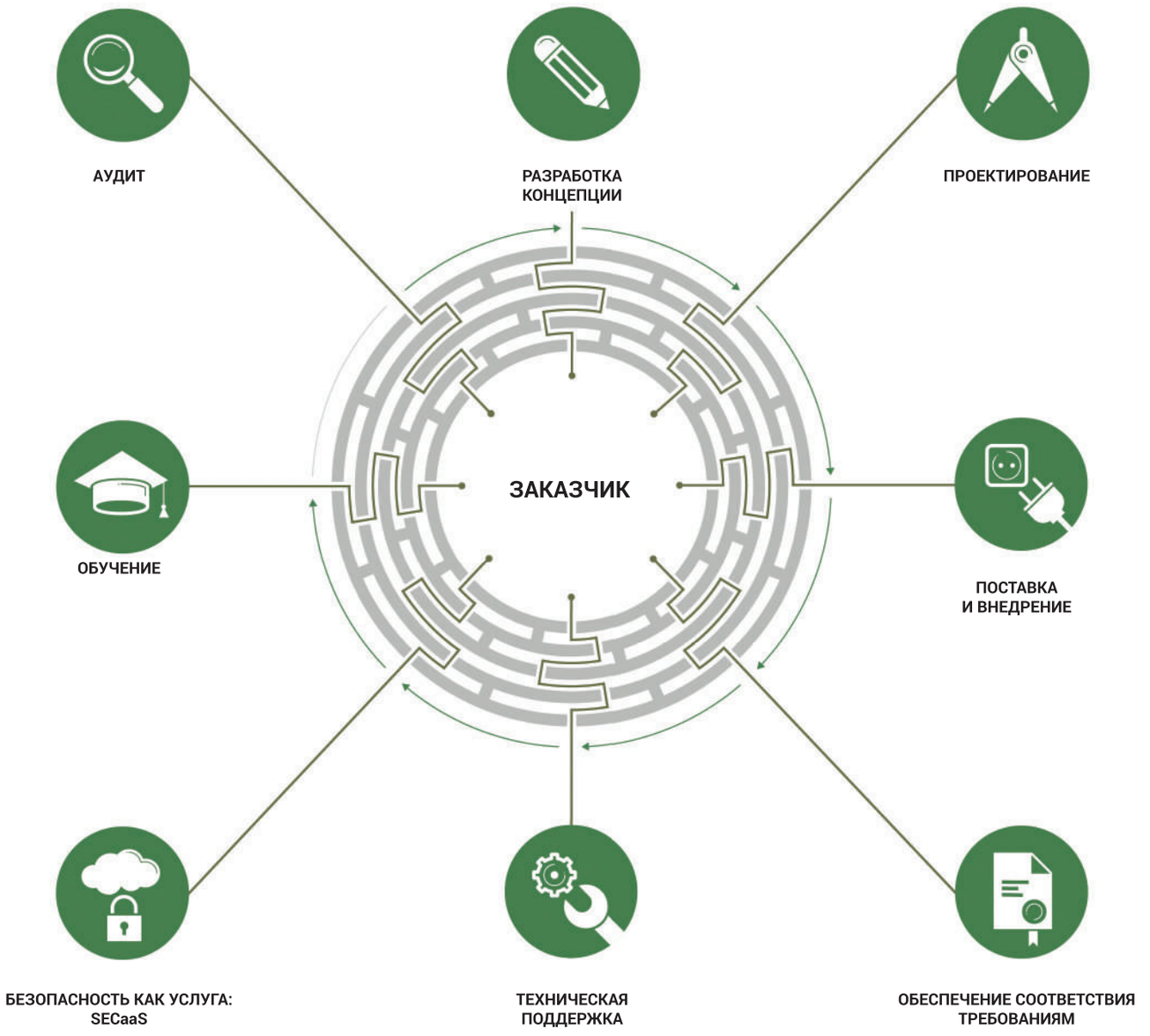
На пути трансформации бизнеса стоит ряд барьеров: недостаток компетенций, негибкие структуры управления, неопределенность и прочее.

Многие компании не успевают адаптироваться к изменениям и уходят с рынка. Давление со стороны потребительского спроса, быстрое развитие и распространение технологий повысили значимость и сложность инновационного процесса в компаниях, сделав его более дорогостоящим и рискованным. Компании развивают новые модели инновационной деятельности.

Примеры роста скорости изменений:

- если на то, чтобы телефон и радио стали привычными для четверти населения США, потребовалось более 30 лет, то интернет достиг массового потребителя всего за 7 лет;
- 52% компаний из Fortune-500 с 2000 г. поглощены или обанкротились;
- знания и умения, которые были важны 10 лет назад, морально устарели по отношению к тенденциям новой модели мира;
- продолжительность жизни крупных компаний уже сократилась в 1,5 раза;
- деятельность 1/3 компаний из TOP-20 будет подорвана новыми технологическими платформами;
- 10 лет назад СМИ для распространения новости требовался день или больше. Сегодня – достаточно одного «клика» мышкой;
- 60% новых вакансий на рынке требуют навыков, которые есть только у 20% населения.

Комплекс услуг по проектам



В Softline сформирована одна из самых мощных команд по информационной безопасности. Выполняя сотни проектов в год и обеспечивая присутствие специалистов в регионах, мы можем гарантировать заказчикам сочетание отличного качества и приемлемой стоимости внедрения систем ИБ. Мы предлагаем широкий спектр решений: от технологий, предотвращающих утечки конфиденциальной информации и защиты персональных данных, до проектов по защите от направленных атак, мошенничества и обеспечения безопасности АСУ ТП.

кибер НЕ безопасность

Каждая 2-Я крупная организация столкнулась с целевыми атаками хакеров в 2017 году.

Каждая 10-Я компания пострадала от вирусов-шифровальщиков типа NotPetya и WannaCry.

От **3** до **5** дней **проходит между появлением нового эксплойта и началом активного его использования хакерами. Особо продвинутые группировки адаптируются** за несколько часов.

По материалам: snob.ru, rusability.ru, samag.ru, ptsecurity.com, habrahabr.ru

На **500%** вырос общий объем «логических атак» на банкоматы в странах Европы за первое полугодие 2017 г.

На **67%** за 2015-2017 годы возросло количество вакансий в сфере информационной безопасности в США.

Более **1** миллиона
IoT-устройств – столько в 2016 г. захватили самые крупные вредоносные ПО Mirai и Bashlight.

$30 млн
потеряли пользователи Parity летом 2017 года из-за уязвимости в коде клиента криптовалютной сети Ethereum

4700 BTC
(около $62 млн) было украдено с кошельков пользователей сайта NiceHash21 (сервиса покупки и продажи вычислительных мощностей для майнинга криптовалюты) в результате хакерской атаки.

$86,4 млрд
было потрачено в мире на ИБ в 2017 г., согласно статистике Gartner.

$7 млн были потеряны в результате подмены злоумышленниками адреса Ethereum-кошелька в атаке на Coindash.io

Конфиденциальные данные и фото **25** тыс. пациентов литовской клиники пластической хирургии Grozio Chirurgija были обнародованы в мае 2017 года преступной группировкой «Царская гвардия» после отказа руководства клиники выплатить злоумышленникам 300 биткоинов (порядка $800 тыс.).

$3,9 млн
из $4 млн удалось восстановить непальскому банку NIC Asia Bank15 после хакерской атаки.

В Новосибирске старшеклассник с помощью вредоносного ПО повысил свои привилегии в сервисе «электронный дневник» до уровня администратора и исправлял оценки на более высокие.

250 тыс.
человек были подписаны на аккаунт New York Times в твиттере в январе 2017 г. в момент взлома и публикации группировкой хакеров OurMine сообщения о ракетном ударе России по США.

Карта решений:

подход Softline к проектированию ИБ-систем

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

Анализ и оценка информационной безопасности компании

Аудит информационной безопасности

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

Разработка концепции информационной безопасности

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

Внедрение и управление политикой безопасности и рисками

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

Защита от мошенничества

Antifraud

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

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

Сервис детектирования взлома хостов (определение зараженности ПК)

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

Системы проверки контрагентов

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

Внедрение системы обеспечения информационной безопасности

Защита онлайн-сервисов

- **Защита веб-приложений (WAF)**

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

- **Защита от DDoS-атак**

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

Нам хорошо знакомы все категории DDoS-атак: объемные атаки, атаки на уровне протоколов, на уровне приложений. Эффективные способы защиты от них различаются в зависимости от типа атаки и расположения защищаемого интернет-ресурса: это фильтрация трафика на площадке заказчика или на уровне дата-центра, либо специализированные внешние сервисы защиты, обладающие достаточными канальными мощностями и вычислительными ресурсами.

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

- **Технический анализ защищенности, тесты на проникновение**

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

- **Анализ кода**

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

Защита веб и почты

- **Защита веб-трафика**

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

- **Защита почтового трафика**

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

Защита серверов, рабочих станций, виртуальной инфраструктуры, мобильных устройств

- **Защита серверов, конечных точек**

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

- **Защита виртуальной инфраструктуры**

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

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

- **Решения класса DBF (DataBaseFirewall) –** комплексный инструмент защиты корпора-

тивных СУБД, предотвращающий основные угрозы для доступности, целостности и конфиденциальности данных.

Управление доступом

- **IDM, SSO, PKI**

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

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

- **PAM**

Процессы предоставления пользователям логинов и паролей, а так же контроля удаленной сессии могут и должны быть автоматизированы, если ваша компания заботится о защите от внутренних угроз.

Мы рекомендуем внедрить современное PAM (Privileged Access Management) решение, особенно тем компаниям, которые прибегают к услугам внештатных специалистов поддержки и администрирования систем и которым необходимо передавать для работы администраторские учетные записи или root пользователей.

- **Аудит доступа к файловым ресурсам**

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

Защита информации

DLP

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

Мы расскажем, как грамотно сочетать оба. При этом вы получите удобную и полноценную систему управления, не требующую специальных технических знаний для управления системой, сбора отчетности и доказательной базы, а также расследования инцидентов безопасности.

IRM

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

Защищенный обмен данными

Для надежного и безопасного обмена данными мы предлагаем следующие решения:

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

Классификация информации

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

Шифрование

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

Защита сети, ATP

Межсетевые экраны нового поколения

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

Защита от целевых атак и атак «нулевого дня»

Современные кибератаки все чаще ориентированы на конкретную отрасль (банки, ретейл, промышленность, гос. сектор, интернет-магазины и т.п.) или конкретную компанию. Уникальный характер таких угроз позволяет с легкостью обходить классические средства защиты – антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы и т.д. Мы предлагаем услуги по внедрению специализированных средств обнаружения современных атак («песочницы», детекторы аномалий, мониторинг процессов на рабочих станциях), а также услуги по выстраиванию необходимых процессов эффективного противодействия целевым атакам (аналитика по инцидентам, локализация заражения в сети, действия по предотвращению атаки и исключению повторных инцидентов).

Firewall management

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

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

Безопасность КИИ и АСУ ТП

Защита АСУ ТП

Одной из самых горячих тем в текущем году стала безопасность критической информационной инфраструктуры (КИИ). Это связано как с повышением уровня понимания компаниями необходимости защищенности своей инфраструктуры и возможных последствий успешно проведенных атак, так и с вступлением с силу новых нормативных документов. Разработанная методология и опыт реализованных проектов по обеспечению безопасности АСУ ТП, приобретенный за последние годы, помогает нам делиться экспертизой с заказчиками и в других отраслях, которые начиная с текущего года попадают под действие законодательства.

Решения по однонаправленной передаче данных

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

Центры реагирования ИБ (SOC)

SIEM

Одной из самых горячих тем в текущем году стала безопасность критической информационной инфраструктуры (КИИ). Это связано как с повышением уровня понимания компаниями необходимости защищенности своей инфраструктуры и возможных последствий успешно проведенных атак, так и с вступлением с силу новых нормативных документов. Разработанная методология и опыт реализованных проектов по обеспечению безопасности АСУ ТП, приобретенный за последние годы, помогает нам делиться экспертизой с заказчиками и в других отраслях, которые начиная с текущего года попадают под действие законодательства. SIEM (Security information and event management) – это специализированная аналитическая система, предназначенная для управления событиями систем безопасности в организации. Решения этого класса просматривают данные от всех систем ИБ и по определенным критериям отслеживают отклонения от нормы. Если по данным анализа происходит отклонение, система создает инцидент, а затем помогает в его расследовании, предоставляя все необходимые данные.

SECaaS

Безопасность как услуга (Security as a Service) – это логичное и выгодное решение для компаний, которые уже вынесли в облако часть своей инфраструктуры и бизнес-систем.
Помимо того, что эти решения адаптированы к угрозам, специфическим для облачных окружений, они обладают такими преимуществами, как моментальные обновления, быстрое внедрение и, конечно, низкая стоимость за счет оплаты по подписке.

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

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

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

Поддержка

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

Система мониторинга и отчетности использования информационных ресурсов

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

Техническая поддержка и сопровождение систем ИБ

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

Обучение специалистов заказчика

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

Киберпреступность **и решения Check Point Software**

Директор по развитию бизнеса компании Check Point Software в Украине, Грузии и странах СНГ Александр Савушкин поделился своим экспертным мнением о ситуации с киберпреступностью сегодня и рассказал об одном из самых опасных вирусов-шифровальщиков в мире — Petya.

— В чем сегодня заключается самая большая опасность использования современных технологий?

— Есть очень хороший видеоролик, где на сцене один из героев рассказывает публике о «новом умном доме», где он управляет всем с помощью телефона и всего лишь одним движением. Это ведь так просто и удобно. При этом в доме как раз находятся грабители, и они в шоке от того, что перед ними все открывается, выезжает, то есть все доступно. О чем этот ролик? — О том, что, с одной стороны, мы упрощаем нашу жизнь с помощью новейших технологий, но с другой — ровно так же становимся простыми мишенями для злоумышленников.

Это относится к компаниям любых размеров, включая крупные корпорации. Никто не знал, что летом прошлого года пройдет одна из наиболее масштабных кибератак на Украину, которая «зацепила» абсолютно все отрасли — от банков, аэропортов до простых частных компаний, чьи данные были просто зашифрованы.

— Почему атаки в СНГ стали происходить чаще?

— С развитием технологий мы наблюдаем рост количества кибератак не только в СНГ. Такие масштабные атаки, как Petya и WannaCry затронули компании по всему миру: 59% организаций называют программы-вымогатели одним из главных рисков. Однако в СНГ существует проблема низкой цифровой гигиены, что приводит к ускоренному распространению любой атаки. Чтобы снизить риски, корпоративным и частным пользователям необходимо регулярно обновлять ПО, на котором они работают, а также соблюдать базовые правила информационной безопасности: не открывать подозрительные письма и, особенно, вложения к ним, не переходить по непроверенным ссылкам, не использовать на своем устройстве неизвестные флешки. Придерживаясь этих простых принципов, а также используя современные средства защиты, пользователи в любых странах мира могут обезопасить себя от вторжения хакеров. Организации должны сосредоточиться на проактивной борьбе с угрозами, использовать защиту «Пятого поколения», которая поможет блокировать любой подозрительный контент и трафик до его попадания в сеть. Компании, использующие продвинутую защиту, на 30% быстрее устраняют угрозы.

— Как происходило проникновение вируса Petya?

— Распространение Petya происходило в рамках фишинговой кампании с вредоносными вложениями. Корпоративные пользователи открывали файлы, прикрепленные к письмам, тем самым «впуская» зловред в сеть компании. После проникновения Petya использовал те же уязвимости, что и WannaCry — эксплойт EnternalBlue и бэкдор DoublePulsar. Через них вредонос получал контроль над данными устройства, зашифровывал их и выставлял пользователю требование отправить 300 долларов в биткоинах на специальный счет, чтобы вернуть доступ к своим файлам. Важно отметить, что на данный момент не было зафиксировано ни одного случая дешифровки файлов.

— Повысился ли после атаки спрос на системы защиты Check Point в СНГ, в частности, в Республике Беларусь? Способствуют ли атаки продажам в компаниях, которые занимаются кибербезпасностью?

— Решения Check Point пользуются стабильным спросом среди представителей коммерческих и государственных организаций из самых разных отраслей. В этом смысле ситуация на рынке СНГ не отличается от общемировой. Вредоносные кампании не способны изменить ситуацию коренным образом.

— На каком месте сейчас Беларусь по частоте кибератак? Последние данные были в октябре прошлого года. Изменилось ли что-нибудь сейчас?

— По данным майского отчета Global Threat Impact Index, подготовленного исследователями компании Check Point, Беларусь занимает 109 место в рейтинге самых атакуемых стран. С декабря прошлого года количество атак на страну немного увеличилось (тогда она занимала 117 место), однако Беларусь по-прежнему остается одной из самых безопасных стран мира с точки зрения киберпреступности.

Кибербезопасность крупного бизнеса

KASPERSKY lab

Kaspersky® Anti Targeted Attack Platform

Комплексное решение для защиты от целевых атак и сложных угроз

- Блокирование сложных угроз и снижение риска целевых атак
- Постоянный мониторинг на уровне сети и рабочих мест
- Выявление аномалий в поведении объектов IT-инфраструктуры
- Экспертное сопровождение и помощь в расследовании компьютерных инцидентов
- Оценка потенциальных рисков IT-безопасности в текущей инфраструктуре

www.kaspersky.ru/enterprise

#ИстиннаяБезопасность

softline®

Ваш надёжный поставщик ИТ-сервисов и решений

info.by@softlinegroup.com
+375 17 388 95 95

Kaspersky®
Anti Targeted
Attack Platform

Передовая защита от целевых атак и комплексных угроз

Преимущества решения

- Сокращение финансовых и операционных убытков, вызванных кибератаками
- Сведение к минимуму возможности прерывания критически важных бизнес-процессов
- Предотвращение дорогостоящих судебных разбирательств, а также случаев несоблюдения требований и нормативов
- Защита инфраструктуры от злоумышленников, действующих незаметно и причиняющих ущерб в течение долгого времени
- Устранение дополнительных расходов на устранение последствий целевых атак (дополнительное обучение, набор сотрудников, усиление защиты системы)

Обеспечивает ли безопасность ваша стратегия?

Успешные целевые атаки обычно эксплуатируют разные уязвимости. С технической и финансовой точек зрения любой организации стоит как можно лучше изучать каждую атаку: понимание того, какими инструментами и методами пользуется противник, необходимо для улучшения корпоративной стратегии безопасности. Само по себе обнаружение — без понимания того, как отвечать на атаку и как изменять стратегию согласно ситуации), — практически не имеет смысла. Какую бы совершенную технологию защиты вы ни использовали, проблемы будут возникать снова и снова, пока организация не выработает адаптивную, направленную в будущее стратегию безопасности.

Стратегический подход к защите от целевых атак

Kaspersky Anti Targeted Attack Platform воплощает современный стратегический подход к обнаружению целенаправленных атак. Благодаря многоуровневым превентивным технологиям защиты и передовым разработкам в области обнаружения угроз, а также обширному набору сервисов для прогнозирования угроз и реагирования на них, платформа «Лаборатории Касперского» успешно борется с целевыми атаками любого масштаба и любой сложности.

Технологии и сервисы способствуют реализации адаптивной стратегии к отражению целевых угроз, основанной на четырех компонентах (прогнозирование, предотвращение, обнаружение и реагирование).

ICSA labs
CERTIFIED ADVANCED THREAT DEFENSE

«Решение «Лаборатории Касперского» показало превосходные результаты во время тестирования. Оно выявило 99,44% неизвестных угроз и продемонстрировало высочайшую эффективность обнаружения на материале почти 550 новых и малоизвестных угроз».

Отчет ICSA по сертификационному тестированию решений для борьбы с комплексными угрозами, IV кв. 2016 г.

Новые возможности Kaspersky Anti Targeted Attack Platform

В 2017 году решение получило ряд новых возможностей, которые позволяют еще надежнее защитить вашу компанию от целевых атак любого масштаба.

- Интеграция с Kaspersky Secure Mail Gateway
- Улучшенный веб-интерфейс
- Уведомления об инцидентах
- Настраиваемые отчеты
- Обозначение наиболее важных систем и сотрудников
- Контроль доступа на основе ролей
- Повышенная производительность и гибкость за счет кластеризации «песочницы» и поддержки виртуальной среды VMware ESXi™
- Усовершенствованное сопоставление событий

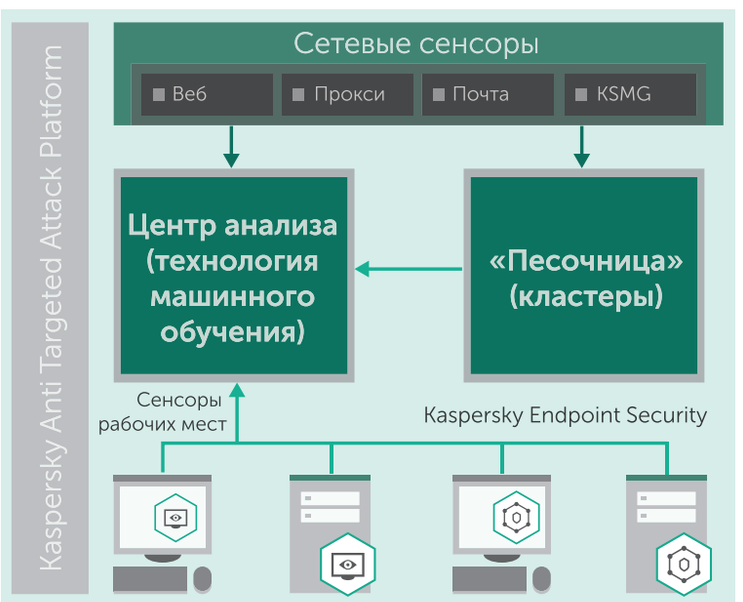
Архитектура решения

В решении Kaspersky Anti Targeted Attack Platform сочетаются динамический анализ на основе «песочницы» и передовые технологии машинного обучения, что обеспечивает защиту от широкого спектра угроз.

Благодаря сочетанию сетевых, веб- и почтовых сенсоров, а также сенсоров рабочих мест решение эффективно обнаруживает угрозы на каждом уровне корпоративной IT-инфраструктуры.

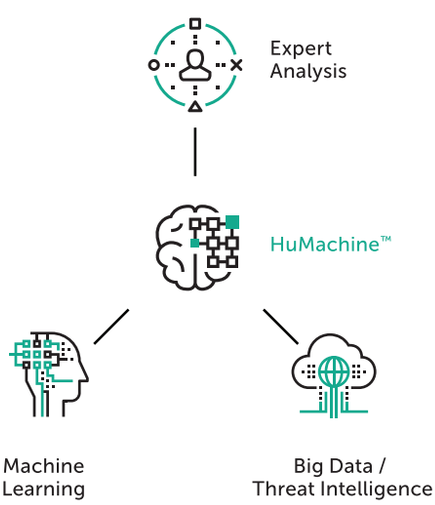
Платформа содержит следующие компоненты:

- **Многоуровневая сенсорная архитектура** — обеспечивает полный контроль
- **Улучшенная «песочница»** — постоянно оценивает возможные угрозы
- **Мощная аналитическая система** — генерирует вердикты с минимальным числом ложных срабатываний



www.kaspersky.ru
#ИстиннаяБезопасность

Решение Kaspersky Anti Targeted Attack Platform внесено в единый реестр российского ПО и соответствует требованиям ФСБ России к антивирусным средствам класса Д.



Инновационные технологии в серверах HPE ProLiant поколения Gen10

Новое поколение серверов ProLiant Gen10 производства компании Hewlett Packard Enterprise обладает целым рядом уникальных технологий для повышения производительности, отказоустойчивости и безопасности ИТ-инфраструктуры.

Повышение производительности вычислительных ресурсов

Jitter Smoothing

Разработана и внедрена технология Jitter Smoothing (сглаживание частоты работы процессора), суть которой состоит в отслеживании сервером «дрожания» частоты CPU в режиме Intel Turbo Boost, доступном в процессорах Xeon, кроме младших моделей. Режим предназначен для кратковременного повышения частоты на пиковых нагрузках. Частые такие переключения вызывают задержки обращения к памяти, в итоге Turbo Boost может даже ухудшить производительность. Технология Jitter Smoothing позволяет использовать предиктивные механизмы, встроенные в сервер. Они обеспечивают работу процессора на большей, чем базовая, частоте, в то же время снижается количество переключений частоты самих ядер. В некоторых задачах, требовательных к частоте (например, Java-приложения), это позволяет получить прирост производительности даже сверх стандартного механизма в режиме Turbo Boost. Ближайшие два года эксклюзивная технология Jitter Smoothing будет доступна исключительно в серверах производства компании HPE.

Core Boosting

Вторая инновационная технология – Core Boosting, ускорение ядер. Она доступна, например, в серверах ProLiant DL380 Gen10 и ProLiant XL230k Gen10 из состава системы Apollo 6000. В дальнейшем список серверов будет расширяться.
Обеспечивает повышение частоты активных ядер процессоров в режиме Turbo Boost сверх обычно доступной в этом режиме. Благодаря технологии можно обеспечить такой же уровень производительности, какой дают процессоры с большим числом ядер, и снизить стои-

мость общего решения (железо + софт), если софт лицензируется поядерно. Следует отметить, что Core Boosting – это не «разгон», а штатная функция процессоров.

Workload Matching

Третье нововведение, доступное в Gen 10 – Workload Matching (профили нагрузки). Существует около 40 параметров работы сервера, каждый из которых имеет несколько возможных значений. С новой технологией в несколько кликов можно выбрать одновременно на многих серверах оптимальные профили настройки для различных классов задач. Это позволяет обеспечить повышение производительности до 9%.

Инновации в работе с оперативной памятью

Fast Fault Tolerance

Память HP Smart Memory обладает уникальным механизмом Fast Fault Tolerance (карантин областей памяти). При обнаружении сбойного участка в одном из чипов памяти FFT назначает проблемной области памяти «запасные» области нужного объема на том же канале памяти. Пропускная способность снижается только для этой маленькой области, а вся остальная память на чипе работает с прежней скоростью.

Эта технология лицензирована Intel, создана эксклюзивно для HPE и не появится в серверах других производителей еще два года.

Persistent Memory

Активно продолжает развиваться направление энергонезависимой памяти – Persistent Memory. Удалось добиться двукратного увеличения емкости (до 192 ГБ) и производительности работы с логами баз данных и задачами с интенсивными операциями записи. Фактически использование такой памяти позволяет вести обработку данных в режиме in-memory в любой СУБД.

Scalable Persistent Memory

Нововведение Gen 10 – Scalable Persistent Memory – способно обеспечить переход на новый уровень емкости, который измеряется терабайтами; автоматическую запись состояния памяти на NVMe-накопитель в случае потери питания; поддержку на уровне BIOS.

Обновления дисковой подсистемы

Увеличение емкости

По сравнению с поколением Gen 9, в каждой модели произошло увеличение внутренней емкости. Вышел новый формат накопителей uFF (micro-Form Factor) – это два флеш-накопителя, которые помещаются на место одного SFF-накопителя (объемы 120 и 340 ГБ, SATA). Такие uFF-SSD могут использоваться как загрузочные или кэширующие диски.

Новые Smart Array-контроллеры

Выросла производительность контроллеров до 1,5 млн IOPS (на 65% выше предыдущего поколения), а энергопотребление снизилось на 45%. Теперь они могут работать одновременно в HBA и RAID-режиме.

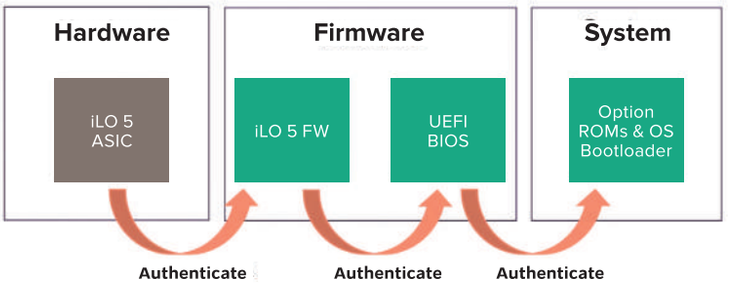
Среди новых возможностей конфигурирования – универсальная корзина SAS/SATA и премиальная корзина 6SFF SAS/SATA + 2NVMe. Кроме того, существенно увеличено количество NVMe-дисков.

Совершенствование системы управления

Поменялось поколение чипа удаленного управления iLO. Ускорены операции с удаленной консолью и виртуальными накопителями, а часть функций управления доступна, даже если система находится в выключенном состоянии.

Серверы стали грузиться в два раза быстрее при использовании UEFI-режима BIOS, по сравнению с поколением Gen 9. На уровне BIOS обеспечивается полная поддержка новых технологий энергонезависимой памяти, реализована комплексная защита RAM от

Silicon Root of Trust



Hewlett Packard Enterprise

потери питания с помощью NVMe-накопителей для реализации HPE Scalable Persistent Memory.

Существенно переработан весь механизм предварительной настройки сервера, включая настройки RAID – его можно запускать прямо из консоли iLO, а не только при загрузке сервера по нажатию F10 (Intelligent Provisioning).

Еще одна новость касается пользователей различных средств автоматизации управления. В iLO расширена поддержка инструкций Open IPMI, а стандарт управления через интерфейс REST API от HPE теперь полностью соответствует стандарту DMTF Redfish, кроме части управления RAID-контроллерами.

Усовершенствована диагностика неисправностей: теперь лог Active Health System Log (бортовой самописец сервера) можно скопировать на флешку через разъем USB на передней панели и изучить самостоятельно в бесплатном сервисе Active Health System Viewer. Раньше iLO мог только отправить лог в Центр поддержки HPE для анализа.

Самые безопасные серверы

Попытки атак и нанесение вреда инфраструктуре заказчиков происходят достаточно часто. Поэтому требования к безопасности возрастают, например, в прошлом году крупная американская компания отказалась от использования серверов одного из крупных производителей, потому что они обнаружили потенциальную уязвимость в прошивке одного из компонентов сервера.

Цель разработки семейства Gen 10 – обеспечение максимальной защищенности решений и абсолютной безопасности инфраструктур заказчиков. Благодаря чипам собственного производства компании HPE iLO удалось обеспечить безопасность на всех этапах жизненного цикла сервера.

Silicon Root of Trust

Полная защита прошивок компонентов реализуется технологией HPE Silicon Root of Trust – это проверка прошивки iLO на наличие в ней вредоносного кода путем сверки контрольной суммы с аппаратным чипом внутри iLO. Затем идет проверка прошивки остальных компонентов сервера, включая BIOS, на предмет нарушения целостности. Уведомления о скомпрометированных прошивках позволяют быстро обнаружить атаку и вернуться к безопасному состоянию.

Защита сети управления имеет четыре уровня, различающихся используемыми алгоритмами, стандартами шифрования, контролируемыми компонентами сети управления.

На уровне сервера реализована фиксация попыток вскрытия корпуса даже при отсутствии питания. А на уровне стойки обеспечить физическую безопасность поможет блокировка/разблокировка двери на основе комбинации электронного ключа и биометрических данных сотрудников.

Уверенность в том, что данные нельзя будет извлечь с устройств и носителей, реализуется услугами безопасной утилизации HPE Point-Next.

На данный момент серверы HPE – это единственные разработки, одобренные американским институтом NLST (National Institute of Standards and Technology, U. S. Department of Commerce). Это служит гарантией соответствия используемых методов контроля, ограничений и требований к firmware высоким отраслевым стандартам и рекомендациям.

Доступные модели

Первыми в новом поколении были выпущены стоечные серверы 300 серии (DL360 и DL380), 500 серии (DL560, DL580), классический блейд BL480c, блейды Synergy SY480 и SY660 и микросервер. Младшие линейки будут доступны немного позже.

Технологические преимущества нового поколения серверов HP становятся доступны эксплантатам всех категорий серверов.

СХД Huawei Enterprise. Продуктовая линейка OceanStor v5

Huawei OceanStor 18500F/18800F V5

Корпоративные решения Huawei в области систем хранения позволяют удовлетворить практически любые требования по части масштабируемости, емкости и отказоустойчивости массивов хранения данных.

Основные характеристики	OceanStor 18500F	OceanStor 18800F V5*
Количество поддерживаемых дисков	2400	3200
Максимальное количество контроллеров	16	16
Объем кэша	512 GB to 16 TB	1 TB to 16 TB
Максимальное количество портов ввода-вывода	384	384

*В OceanStor 18800F V5 применяется специализированный сверхскоростной алгоритм кэширования, предназначенный для повышения скорости чтения и записи данных SSD-дисков. Модификация поддерживает работу с 2,5" SSD-дисками.

Технологические особенности и преимущества OceanStor V5

Превосходная производительность
All-flash система обеспечивает быструю реакцию на основные сервисы. Обладая превосходной масштабируемостью OceanStor 18500F / 18800F V5 может быть оснащена 16 контроллерами, 16 ТБ кэш-памяти и 3200 SSD-накопителей корпоративного класса с рекордной производительностью в 6 миллионов IOPS при задержке 1 мс.

Надежность

Современная интеллектуальная архитектура SmartMatrix 2.0 в сочетании с бесшлюзным конвергентным решением, поддерживающим работу в режиме Active-Active, позволяет сохранить задержку 1 мс и обеспечить готовность данных на уровне шести девяток (99,9999%), гарантируя непрерывность бизнеса для клиентов.

Интеллектуальное управление

В СХД OceanStor 18500F / 18800F V5 используется технология eService для поддержки интеллектуального управления устройствами на протяжении всего жизненного цикла (план, дизайн и O& M).

При исчезновении напряжения в сети модули BBU, встроенные в блоки питания, продолжают поставлять питание контроллеру и первым четырем дискам, позволяя им записать данные из кэша контроллера. Это позволяет сохранить все данные и штатно завершить работу системы.

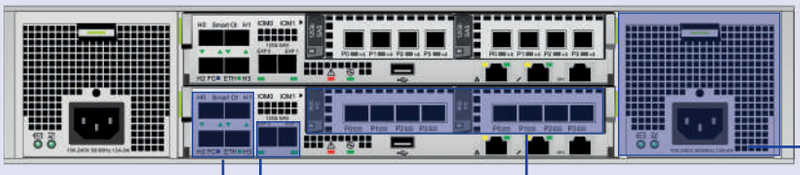
Huawei установила Мировой рекорд! Согласно исследованию некоммерческой организации «Совет по производительности СХД» (Storage Performance Council (SPC) система хранения данных OceanStor 18800F V5 от Huawei признана **самой высокопроизводительной**. Отрыв от ближайшего конкурента – в 4 раза. В целом, среди 10 лучших СХД – 6 производит Huawei.

СХД начального уровня OceanStor 5300/5500 V5

Выполнены в форм-факторе, в котором контроллер и полка с жесткими дисками совмещены в одном корпусе. Контроллер располагается на задней части, жесткие диски – спереди.

Основные характеристики

	5300 V5	5500F V5 (только отличия)
Контроллерная платформа (SAN+NAS)	2U + контроллер	
Количество поддерживаемых дисков	500	750
Максимальное количество контроллеров	8	88
Объем кэша	**64 GB to 512 GB**	**128 GB to 1,024 GB**
Максимальное количество портов ввода-вывода (на контроллер)	**20**	



Блоки питания

(1+1), модули BBU и система охлаждения

Порты Ethernet

- 5300 V5: четыре порта Gigabit Ethernet в каждом котроллере
- 5500 V5: четыре порта 8 Gigabit Ethernet в каждом контроллере

Порты расширения SAS

Два порта расширения SAS в каждом контроллере

Интерфейсные модули

- Два слота для интерфейсных модулей с возможностью «горячей» замены
- Типы портов: 8 или 16 Гбит/с Fibre Channel, GE, 10GE TOE, 10GE FCoE и 12 Гбит/с SAS, 56 Гбит/с InfiniBand, SmartIO

Полки расширения и полки высокой плотности

Для увеличения дисковой емкости СХД Huawei предусмотрены двух- и четырехъюнитовые полки расширения, а также полки высокой плотности.

Двухъюнитовые полки предназначены для размещения 25 дисков размером 2,5". Четырехъюнитовые полки вмещают 24 диска размером 3,5". Допустимо совмещение в одной системе полок разного вида, так как блоки питания и интерфейсные модули, через которые производится подключение, унифицированы. Дисковые полки высокой плотности вмещают 75 дисков размером 3,5". Диски загружаются вертикально. В полке размещены четыре блока питания, вентиляторный модуль и интерфейс SAS. Полки высокой плотности несовместимы с другими видами полок.

СХД среднего уровня OceanStor 5600/5800 V5

Контроллерная полка обособлена. Жесткие диски находятся на полках расширения. СХД 5600/5800 поддерживают до 1250 дисков.

Основные характеристики

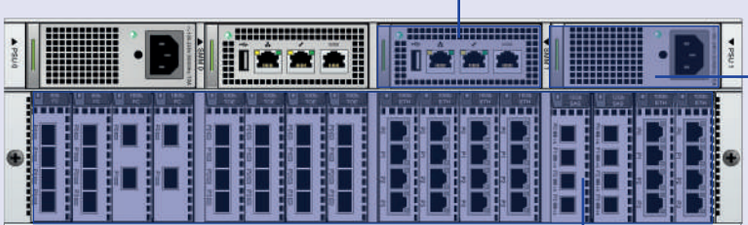
	5600 V5	5800 V5 (только отличия)
Контроллерная платформа (SAN+NAS)	3U	
Количество поддерживаемых дисков	1000	1200
Максимальное количество контроллеров	8	
Объем кэша	256 GB to 2,048 GB	512 GB to 4,096 GB
Максимальное количество портов ввода-вывода (на контроллер)	28	

BBU-модули

- 5600 V5: 1+1. 5800 V5: 2+1
- Защита данных при перебоях питания

Контроллеры

- Двухконтроллерная система



Модули управления

- 1+1
- Управление контроллерами и их настройка
- Поддержка веб-интерфейса и командной строки

Интерфейсные модули

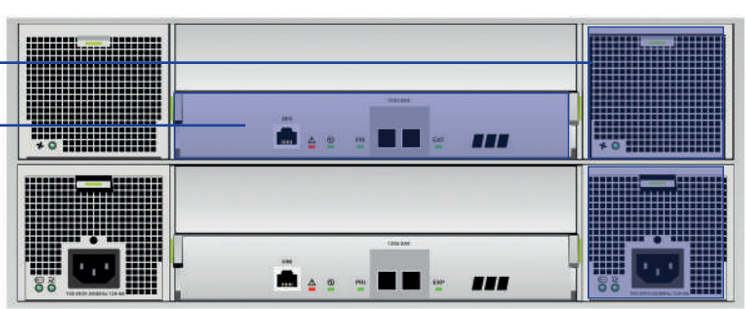
- 16 слотов для интерфейсных модулей с возможностью «горячей» замены
- Типы портов: 8 или 16 Гбит/с Fibre Channel, GE, 10GE TOE, 10GE FCoE и 12 Гбит/с SAS

Блоки питания

- 1+1
- Возможность «горячей» замены

4U полка расширения позволяет разместить 24x3,5" дисков

- Дисковый модуль
- Вентиляторный модуль
- Модуль расширения
- Блоки питания



SOLIDWORKS Впереди — лучшее

Уже почти 20 лет бренд SOLIDWORKS компании Dassault Systèmes доступен в странах СНГ. Только в России у него более 25 тыс. активных пользователей и около 10 тыс. постоянных подписчиков, а 30 тыс. студентов используют SOLIDWORKS в учебе. О том, что нового нам предложат решения SOLIDWORKS 2018 и SOLIDWORKS Manage рассказывает Алексей Маликов, директор по развитию бизнеса SOLIDWORKS в России и СНГ, Dassault Systèmes.

— Алексей, прошлый год принес большие изменения в бизнес SOLIDWORKS в России и СНГ. Расскажите, пожалуйста, о них.

— В четвертом квартале 2017 года мы объявили о стратегическом изменении бизнес-модели и расширении бизнеса SOLIDWORKS в России и странах СНГ. Решение об увеличении территории продаж SOLIDWORKS обосновано растущим спросом на продукты и сервисы, а также широким географическим разбросом клиентов Dassault Systèmes в России и СНГ. Таким образом, Dassault Systèmes начала выстраивать сеть партнеров и реселлеров, которая будет предлагать продукты бренда SOLIDWORKS, включая новейший релиз – SOLIDWORKS 2018.

Начиная с 1 октября 2017 года, компания Dassault Systèmes начала добавлять дистрибуторов, партнеров и реселлеров в России и странах СНГ, включая Казахстан, Украину, Молдову, Центральную Азию и Кавказ (Армения, Азербайджан, Грузия). Сеть партнеров в России будет включать в себя помимо Москвы, Санкт-Петербурга, Самары и Екатеринбурга другие крупные города, такие как Калининград, Воронеж, Ростов, Челябинск, Новосибирск, Красноярск и Владивосток. Это значительное расширение обеспечит поддержку клиентов и потенциальных клиентов в 11 часовых поясах, охватывающих более 70 городов. Мы рады, что такое значительное расширение партнерской сети произошло за счет нашего сотрудничества с Softline.

Значительное расширение партнерской сети произошло за счет нашего сотрудничества с Softline

На фоне этих изменений пользователи SOLIDWORKS смогут выбирать локальных поставщиков и получать индивидуальные услуги (например, тренинги, образовательные программы, центры компетенций, экзамены). В рамках этого диапазона сервисов партнеры и реселлеры будут играть ведущую роль в развитии сообщества пользователей SOLIDWORKS и их экосистемы в будущем.

В рамках глобальной стратегии развития каналов сбыта SOLIDWORKS, Dassault Systèmes стремится развивать свою партнерскую сеть и сеть реселлеров в России и странах СНГ для того, чтобы увеличить доступность портфеля продуктов SOLIDWORKS и предоставлять клиентам более широкий выбор. Упрощенное предоставление продвинутых приложений для проектирования и инженерии означает немедленный и индивидуальный доступ к ноу-хау, которые поддержат задачи разработки изделия. В результате, пользователи смогут в полной мере использовать возможности и преимущества этого портфеля продуктов. В данный момент более 2 млн дизайнеров и инженеров по всему миру используют SOLIDWORKS в своей ежедневной работе, создавая лучшие продукты за меньшее количество времени.

— Какие инновации появились в SOLIDWORKS 2018? Несколько слов об AI Denoiser – каковы преимущества этой функции?

— В грядущем SP3.0 появится обновление, разработанное в NVIDIA, AI Denoiser для SOLIDWORKS Visualize 2018. Данная функция ускоряет процесс рендеринга в 10 раз, благодаря AI (искусственному интеллекту) и уменьшает уровень шума. Это может быть неподвижное изображение, анимация, камера, покомпонентный вид, новый контент 360-VR

и т. д. — все это в 10 раз быстрее, чем сейчас. Это действительно делает Visualize самым быстрым и простым в использовании инструментом визуализации на рынке.

AI Denoiser будет работать как в режимах Fast, так и в Accurate. Чтобы воспользоваться преимуществами этой новой функции, необходимо настроить окончательные параметры рендеринга. Если раньше задавалось количество проходов 3000, для Accurate теперь нужно только 300 проходов. Поскольку рендеринг в Denoiser в 10 раз быстрее, можно ввести в 10 раз меньше проходов рендеринга! 5000 = 500; 2500 = 250; 1000 = 100; 500 = 50 и так далее.

AI Denoiser будет доступен с SOLIDWORKS Visualize 2018 SP3, как в Standard, так и в Professional.

Для того чтобы воспользоваться новой функцией, понадобится видеокарта NVIDIA, которая имеет как минимум 4 ГБ памяти (VRAM). Видеокарта также должна быть серии Kepler или новее.

Обновление для включения AI Denoiser означает, что графические карты NDIVIA поколения Fermi поддерживать не будут. Эти карты больше не поддерживаются Quadro FX серии и Quadro x000. Обновление Visualize 2018 SP3 и новее с этими устаревшими картами приведет к тому, что Visualize не будет использовать ваш графический процессор и работать только в режиме CPU. Чтобы продолжить использование Visualize с вашим GPU поколения Fermi, пожалуйста, оставайтесь на Visualize 2018 SP2 и не обновляйтесь до новых версий.

— Какие возможности предоставляет пользователям решение для управления данными SOLIDWORKS Manage?

— SOLIDWORKS Manage — это продвинутый продукт семейства PDM (Product Data Management), который предоставляет комплексные инструменты для управления проектами, процессами и элементами вашей компании.

Программа позволяет детально спланировать ключевые задачи, которые необходимо

AI Denoiser для SOLIDWORKS Visualize 2018 ускоряет процесс рендеринга в 10 раз!

выполнить для завершения этапов проекта и достижения поставленных задач. Задачи могут быть назначены конкретным департаментам или сотрудникам. Они сообщают о проделанной работе, используя «Временные ведомости» (time sheet), тем самым информируя менеджеров о ходе работы над проектом. Функции, которые могут связывать время и ход работы по каждой отдельной задаче, помогут коллегам получить подробную информацию о уже выполненных и планируемых задачах. Благодаря этому руководители могут легко контролировать ход работы над проектами.

Возможность создания простых и детализированных процессов позволяет осуществлять расширенную настройку состояний и точек принятия решений для всех типов бизнес-процессов. Во время процесса пользователи могут присоединять необходимые элементы и файлы, а менеджеры — устанавливать отдельные задачи, которые должны быть выполнены до следующего этапа разработки.

В результате интеграции SOLIDWORKS Manage и SOLIDWORKS PDM процессы разработки можно автоматически обновлять путем изменения состояния файла в рабочем процессе, создаваемом в SOLIDWORKS PDM. Панель мониторинга позволяет создавать интерактивные и графические информационные диаграммы для отображения всех критических данных, относящихся к любой переменной, которая хранится в базе данных SQL. Эта функция собирает всю важную информацию и показывает ее пользователям сразу после входа в систему.

Интегрированные отчеты, предоставляющие всю детальную информацию в зависимости от этапа проекта, могут генерироваться как автоматически по достижению определенного этапа, так и по запросу. ■

Благодаря взаимодействию с SOLIDWORKS PDM все операции, выполняемые непосредственно в SOLIDWORKS Manage, автоматически и без задержки отображаются в системе PDM. Интеграция взаимная.

Аддитивные технологии в учебных лабораториях

Наш мир быстро изменяется и приходится подстраиваться под темпы его изменения. Еще вчера учебные модели приходилось заказывать в специализированных магазинах, как и детали для лабораторных и практических работ по многим дисциплинам (моделирование, робототехника, химия, анатомия и др.).

В настоящее время все необходимое можно спроектировать, напечатать или размножить самостоятельно с помощью аддитивных технологий, позволяющих создавать объекты с помощью послойного наращивания и синтеза объекта. С одной стороны, это делает учебный процесс намного более увлекательным и запоминающимся для учащихся, с другой – упрощает задачу учителя, позволяя свободно выбирать темы для занятий, ведь любое наглядное пособие теперь можно просто напечатать.

MakerBot Replicator+

3D-принтер MakerBot Replicator+ предназначен как для любителей, так и для профессиональных инженеров и дизайнеров. В комбинации с новыми материалами и усовершенствованным экструдером, Replicator+ демонстрирует широкие возможности быстрого прототипирования и высокую надежность. В качестве расходного материала используется нетоксичный биопластик PLA (полилактид) двух типов: обычный или с повышенной ударостойкостью, прочностью на сжатие и разрыв (Tough PLA).

Но учебный процесс – не самоцель, а лишь средство для того, чтобы по завершению обучения учащиеся заведения умели использовать современное оборудование. Если еще вчера в резюме не стыдно было написать «умение пользоваться офисной техникой», то завтра понадобится «умение работать с устройствами 3D-печати», а офисной техникой и сегодня никого уже не удивить. Таким образом, создавая специализированные лаборатории, учреждения среднего, средне-специального и высшего образования не только делают учебный процесс наглядным и запоминающимся, но и повышают свой престиж, давая своим студентам знания, соответствующие запросам современного мира.

Зачем это нужно?

Действительно, уже сейчас 3D-технологии широко используются в медицине, робототехнике, постепенно внедряются на производстве. В промышленности появились скоростные модели 3D-принтеров. Уже известны отдельные случаи использования таких принтеров для серийного производства. Например, компания Adidas запустила 3D-печать подошв для кроссовок. В прошлом году первые партии такой обуви поступили в магазины. Потенциально это способно в корне изменить многие отрасли промышленности, так как такая печать стоит намного дешевле и осуществляется быстрее.

Навыки и знания, полученные в лаборатории 3D-моделирования и прототипирования, совершенно необходимы будущим инженерам-конструкторам, инженерам-проектировщикам, архитекторам, дизайнерам интерьеров и архитектурных проектов, дизайнерам одежды и многим другим специалистам.

В чем заключается сложность?

Итак, мы пришли к выводу, что создание лабораторий 3D-моделирования и прототипирования является не-

обходимым атрибутом учебного заведения, которое хочет соответствовать современным образовательным стандартам. Но есть одна проблема. Вполне решаемая. Дело в том, что сегодня нет ни одного производителя (поставщика), который бы обеспечивал образовательные учреждения одновременно и оборудованием, и программными продуктами. Так, компании, поставляющие ПО для моделирования, не согласовывают информацию с поставщиками 3D-принтеров, и как результат, преподаватель остается один на один с разрозненными технологиями.

Что же делать?

Из сложившейся ситуации есть простой и очевидный выход. Компания Softline предлагает комплексное решение в оснащении лаборатории 3D-моделирования и прототипирования. Мы используем опыт мировых лидеров – программы по 3D-моделированию Autodesk и 3D-принтеры MakerBot и многие другие.

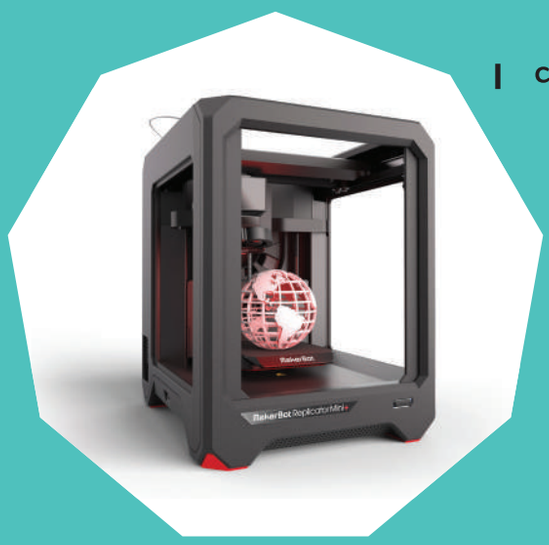
Решения Softline включают современные облачные технологии, позволяющие ученикам продолжить проект дома, а преподавателю дистанционно отслеживать процесс работы и его результаты. Такой подход позволит вывести проектную деятельность на новый уровень, обеспечить стабильную работу программ и техники для непрерывности учебного процесса.

На белорусском рынке только компания Softline обладает необходимыми компетенциями, опытом и квалифицированным персоналом, который может помочь в решении проблем, возникающих при создании лаборатории 3D-моделирования и прототипирования.

TINKERCAD AUTODESK TINKERCAD AUTODESK FUSION 360 Thingiverse 3DS MAX

Компоненты лаборатории 3D-моделирования

- Программное обеспечение для 3D-моделирования компании Autodesk с бесплатной лицензией для образовательных учреждений.
- Комплект учебно-методических материалов, обучение работе с программами моделирования и работе с оборудованием.
- Методологическая и техническая поддержка.
- Комплект 3D-оборудования для лаборатории в составе: 3D-принтер MakerBot: Replicator+ (флагманское решение), Replicator Mini+ (компактное решение) и 3D-сканер Digitizer.



Replicator Mini+

MakerBot Replicator Mini, усовершенствованный вариант компактного 3D-принтера, предназначен для бытовой и образовательной 3D-печати. Replicator Mini+ имеет скромные габариты, более низкую стоимость, чем его предшественник, но при этом демонстрирует более высокие характеристики и надежность. Принтер спроектирован с учетом пользовательской безопасности и использует только нетоксичные расходные материалы.

Digitizer 3D scanner

Портативный настольный 3D-сканер предназначен для качественной оцифровки физических объектов. Makerbot Digitizer создавался для работы в комплекте с 3D-принтерами Replicator 2 и Replicator 2X, однако полностью совместим с новейшими 3D-принтерами Replicator пятого поколения, а также большинством настольных 3D-принтеров других брендов. Дизайн устройства и программного обеспечения направлен на упрощенную эксплуатацию при максимальном качестве получаемых цифровых 3D-моделей.

Остались вопросы?

Обращайтесь к Роману Довганчуку, менеджеру по направлению «Строительство/ГИС» Softline по телефону +375 (17) 388-95-95 (доб. 4400) или по e-mail: Roman.Dovganchuk@softline.com

Инструменты для проектирования систем отопления

BIM-технология позволяет не просто моделировать сооружения, но и получать информационную модель объекта. По сути, это процесс коллективного создания и использования информации о сооружении, формирующий надежную основу для всех решений на протяжении жизненного цикла объекта (от самых ранних концепций до рабочего проектирования, строительства, эксплуатации и сноса).

Что дает нам BIM?

Для проектировщиков – это автоматизация сложных процессов и, как следствие, значительное сокращение сроков проектирования. BIM дает возможность совместно работать над одной цифровой моделью, тем самым объединяя участников проекта. Имея трехмерную информационную модель, мы исключаем ошибки проектирования, сокращаем сроки на внесение изменений и на выходе получаем высококачественную проектную документацию.

Применение при проектировании системы центрального и внутрипольного отопления

Программа Audytor OZC 6.9 предназначена для тепловых расчетов зданий.

Для ввода конструкции здания в графическом режиме требуется значительно меньше времени, чем для ввода информации в таблицы.

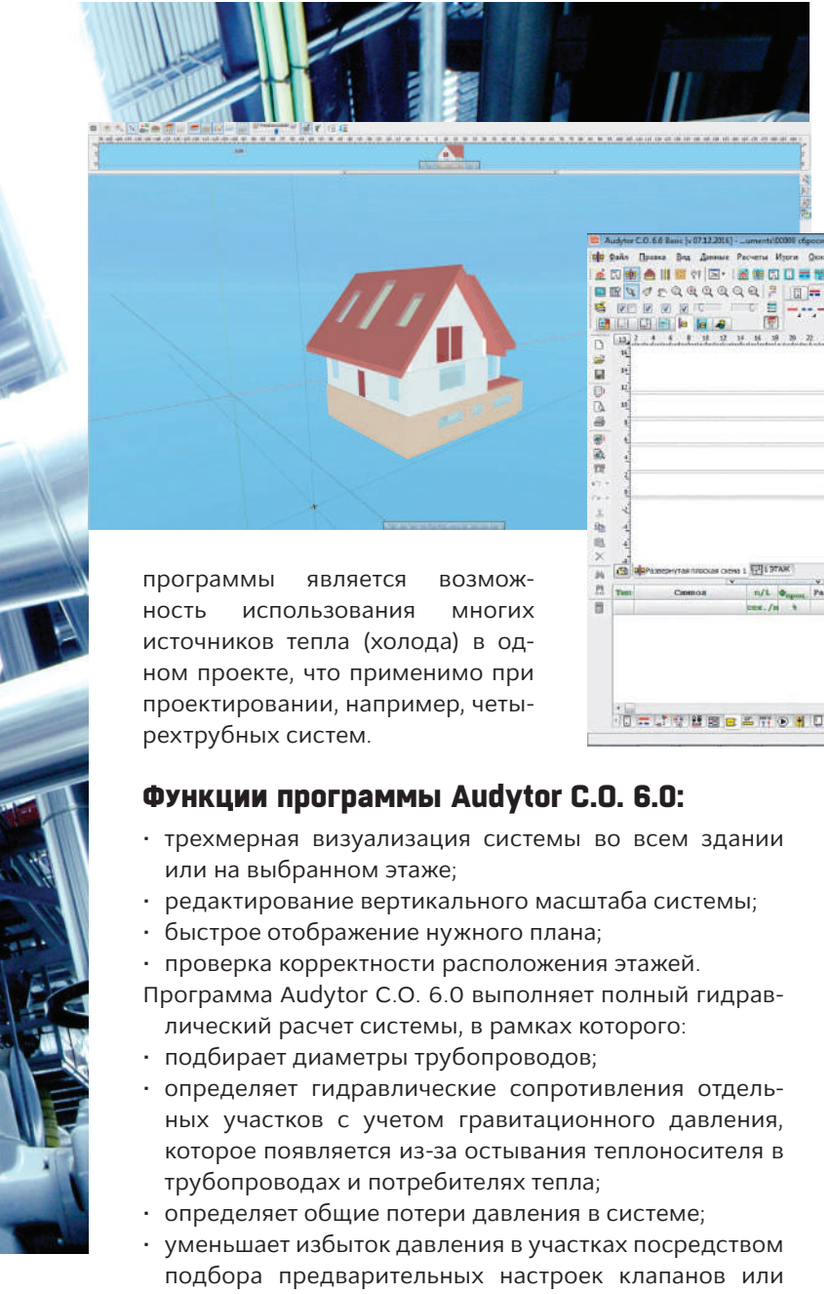
Главные преимущества программы заключаются в ее повышенной функциональности. Приложение оснащено рядом полезных инструментов, в том числе функцией автоматической вставки полов, крыш и зон помещений, а также функциями, облегчающими связывание строительных ограждений. Программа дает возможность выполнять автоматический расчет объема помещений даже со сложной формой, например, расположенных на чердаке.

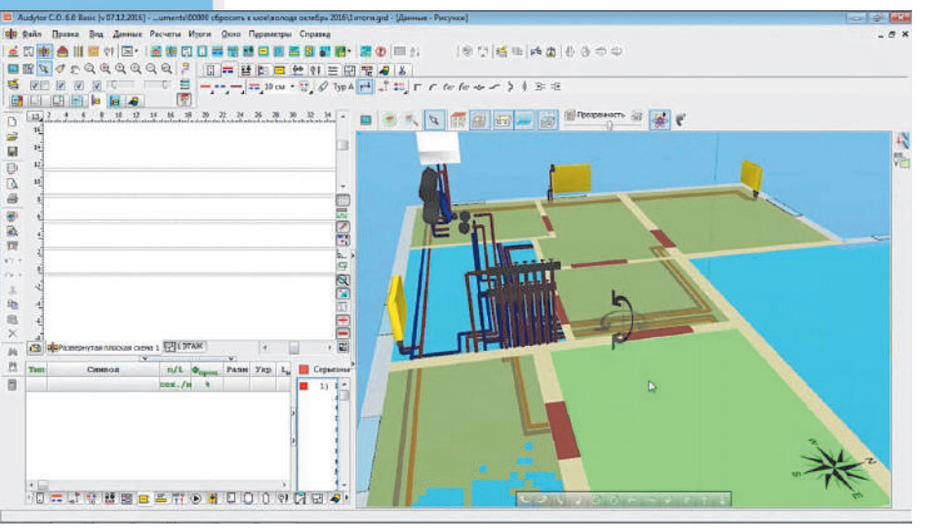
Визуализация здания позволяет легко найти ошибки, которые могут быть незамечены в таблицах (отсутствие крыши, слишком краткая стена, слишком низкая стена и т.д.).

Главные преимущества программы Audytor OZC 6.9:

- создание графической трехмерной модели здания;
- анализ графической трехмерной модели здания и создание на ее основе расчетной модели;
- отрисовка скатных крыш, а также автоматический расчет объема помещений с разной высотой потолка (например, на чердаке);
- сканирование строительных подоснов без необходимости использования других программ;
- склейка сканированных частей строительной подосновы.

Программа Audytor C.O. 6.0 предназначена для проектирования новых систем отопления и регулирования существующих (например, в зданиях после тепловой модернизации), а также для проектирования систем трубопроводов в холодоснабжении. Преимуществом





программы является возможность использования многих источников тепла (холода) в одном проекте, что применимо при проектировании, например, четырехтрубных систем.

Функции программы Audytor C.O. 6.0:

- трехмерная визуализация системы во всем здании или на выбранном этаже;
- редактирование вертикального масштаба системы;
- быстрое отображение нужного плана;
- проверка корректности расположения этажей.

Программа Audytor C.O. 6.0 выполняет полный гидравлический расчет системы, в рамках которого:

- подбирает диаметры трубопроводов;
- определяет гидравлические сопротивления отдельных участков с учетом гравитационного давления, которое появляется из-за остывания теплоносителя в трубопроводах и потребителях тепла;
- определяет общие потери давления в системе;
- уменьшает избыток давления в участках посредством подбора предварительных настроек клапанов или подбора диаметра отверстия дроссельной шайбы, а также учитывает необходимость обеспечения надлежащего гидравлического сопротивления участка;
- подбирает настройки регуляторов перепада давления, установленных проектировщиком в выбранных им местах (основание стояка, ветвь системы, т.д.);
- автоматически учитывает требования относительно авторитетов термостатических клапанов (соответствующий перепад давления на клапанах);
- подбирает квартирные станции с теплообменниками;
- подбирает буферные накопители тепла, работающие с квартирными станциями;
- подбирает насосы, насосные группы;
- позволяет применять гидравлические стрелки и спаренные коллекторы.

Программа Audytor C.O. 6.0 выполняет тепловой расчет, в рамках которого:

- определяет теплопоступления от трубопроводов, находящихся в помещениях;
- определяет остывание теплоносителя в трубопроводах;
- для указанной потребности в тепловой мощности определяет требуемые размеры отопительных приборов;
- подбирает нужный расход теплоносителя, поступающего в существующие потребители тепла с учетом его остывания в трубопроводах, а также теплопоступления от трубопроводов (вариант регулирования существующей системы, например, в утепленных зданиях);
- учитывает воздействие остывания теплоносителя в трубопроводах на значение гравитационного давления в отдельных участках, а также на тепловую мощность потребителей тепла;
- определяет параметры проектируемых напольных отопительных приборов.

Audytor C.O. 6.0 позволяет создать проект:

- насосной системы;
- системы трубопроводов (однотрубной, двухтрубной, смешанной);
- тепло- или холодоносителя (воды, этиленгликоля, пропиленгликоля);

BIM в Беларуси

Беларусь является лидером среди стран Восточной Европы и Центральной Азии в освоении технологии информационного моделирования (BIM, Building Information Modeling). В 2012 году в стране была утверждена отраслевая программа внедрения информационных технологий комплексной автоматизации проектирования и поддержки жизненного цикла здания, сооружения. Таким образом, Беларусь стала одной из первых стран (наряду с Великобританией), которая на государственном уровне приняла программу внедрения BIM. Существенным вкладом в развитии BIM-технологий явилось введение 1 марта 2016 года СТБ ISO/TS 12911-2015 «Основные положения руководства по информационному моделированию зданий». Одним из последних прорывных событий развития BIM можно назвать приказ № 70 от 16 марта 2018 года Министерства архитектуры и строительства «О внедрении технологии информационного моделирования», в котором расписан четкий план внедрения BIM до 2022 года.

В прошлом году программы Audytor OZC 6.9 и Audytor C.O. 6.0 разделились на версии Basic и Pro. Отличие версии Pro от Basic заключается в возможности импорта модели здания из программы Autodesk Revit в программу Audytor OZC 6.9 Pro и экспорта запроектированной системы из программы Audytor C.O. 60 Pro в программу Autodesk Revit. Файлы, созданные в версиях Basic, будут открываться в версиях Pro.
Вместе с тем в программе Audytor OZC 6.9 Pro появилась возможность загружать трехмерную расчетную модель здания непосредственно из программы REVIT 2016, 2017 с помощью бесплатного плагина Audytor gbXML, а также механизм проверки корректности загруженной модели здания и автозаполнения необходимых данных для выполнения теплового расчета.

- нижней и верхней разводки, системы с горизонтальной разводкой, коллекторных систем;
- конвекционных, напольных или стеновых отопительных приборов;
- автоматических воздухоотводчиков;
- обычных или термостатических радиаторных клапанов;
- предварительной регулировки посредством использования клапанов с преднастройкой или дроссельных шайб.

В одном проекте можно одновременно использовать арматуру, трубопроводы и отопительные приборы различных производителей.
Программа Audytor C.O. дает возможность проектировать большие системы (даже 140 стояков и 12 000 отопительных приборов). Поставляемая вместе с программой библиотека типовых фрагментов рисунков (блоков), таких как этажные стояки, элементы поквартирных и распределительных систем, позволяет быстро создавать развернутую плоскую схему. Кроме того, пользователь может создавать почти неограниченное количество собственных блоков, состоящих из любых фрагментов рисунка. Данные блоки могут быть затем использованы в других проектах. Благодаря функции размножения элементов рисунка можно, например, ввести фрагмент развернутой плоской схемы системы для всего этажа (очередные стояки или поквартирные системы) и затем автоматически создать схему и данные для следующих этажей.

Импорт строительных подоснов из программы Autodesk Revit

Функция позволяет в программе Audytor C.O. создать схему планов, соответствующих этажам из программы Autodesk Revit, на которых были созданы помещения. Перенос данных из файла, созданного в программе Autodesk Revit, осуществляется с использованием плагина Audytor gbXML.

Экспорт проекта системы в программу Autodesk Revit

Функция позволяет экспортировать проект системы и загружать его в программу Autodesk Revit с помощью плагина Audytor C.O. for Revit. Также можно экспортировать систему как из данных, так и из итогов. Экспорт из данных позволяет сохранить неполный проект системы (еще не рассчитанный), например, только схему стояков или схему размещения отопительных приборов. Экспорт из итогов позволяет использовать в программе Autodesk Revit технические данные подобранных трубопроводов, а также другого оборудования (например, диаметры и настройки клапанов, размеры отопительных приборов, шаг укладки трубопроводов в ТП).

Отдел САПР/ГИС компании Softline активно работает со всеми заказчиками, которые создают проекты и принимают проектные решения, занимаются строительством или эксплуатацией объектов капитального строительства. Мы предлагаем проверенные инструменты и решения лидирующих разработчиков BIM-систем со всего мира, позволяющие ускорить процесс создания объектов капитального строительства, повысить качество выпускаемой продукции и обслуживания.

Новости Учебного центра Softline

Предлагаем анонс новых курсов, проводимых Учебным центром Softline

Microsoft System Center 2016

Курс	Длительность
Администрирование System Center Configuration Manager (20703-1)	5 дней/40 ак. ч.
Интеграция MDM и облачных сервисов с System Center Configuration Manager (20703-2)	3 дня/24 ак. ч.

Администрирование System Center Configuration Manager (20703-1)

Курс описывает использование System Center Configuration Manager и связанных с ним систем сайта для эффективного управления ресурсами сети. Слушатели курса изучат ежедневные задачи управления при помощи System Center Configuration Manager: управление приложениями, мониторинг здоровья клиентов, инвентаризацию программного и аппаратного обеспечения, развертывание ОС и обновление ПО.

Интеграция MDM и облачных сервисов с System Center Configuration Manager (20703-2)

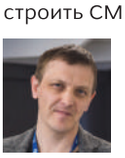
В этом курсе даются знания по технологии управления мобильными устройствами (MDM) и интеграции различных облачных сервисов с Microsoft System Center Configuration Manager (SCCM). Курс сфокусирован одновременно на двух сценариях управления мобильными устройствами (MDM): локальном и гибридном с использованием Microsoft Intune.

Информационная безопасность

Курс	Длительность
Создание системы менеджмента информационной безопасности на основе требований ISO 27001	2 дня/16 ак. ч.
Аудит информационной безопасности	4 дня/32 ак. ч.

«Создание системы менеджмента информационной безопасности на основе требований ISO 27001»

Курс предназначен для руководителей и специалистов подразделений по информационной безопасности (ИБ); аудиторов, ответственных за разработку и внедрение систем менеджмента по качеству и ИБ; для всех желающих понять, как строить СМИБ и пройти сертификацию ISO/IEC 27001.



Тренер курса Алексей Евменков, специалист по ИТ-безопасности

Опыт работы в сфере ИТ более 19 лет, в области информационной безопасности – более 10 лет в качестве специалиста, аудитора, руководителя подразделений и консультанта. Преподаватель авторских курсов по информационной безопасности.

«Аудит информационной безопасности»

В программе курса вопросы разработки программы, методики, процедуры аудита информационной безопасности (ИБ) предприятия в соответствии с PCI DSS, ISO 27001, ISO 27002, ISO 19011 и лучшими практиками в области ИБ. Подробно изучаются все аспекты аудита – от общих высокоуровневых подходов к планированию и проведению аудита до технических деталей аудита конкретных средств управления информационной безопасностью.

В ходе практических занятий проводится аудит специально разработанной для курса информационной системы.

Тренер курса Вячеслав Аксенов, специалист по ИТ-безопасности

Опыт работы в сфере информационной безопасности: более 13 лет в качестве специалиста, инженера, аудитора, менеджера, руководителя проекта, архитектора и консультанта. Преподаватель авторских курсов по информационной безопасности.

PostgreSQL

Курс	Длительность
Основы сервера базы данных PostgreSQL. Основы развертывания и использования приложений для базы данных. Трехзвенная архитектура	5 дней/40 ак. ч.

Курс предназначен для начинающих администраторов, которые сопровождают или планируют сопровождать приложения для сервера базы данных PostgreSQL и сервера приложений WildFly (или подобного ему).

В программе курса также рассматриваются основные концепции построения приложений масштаба предприятия и размещение их на сервере приложений для организации транзакционного доступа к базе данных PostgreSQL.

Обучение будет полезно как администраторам серверов баз данных, так и руководителям ИТ-подразделений – в процессе занятий будет рассмотрено множество конкретных примеров построения и сопровождения приложений на предприятии.

С полным перечнем курсов по информационной безопасности вы можете ознакомится на нашем сайте **edu.softline.by**.

Подписывайтесь на страничку нашего учебного центра на Facebook, чтобы быть в курсе последних новостей, акций и полезных советов наших инструкторов:

https://www.facebook.com/SoftlineEducationBelarus

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
20412	Дополнительные службы Windows Server 2012 R2	5 /40
20413	Проектирование и реализация серверной инфраструктуры	5 /40
20414	Реализация продвинутой серверной инфраструктуры	5 /40
10961	Автоматизация администрирования с использованием Windows PowerShell	5 /40
10962	Расширенная автоматизация администрирования с помощью Windows PowerShell	3 /24
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 в Windows Server 2016	5 /40
20743	Обновление навыков до MCSA: Windows Server 2016	5 /40
20744	Обеспечение безопасности Windows Server 2016	5 /40
Курсы Windows 10		
20697-1	Внедрение и управление Windows 10	5 /40
20697-2	Развертывание и управление Windows 10 с помощью корпоративных служб	5 /40
20698	Установка и конфигурирование Windows 10	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
20765	Обеспечение баз данных SQL	3 /24
20767	Внедрение хранилищ данных SQL	4 /32
20768	Разработка моделей данных SQL	3 /24
10986	Обновление навыков до SQL Server 2016	3 /24
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 Azure		
20532	Разработка решений Microsoft Azure	5 /40
20533	Применение инфраструктурных решений Microsoft Azure	5 /40
Курсы по Office 365		
20347	Подключение и управление Office 365	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
20696	Администрирование System Center Configuration Manager и Intune	5 /40
20745	Внедрение программно-определяемого центра обработки данных	5 /40
10748	Планирование и развертывание System Center 2012 Configuration Manager	3 /24

Код	Название курса	Дни/часы
Курсы по виртуализации серверов		
20409	Виртуализация серверов с использованием Hyper-V и System Center	5 /40
20694	Виртуализация корпоративных рабочих столов и приложений	5 /40
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 - программы корпоративного обучения		
Excel	Базовый курс по Microsoft Excel	2 /16
Excel-Adv	Углубленный курс по Microsoft Excel	3 /24
VBA-Excel	Программирование на VBA для Microsoft Excel	3 /24
BI-Excel-Adv	Бизнес-аналитика средствами Microsoft Excel, Power BI и Power BI Desktop	3 /24
Word	Базовый курс по Microsoft Word	2 /16
Word-Adv	Углубленный курс по Microsoft Word	2 /16
PowerPoint	Создание презентаций в Microsoft PowerPoint	1 /8
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
CCNAX	Создание сетей на базе оборудования Cisco: ускоренный курс	5 /60
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
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
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 в сетях Cisco	Реализация мультипротокольной коммутации с использованием меток 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
SQL1	Oracle Database: основы SQL 1	3 /24
SQL2	Oracle Database: основы SQL 2	2 /16
PLSQL	Oracle Database: основы PL/SQL	2 /16
DPU	Oracle Database: разработка программных модулей на PL/SQL	3 /24
APLS	Oracle Database: передовые методы PL/SQL	3 /24
TSQL	Oracle Database: настройка SQL-операторов баз данных	3 /24

Код	Название курса	Дни/часы
ASQL	Oracle Database: аналитические функции SQL в хранилищах данных	2 /16
BAR	Oracle Database: резервирование и восстановление	5 /40
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-104	Основы системного администрирования SUSE Linux	3 /24
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
SL-108	Расширенное администрирование SUSE Linux Enterprise Server 12	5 /40
CentOS-1	Введение в администрирование операционной системы CentOS 7	4 /32
VMware		
VSICM 6.5	VMware vSphere: установка, настройка, управление [v.6.5]	5 /40
VSFT 6.5	VMware vSphere: ускоренный курс [V6.5]	5 /50
VSOS 6.5	VMware vSphere: оптимизация и масштабирование [v.6.5]	5 /40
VSTW 6.5	VMware vSphere: устранение неисправностей [V6.5]	5 /40
VHICM 7	VMware Horizon 7: установка, настройка, управление [V7.3]	5 /40
«Лаборатория Касперского»		
KL 002.104	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 009.10	Kaspersky Endpoint Security and Management. Управление системами	1 /8
KL 010.10	Kaspersky Endpoint Security and Management. Управление мобильными устройствами	2 /16
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-F	Основы ITIL 2011	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
ServiceDesk	Организация службы Service Desk	3 /24
COBIT-F	Основы COBIT 5. Расширенный курс	3 /24
IT4IT	IT4IT: эталонная архитектура и операционная модель для управления ИТ-деятельностью	3 /24
KeyPractices	Ключевые практики руководства, контроля и управления ИТ-службой организации на основе подходов COBIT 5 и ITIL-2011	4 /36
Информационная безопасность		
ОИБ	Основы информационной безопасности	3 /24
ISO 27001	Создание системы менеджмента информационной безопасности на основе требований ISO 27001	2 /16
ISRM	Оценка и управление рисками информационной безопасности в организации	2 /16
ISA	Аудит информационной безопасности	4 /32
САИС	Создание автоматизированных систем в защищенном исполнении	3 /24

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

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 lab

PEARSON VUE AUTHORISED CENTRE

Контакты

г.Минск, 220113,
ул. Мележа, 5/2-1103
+375 17 216 18 66
educ@softline.by

ГЛОБАЛЬНЫЙ ПОСТАВЩИК ИТ-РЕШЕНИЙ И СЕРВИСОВ

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

+375 (17) 388 95 95 | www.softline.by